Data-driven approaches for cyber defense of battery energy storage systems

Kharlamova, Nina; Hashemi, Seyedmostafa; Træholt, Chresten

Published in:
Energy and AI

Link to article, DOI:
10.1016/j.egyai.2021.100095

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

Energy and AI 5 (2021) 100095

Contents lists available at ScienceDirect

Energy and AI

journal homepage: www.sciencedirect.com/journal/energy-and-ai

Data-driven approaches for cyber defense of battery energy storage systems

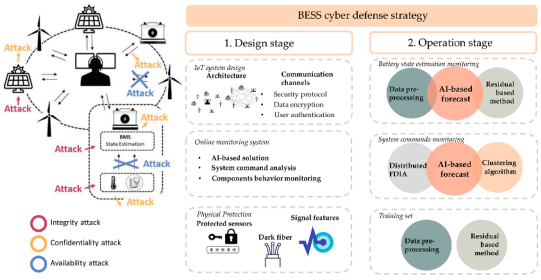
Nina Kharlamova, Seyedmostafa Hashemi *, Chresten Træholt

Technical University of Denmark, Copenhagen, Denmark

HIGHLIGHTS

- Utility-scale battery energy storage systems are vulnerable to cyberattacks.
- There is a lack of extensive review on the battery cybersecure design and operation.
- We review the state-of-the-art battery attack detection and mitigation methods.
- We overview methods to forecast system components behavior to detect an attack.
- We discuss how ML and AI-based methods can support cyber defense of battery systems.

GRAPHICAL ABSTRACT



ARTICLE INFO

Keywords:
Cyber security
Artificial intelligence
Battery energy storage system
False data injection attack
Cyberattack
Machine learning

ABSTRACT

Battery energy storage system (BESS) is an important component of a modern power system since it allows seamless integration of renewable energy sources (RES) into the grid. A BESS is vulnerable to various cyber threats that may influence its proper operation, which in turn impacts negatively the BESS and the electric grid. The potential failure of a BESS can cause economic issues and physical damage to its components. To ensure cyber-secure and reliable BESS operation in grid-connected or islanded modes of the BESS operation, a cyber-defense strategy is needed. However, a comprehensive review on the requirements for the BESS design as well as the attack detection and mitigation methods is lacking. In this paper, we review state-of-the-art attack detection and mitigation methods for various BESS applications focusing on machine learning (ML) and artificial intelligence (AI)-based methods. In addition, the state-of-the-art methods for designing and operating a cyber-secure BESS are investigated. Based on the literature review, we identified gaps in the current research, defined the possible cyberattacks against the BESS that have not been considered before, and suggested the potential approaches to detect them.

1. Introduction

Nowadays, the battery energy storage system (BESS) has become an important component of the electric grid [1]. It can serve multiple services such as frequency regulation, voltage control, backup, black start, etc. [2]. The inability to provide a requested service can compromise the reliability of electric grid operation, the drop of energy quality as well as the failure to supply energy, economic challenges and physical damage [3]. Moreover, inadequate BESS management can cause rapid battery degradation. The batteries integrated into smart grids are vulnerable to cyber threats. Cyberattacks can be divided into groups based on various features [4] such as based on the part of the system that they are targeted

* Corresponding author.
E-mail address: shtog@elektro.dtu.dk (S. Hashemi).

https://doi.org/10.1016/j.egyai.2021.100095
Received 8 February 2021; Received in revised form 4 April 2021; Accepted 11 June 2021
Available online 13 June 2021

at, or the jeopardized feature of data [5]. In this review, the latter classification is used.

A BESS is vulnerable to various cyber threats [6]. Since it is connected to the electric grid, cyberattacks against the smart grid might also jeopardize the work of the BESS and system in general. The BESS contains several parts that are interconnected and in case one system component is attacked, the whole system operation is corrupted. For instance, the cyberattack on communication channels might result in the false state of charge (SOC) estimation and forming a false command for the BESS. It is important to take into account all BESS components in order to provide a reliable defensive strategy that includes detecting false data injection attack (FDIA) against sensing data, battery, and grid state estimation (SE), protecting sensing units and communication channels.

The existing research related to the cyber security of batteries is mostly related to their applications in the electric vehicles (EV) domain [7–10]. Cyberattacks on certain BESS components such as battery management system (BMS) [11–13], SOC forecast [14–17], communication channels [11], and algorithms for attack vector development [18] are suggested in recent literature. Due to the digitalization of the electric grid, the technology of the internet-of-things (IoT) is applied for the electric grid, and the approaches for cyber-secure IoT system operation and encryption technologies can be used for the BESS as well [11,13,19]. Nevertheless, to the best of our knowledge, there is no comprehensive study reviewing and investigating the BESS cyber defense algorithms neither for the design nor operation stages. In addition, the reliability of system commands is not considered. The paper provides a comprehensive overview of BESS cyber threats, both for design and operation stages. This work focuses on the techniques proposed for cyber-secure BESS design as well as online attack detection and mitigation methods in the operation stage. It aims at providing a path for a trustworthy and cyber-secure BESS operation.

The paper is organized as follows. In Section 2, we survey BESS cyber threats that can result in the failure of ensuring data integrity, confidentiality and availability of the system. We investigate the challenges of applying stolen data for designing more complex and hard-to-detect cyberattacks. In Section 3, we derive the approaches to design the BESS to curtail the possibility of a cyberattack. In Section 4, cyberattack detection methods are reviewed and analyzed, and in Section 5, the mitigation of cyberattacks is discussed.

2. Classification of Cyber Threats for the BESS

Cyber threats of the BESS might have a different nature: the attack can be carried out physically or remotely. There are three major requirements for system data that are integrity, confidentiality, and availability. Data integrity implies that the measurements or commands were not modified, the confidentiality stands for the absence of data leakage since no unauthorized party can retrieve it. The availability means that an authorized party can access the data at any time needed. Possible attacks on the system are presented in Fig. 1. Based on described data features we apply the classification of cyberattacks that is depicted in Fig. 2. Table 1 summarizes the literature sources depending on the type of the attack they consider.

2.1. Integrity attack

The integrity attack modifies, delays, or replays data to manipulate system parameters [5]. The attack can be not targeted or targeted to achieve some particular goal. FDIA is an integrity attack since they imply the injection of false data to the system. Every system component is vulnerable to integrity attacks. Adding physical protection of system layers on the design stages diminishes the possibility of the attack. In this section, we describe data integrity attacks.

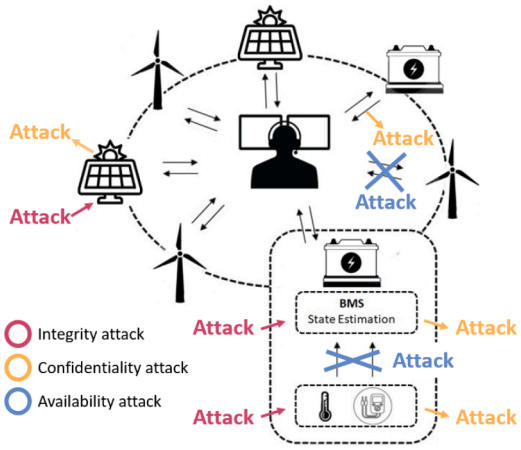


Fig. 1. The cyber threats of the BESS.

2.1.1. FDIA attacks

FDIA results in data manipulation and depending on the knowledge of the attacker about the system, its topology, and retrospective data, these attacks are divided into multiple groups. We categorize FDIA as purely data integrity-based that does not use any system data to form an attack vector and a confidentiality-based data integrity attack that applies previously stolen data to complicate the FDIA detection.

As mentioned above, we consider battery cells to be a black box in which measurement units, BMS, and control system are physically protected by the battery producer. Thus, we limit the possibilities of FDIAs against the BESS to battery and electric grid SE as well as command attacks. The concept of cyberattack against the electric grid that can be carried out unnoticed for the bad data detector (BDD) was firstly introduced by Liu in 2009 [32]. Since then the topic of FDIA against the electric grid gained wide attention of researchers [33]. There are also examples of the cyberattacks that happened in Pakistan [34] and Ukraine [35], and have cause economical damage to the grid. In [36], authors describe two attack scenarios in which the attack is targeted against all sensors of the system or it is assumed that there are physically protected sensors that cannot be hacked.

2.1.2. FDIA against electric grid SE

The FDIA against the electric grid is the most frequent attack in the electrical energy domain. The measurements within the electric grid are connected physically depending on the Kirchhoff laws and system topology. Physical dependencies are used to detect the FDIA. The attacker has to take into account these dependencies for the attack to not be easily detected. Replay attacks are the type of FDIA that are based on real data and, therefore, are hard to detect. In addition, zero-dynamic attacks use unstable zero bugs to attack meters [20,21]. FDIA can be aimed to achieve a certain goal, e.g., to sabotage frequency or voltage control system. There are FDIA attacks that can be targeted against various parts of the system [37]. For example, supervisory control and data acquisition (SCADA) system can be damaged or totally disturbed by cyberattacks [38]. Moreover, the attacker can utilize retrospective system data to construct attacks that are more challenging to detect as highlighted in [38]. Coordinated attacks are aimed to cover the real operation conditions of the system in order to distract its operation [39]. For example, the physical attack against a transmission line can be hidden by means of cyberattack [40]. The actions of control system can be further manipulated by hiding system failure that was not caused by attacker to avoid the correct work of protection system (e.g. in case of the shortcut) or replaying the data obtained during the shortcut while there are no system failures in the reality [41]. The example of FDIA based on the system data obtained through confidentiality attack is described in details in Section 2.2.2.

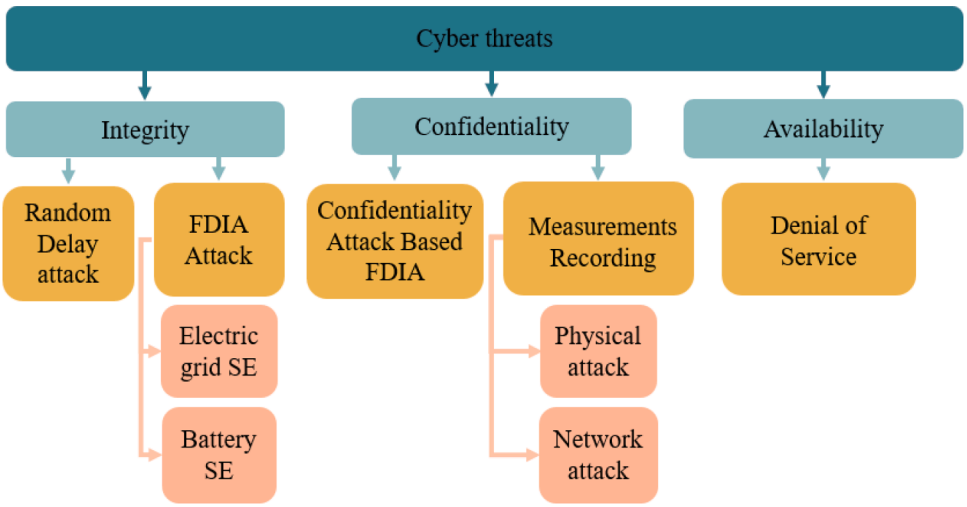


Fig. 2. The classification of cyber threats for the BESS.

Table 1
Literature review for each type of cyberattack.

Source	Integrity Attack	Confidentiality attack	Availability attack	Detection
[5]	X	X		
[20,21]	X			
[22]	X	X		
[23,24]	X			X
[25]	X			
[18]		X		
[26]		X		
[13,27]	X	X		
[5]	X	X		X
[28–30]			X	
[31]			X	

2.1.3. FDIA against battery SE

Cyberattack can be targeted at any system component including the BESS [42]. The distributed nature of BESS expands the possibilities of cyberattacks against it and required the application of cyber defense mechanism to minimize the possibility of such an attack [4]. The attack can potentially corrupt the battery's SE that contains the data about SOC, state of health (SOH), based on the measurements obtained in battery cells since these parameters cannot be measured directly [43]. In this paper, we use the definition of SOC provided in [16] that is the ratio between the available to rated battery capacity. SOH represents battery degradation in order to estimate the change in the battery capacity due to the aging process. Inaccurate SOC and SOH evaluation results in forming corrupted control command that might lead to the battery overcharge causing the degradation and physical damage and financial losses [23,24] as well as failure to provide the required service. In the frame of the EV battery application, an undetected cyberattack accelerates battery degradation. Battery capacity decreases within the lifetime of the battery cell due to degradation. It is important to take this change into account since otherwise the system operator (SO) or local management unit does not possess reliable battery capacity data to manage the power supply. This might lead to the BESS being unable to act according to the control commands.

2.1.4. Random delay attack

A random delay attack stands for an attack that adds a delay into the sequence of measurements or control commands. This attack can disturb the work of the grid. The additional complexity is added due to the inability of cryptography to protect the system from cyberattacks [22]. The cyberattacks on batteries are mostly discussed in the frame of the EV domain. Therefore, we use the research carried out in the EV sector to describe attacks to which the BESS can be potentially vulnerable. Potential and real cyberattacks were considered in the literature [23,24]. The most straightforward attack against SOC is to inject higher values of SOC in the situation of low charge. The defense strategy is to form an acceptable range of SOC between the minimum and maximum value. In this case, the attacker cannot increase SOC more than the fixed maximum parameters. To prevent an attack detection, the adversary can form false SOC so that it satisfies physical constraints and increases the value of SOC gradually, removing an attack as soon as the boundary condition is met and inject it back within the attack period is reached to further add false data once the boundary is reset. In addition, the targeted attack against the electric grid or battery SE causes rapid degradation and loss of efficiency [25]. In this case, an attack vector formed to decline battery lifetime and decrease battery capacity.

2.2. Confidentiality attack

Confidentiality is the feature of data that implies that data can be accessed only by authorized parties [44]. A confidentiality attack is an attack in which system data is recorded and stolen by an unauthorized party. Some researchers state that confidentiality is not necessary for the system data [45]. However, although this attack might seem less dangerous for a system, the data retrieved during this attack might be implemented to design a more complex FDIA. In this section, the attacks that violate system data confidentiality are discussed.

2.2.1. Cyber threats for the BESS confidentiality

The data can be retrieved from the system in various ways. Firstly, sensing units or communication channels, as well as system specific data such as grid topology, can be stolen physically (e.g. physical theft, manipulating meters on the consumer side, dumpster diving). Besides, the data can be stolen without physical access to it through direct download, passive monitoring, unauthorized user access to the data, spyware malware, phishing, and cross-site scripting [18]. Confidentiality attacks can be targeted at sensors, communication channels, and data storage. The man-in-the-middle attack is a type of attack against data confidentiality that records data that is transferred through a communication channel by placing an unreliable user between two nodes [26]. Confidentiality attacks on battery are mostly studied in electric vehicle (EV) domain [46].

2.2.2. Confidentiality attack based FDIA

One of the threats of confidentiality attacks is the ability of an attacker to utilize obtained data to construct another attack. An adversary can spam storage with stolen data [13], as well as injecting it back

to the system making a replay attack.

The major threat of confidentiality-based FDIA is that since the attack is based on seized historical data or system topology it is challenging to detect and can be confused with unusual but unspoiled system measurements. Moreover, the attacker can follow a particular goal, e.g. to manipulate the system state. To be successfully injected into the system, confidentiality attack based FDIA requires carrying out integrity and confidentiality attack simultaneously. Confidentiality attacks enable the attacker to carry out coordinated attacks that are capable of causing more harm than ordinary FDIA. For instance, the attacker can organize the replay attack in such a manner that the system disturbance is unnoticed by the control system [40].

The replay attack is one of the examples of confidentiality-based FDIA that include stealing sensing data and repeatedly broadcasting in [20]. Furthermore, some FDIAs are based on full or partial knowledge of historical data or system topology. Detecting the attack is one of the challenges tackled in the electric grid domain [5]. Resonance attacks manipulate system SE by adjusting system measurements [27].

2.3. Availability attack

Availability of data is the ability of the authorized parties to access data upon the request. The loss of this data quality can be caused by multiple factors including power supply loss, operating system or application problems, cyberattacks, compromised system, etc. [47,48]. The failure to provide data availability results in the absence of system observability. According to [47], the availability attack can be also caused by integrity attack when the configuration file that is in charge of managing the particular service behavior is accessed and altered; therefore, the service availability might be affected by changing the content of the file. One of the most common attacks against data observability is a denial of service (DoS) attack in which physical or network connections are overloaded [49]. The attack disturbes the operation of communication channels [28–30] and might be especially dangerous for the islanded grid in which the BESS might be a major power supply source [30]. Besides, secondary frequency control might be vulnerable towards this kind of an attack [31]. DoS can potentially disturb the work of the smart grid. The latency attack delays dispatch signal in order to modify system characteristics and harm the reliable operation. This attack can be difficult to detect since it can be confused with system latency. Being cost-effective, this attack is efficient from the viewpoint of the resources needed to maximize the negative influence on the system [50].

3. Design of cyber-threats-aware BESS

While we cannot eliminate the possibility of a cyberattack, the proper design of the BESS allows us to minimize the chance of successful cyber arracks. In this section, we overview existing approaches for cyber-secure aware smart grid and BMS design to provide a list of tools to consider while designing the BESS. The main steps of the BESS design include choosing the system architecture, communication channel protection methods, user authentication, as well as physical methods. The steps are depicted in Fig. 3.

3.1. Architecture

Depending on the system architecture, the system vulnerability towards cyberattacks may vary. An electric grid with multiple BESS can be controlled through decentralized, centralized, and distributed control architectures. The centralized architecture allows us to realize the collaborative control strategies through utilizing central controller that collects data from each BESS and finds the global optimum that cannot be computed for each BESS separately. The vulnerability of such architecture is the single failure point since in case the central controller is corrupted, operation of all BESSs in the system will be disturbed [4]. The

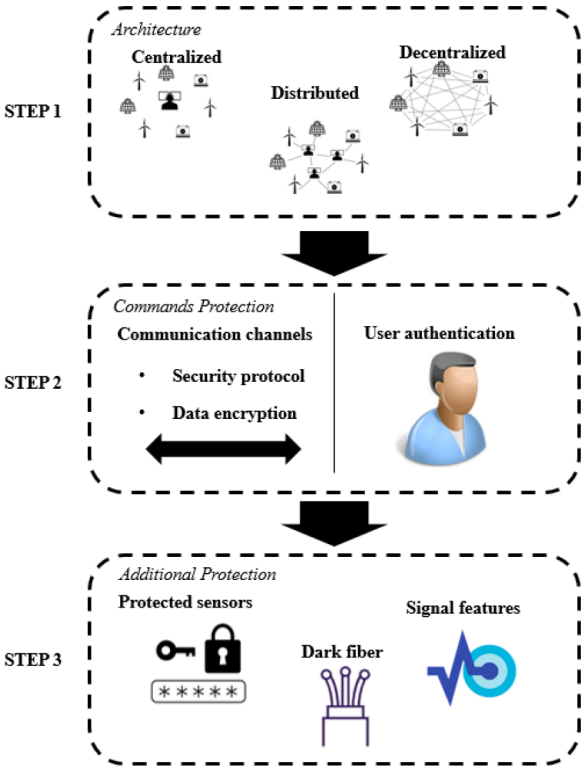


Fig. 3. The stages of the cyber-secure BESS design process.

decentralized architecture (that is also referred to as a flat architecture [51]) does not have this weakness; however, since each BESS gathers measurements locally, the work of BESS cannot be optimized in a centralized way [52]. This type of architecture provides the highest level of security [51]. The additional drawback of the centralized approach is the high cost since it requires a fast and highly reliable communication network [53].

The distributed control architecture (that is also referred to as hierarchical or cluster architecture [51]) combines the benefits of the two above-mentioned approaches and is recommended for the implementation in case the hybrid solution is necessary [51]. Each BESS is presented as an autonomous agent connected to multiple neighbors to exchange information for operation mode calculus. In this way, the distributed architecture enables us to reach a common objective while managing multiple BESSs and widen the surface of an attack. One of the most secure architectures of distributed systems is blockchain that is the system that register each transaction by means of multiple devices connected in a peer-to-peer network [4]. Distributed topology formation algorithms allow mitigating the negative influence of DoS attack since it allows to isolate attacked nodes so that they are circumvent and the algorithm successfully converges in the distributed manner while multiple nodes of the system are attacked by DoS [31].

3.2. Communication channels and user authentification

Smart grid experiences cyber threats of a different kind such as unauthorized software updates or IoT devices that can potentially cause havoc [54] and inadequate battery management resulting in battery damage. Confidentiality of the data can be disturbed mainly through communication channels. The probability of the availability attack that mostly is related to the DoS can be diminished by adding physical protection of communication channels' security as well as data encryption and user authentication. Although in this paper, we consider cyber security from the BESS perspective assuming that the methods to provide cyber security for the electric grid are set by default, we overview the

existing approaches in order to detect which of them might be adapted for implementation in the BESS framework.

There are numerous approaches to secure communication channels in the literature including, e.g., security protocols, data encryption, blockchain technologies implementation, security protocols. Applicable authentication mechanisms (e.g. LoadAP, S3PAP-C, etc.) and encryption methods are overviewed in detail in [55]. The applicability of the protocol depends on the level of data security that is required for the particular implementation. For example, some network protocols such as MQTT and HTTP that are widely implemented and not secure enough might cause a failure of ensuring secure management of the system; however, they are widely used by browsers (e.g. Opera, Google Chrome, etc.). HTTP also provides the possibility of introducing the security protocol. Various protocols that use encryption can be ranked depending on the security and configurability [56]. The variations of security level come from the difficulty of hacking the encryption key that can be symmetric or asymmetric [57]. The symmetric key is used for both encrypting and decrypting data, while asymmetric key is used only for one purpose. In centralized a architecture, the central controller has to provide security keys to all the members and to monitor system safety. The centralized architecture is less secure than decentralized and distributed one since if the attacker is able to disturb a few transactions from central controller, the entire network can be isolated [51].

The blockchain was initially introduced as a financial transaction (TX) protocol. However, since this technology provides the high level of security since it uses cryptographic security benefits e.g. distributed architecture, asymmetric keys in the combination with user authentication, it was implemented in other domains [58]. In addition, the data can be encrypted and decrypted in the distributed manner, which means that the data cannot be read or introduced into the system by hacking only one node [58]. Blockchain is a promising technology for implementation in BMS design. It ensures network, data storage, software, onboard interface security as well as hardware security [11] as an alternative to the state of the art. The main advantage of the blockchain is the decentralized structure. Each user has access to the historical data only through the agreement with other users. The data are encrypted with an asymmetrical key that tangles the data-stealing. In addition, each user is going through the authentication procedure to avoid unauthorized access to the data [59].

Adapting blockchain technology for the BESS management results in using more light-weight security protocols minimizing the computational cost and memory size comparing with state-of-the-art strategies [19]. Data storage security is maintained by applying the distributed architecture of blockchain [58]. Blockchain provides authorized identity management to avoid the access of unauthorized users from sending commands and retrieving data. However, there are additional challenges of adapting blockchain technology such as limitations by the memory size of embedded systems since all nodes have to store complete blockchain ledgers, limited randomness of private keys, and scalability issues. Nevertheless, due to the specific requirements of BESS, these challenges do not have a significant impact on the high potential of blockchain technology in BESS management. Thus, the technology is suggested for the implementation by multiple sources [4,11] to safeguard cyber-secure communication between the SO and BESS, data storage, reliable battery control.

3.3. Additional protection

In the smart grid domain, the numerical attack detection methods are combined with utilizing the equipment and physical features of signal to complicate the cyberattack. One of the state-of-the-art approaches to detect FDIA for electric grid SE is to combine the cyberattack detection algorithm with physical protection of the part of sensors [60]. Moreover, the measuring units within the utility-scale BESS are protected physically from cyberattack, and, consequently, the data can be jeopardized only through communication channels. Although there is a physical possibility to protect each part of the system using the secure equipment, it raises the installation cost; therefore, the engineers are required to find the balance between utilizing the equipment to minimize the possibility of cyberattack and numerical algorithms to detect and mitigate it.

As to communication channels security, blockchain is suggested for the implementation in the BESS cyber defense to reduce the possibility of understanding stolen data and injecting FDIA (by using data encryption and distributing the keys across multiple nodes so that hacking one user is not enough to encrypt and decrypt data). Moreover, the system can be protected using the equipment. For example, dark (unlit) fiber that is not connected to the internet or managed by the SO can be used as a communication channel.

Random delay attacks can be detected by adjusting signal features. If the control signal frequency is high, the control period exceeds the delay introduced into the system. In this case, the attack can be mitigated by dropping timeout control packets [22].

4. Detection Methods of BESS Cyberattacks

To ensure cyber-secure operation of the BESS, it is important to carry out online detection of possible cyberattacks on sensing measurements [14,61]. The detection methods are presented in Fig. 4.

4.1. Manipulated battery SE attack detection

The dataset of the proper size and quality is required to obtain a sufficient detection accuracy. Due to the EV being a spread application of batteries, most battery SOC forecast methods are tested on EV datasets. One of the common datasets described in the literature are Federal Urban Driving Cycles (FUDS), and US06. The efficiency of machine learning (ML) and ANN approaches application on different datasets is highlighted in [62]. However, there is no state-of-the-art attack detection algorithm for industrial implementation.

It is worth mentioning that the utility-scale BESS has a different working cycle from the EV. Despite there are many EV-related datasets available and various forecast approaches tested on them, we cannot fully rely on the test results due to the difference in the datasets. We can adjust methods used for EV datasets data preprocessing to increase the forecast accuracy with the regard to the differences between datasets.

BMS is used to manage the BESS taking into account battery parameters e.g. SOC. Based on the measurements, the battery can achieve better performance, slow down degradation, and provide a safe operation. Sensing units are placed in battery cells to control voltage, current, and temperature. In this work, we assume that the sensing units in batteries are protected and, therefore, the possibility of FDIA is eliminated. To prevent the attack against battery SOC, the forecasting methods can be applied.

The state-of-the-art FDIA against the electric grid detection method is based on comparing the SE forecast with the sensing data. If the difference between the estimation and measurements that is called residual exceeds the given threshold, the FDIA is considered to be detected. BDD is based on the residual method. It applies the weighted least square criterion (WLS) for FDIA detection [61]. The drawback of this method is that with some limited amount of hacked sensors the FDIA can stay undetected. To ensure that the detection of FDIA is possible, physical protection of sensors is used [32].

The measurement forecast is necessary for residual-based method implementation. Therefore, we overview the methods to forecast SE in Section V. The ML and artificial intelligence (AI) methods are suggested to use for battery SE forecast since they have a high potential for forecast implementation due to their robustness and accuracy.

Data preprocessing algorithm has to be improved to meet the needs of data-driven approaches due to high requirements to initial data. Model adjustment (e.g. adjusting hyperparameters, activation function), and work under uncertainties (e.g. battery degradation) further complicates the issue of the attack detection and requests further

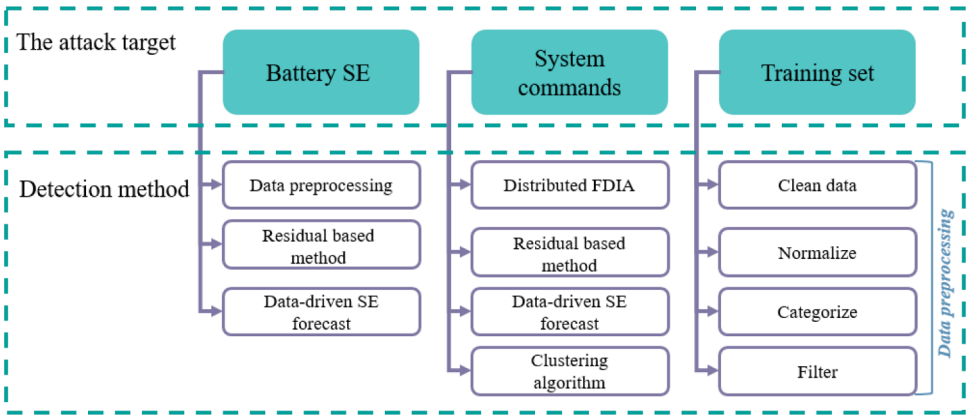


Fig. 4. The methods for the BESS cyberattacks detection.

exploration.

Since the performance of the ML and AI-based approach is critical for system safety, it is vital for the detection algorithm to be understandable [63]. The transparency of the AI algorithms is not only critical for evaluating the method performance but also useful for cyberattacks studying by engineers [64]. Despite the articles mentioned above did not take into account the transparency of the decision making process as a criterion for performance evaluation, there are studies related to improving discussed methods transparency. The problem of transparency of cyberattack detection mechanism is studied by various researchers in different domains [64], e.g. EV [63]. The main aim of explainable AI (XIA) is to detect the main features based on which the decision is made. These features' relevance for the output forming can be evaluated using domain knowledge so that the XIA algorithm's performance is evaluated. There are multiple libraries (e.g. Lime, What-if Tool, etc.) that are used to visualize the importance of each feature for the output. However, most of these libraries are applicable in case of test or image processing, while it is more challenging to visualize this process for time series processing [65]. One of the proposed solutions is hybrid oracle-explainer intrusion detection system that visualized the AI decision-making process [64].

4.2. System commands attack detection

Due to the constant data exchange between the BESS and the electric grid, possible cyberattacks against the smart grid might influence the integrity of commands that the BESS receives. In this paper, we define a novel type of attack on the BESS data integrity employing FDIA against the grid. The detection of the system cyberattack from the BESS viewpoint is a challenging problem that does not have an accepted solution yet.

The BESS is managed with the regard to the needs and requirements of the system it is connected to. Therefore, there is a possibility of a cyberattack on the integrity and confidentiality of control commands as well as the combination of those since the data stolen during the confidentiality attack might be applied to create an undetectable integrity attack. There is no widely accepted solution regarding control commands FDIA detection in the BESS domain. In the section, we overview potential solutions for this attack detection.

Distributed methods were introduced in the smart grid domain in order to carry out the cyberattack detection in decentralized systems. Guan and Ge in [66] introduced a distributed cyberattack detection method for wireless sensor networks applying design desired resilient attack detection estimators. The primary idea of the method is to form a residual signal and to determine a residual evaluation function that is compared to the predefined threshold. Distributed FDIA detection is split into multiple groups that are statistical-based, data time-stamps based, and estimation residuals based [49]. A decentralized consensus strategy is the type of statistical-based one. It includes a distributed average consensus algorithm and distributed receding-horizon control [67]. The residual-based methods are based on state-of-the-art FDIA detection on SE [68]. It includes juxtaposing the sensing and forecasted data [32], the difference should not exceed a given threshold. A reliable forecast is needed for the residual-based approach application.

Local measurements are necessary to improve the quality of the SE forecast to take into account the type of service. Mashlakov et al. [69] propose SOC forecasting algorithm for the BESS that works for frequency control. The algorithm is tested on different datasets to study the features of frequency control and the system's dynamics. In [14], the forecast of SOC is carried out utilizing the frequency measurements to manage the BESS.

In addition, ML and AI-based FDIA methods are applied to detect cyberattacks locally. Deep learning is widely implemented in FDIA detection, e.g. feed forward deep neural network (NN), convolutional NN, deep NN, recurrent NN, deep belief network, restricted Boltzmann machine, deep auto-encoder, deep migration learning, self-taught learning, and replicator NN [70]. The paper analyzed the results of the listed above methods application with the system features as an input and the data about the reliability of measurement as an output. The case studies described in the paper showed that deep learning detects cyberattacks with the sufficient accuracy above 98%. Based on the literature review, the authors prove that deep learning is a robust and efficient tool for cyberattack detection. In [71], the application of deep learning for IoT local attack detection is overviewed. It was defined that deep learning algorithm shows higher accuracy than ordinary machine learning approaches and raises the accuracy up to 99%. The training set for the deep learning algorithm can be obtained through simulations [72] or from the existing databases [62].

The clustering approach is unsupervised algorithm widely used for typical load profiles [73,74] might be adapted for system commands forecast that does not require labelled data. In [74], probabilistic neural networks (PNNs) are applied to cluster consumers based on their load profile to form a typical load profile. The number of clusters is estimated by the "knee" criterion. This criterion is described in [74], and the optimal number of clusters is such a number for which the value of objective function representing cluster validity measure reaches its' knee.

5. Mitigation methods of BESS cyberattacks

Once the attack is detected, its influence on BESS operation has to be mitigated. In this step, we are aware that some system data are not reliable; however, we are not able to obtain the accurate measurements. An undetected FDIA might result into jeopardizing historical data applied for the training purposes and corrupting the forecast. For that reason, we generate pseudo-measurements to feel the gap generated by a

cyberattack. With no regard to the type of an attack, there is a cyber insurance option in which the responsibility on the system integrity protection and mitigation of the possible negative impact is given to the third party [75]. In this section, two major mitigation methods that are pseudo-measurements generation [73] and SE forecast are considered. The methods are summarized in Fig. 5.

5.1. Pseudo-measurements generation

In order to mitigate the negative influence of cyberattacks on the BESS, pseudo-measurements are generated to fill the gaps caused by unreliable data. Active and reactive energy consumption pseudo-measurements generation is a widespread task. Consumption can be potentially forecasted through nonlinear functions of measurements available at the main substations. Nevertheless, this approach is not widely implemented due to its low scalability. Thus, researchers apply data-driven approaches to tackle this problem. In [76] the artificial neural network (ANN) is applied for direct current SE. The input is real power flow, while the output is a forecast. The training set contains an annual offline system SE with various profiles. One of the spread approaches is forecasting the consumption by clustering typical load profiles using labeled data [73,74]. In [74], the authors use PNNs to form a typical load profile by clustering consumers into groups based on their behavior, where an input data is labeled using domain knowledge. The number of clusters can vary. It is chosen depending on the "knee" criterion. In [74], the frequency-based clustering is applied to forecast the behavior of consumers that are not equipped with smart meters based on those that are equipped. In [77] parallel distributed processing networks (PDP) are implemented to forecast loads. The method was proved to resist the errors in sensing data and the temporary failure of the communication system [78].

The above-mentioned methods can be potentially adapted for the generation of the pseudo measurements for battery SE FDIA. Summarizing the state-of-the-art, we derive that the forecast methods form the core of pseudo-measurements generation. In the following section, we provide a detailed review of the existing methods for battery SE prediction.

5.2. Battery SE forecast

5.2.1. Model-based methods for battery SE

Battery SE parameters such as SOC cannot be measured directly. They are estimated from current, voltage, and temperature measurements of the battery. Despite coulomb counting and equivalent circuit model (ECM) being the state-of-the-art approaches for SOC forecast, these methods have significant drawbacks. The data related to the initial cell state is required for coulomb counting. The inaccuracy in the initial data caused by model and sensor errors results in further mistakes in the forecast. ECM does not take into account the physicochemical processes that appear in the battery cell. Besides, comprehensive empirical parameterization is required.

Kalman filter (KF) was initially used for experimental data processing. Plett adapted KF for Li-ion cells modeling [12]. In addition, he suggested combining the extended Kalman filter (EKF) with the dynamic cell model to dynamically estimate SOC. The typical estimation error is within a few percent. Despite the complexity of the method implementation compared to coulomb counting, it diminishes the accumulative error comparing with the state-of-the-art battery test equipment (an Aerovironment ABC-150). EKF provides an accurate forecast for the short tests of several hours. The ambient temperature below 0C increases the forecast error of EKF [12].

5.2.2. Data-driven methods for battery SE

The robustness of data-driven forecast algorithms and their ability to detect implicit correlations between parameters attracted researchers' attention. These algorithms were suggested for the implementation of the SOC forecast in the EV domain and can be potentially exploited for other BESS applications [7,9].

Data-driven algorithms for SOC estimation can be divided into multiple groups [62]. There are multiple classifiers applied for SOC forecast in the literature. One of the most commonly implemented is ANN: feed-forward neural network (NN), recurrent NN for sequential data processing [31], deep NN (e.g. deep belief NN) [16]; fuzzy logic, and the combination of ANN and fuzzy logic that is adaptive neuro-fuzzy inference system. Support vector machine (SVM), Gaussian process regression, random forest as well as hybrid algorithms are implemented. ANN is the most widely mentioned approach. We highlight that in the literature the high emphasis is put on the application of feed-forward NNs that are the simplest type of ANN.

The results of ANN implementation for SOC forecasts are widely presented in the literature. Despite the conclusion regarding the most suitable approach for the SOC forecast cannot be derived based on the literature review since the methods were tested on different datasets, we distinguish that normally the maximum SOC error is between 2 and 8 %. The minimum-maximum SOC error was obtained using the RF but this does not imply that this method is normally more accurate than competitors. It is vital to highlight that in most cases the forecast was carried out for the implementation in EVs, while in this work we are focused on the utility-scale BESS implementation [62]. Consequently, an additional numerical evaluation is required to choose the most suitable method for SOC forecast of utility-scale BESS.

There can be a combination of reasons for the anomaly, such as the difference between batteries' features due to lot-to-lot variation together with the cyberattack that may increase the complexity of forecast to

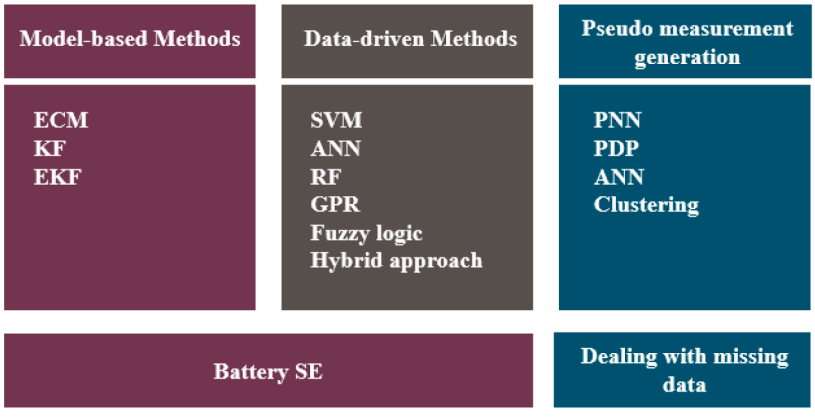


Fig. 5. The methods for the BESS cyberattacks mitigation.

detect the attack. The SOH influences the SOC forecast that adds additional complexity to the problem. It is critical to detect not only short-term anomalies utilizing battery operation forecast but also long term anomalies such as anomalous degradation [79] since some cyberattacks are designed to damage the BESS in the long run.

6. Conclusions

BESS is becoming an important part of power systems, and cyber security of BESS has to be provided in both design and operation stages. In addition, cyberattacks on electric grids that can influence the work of the BESS have to be considered. We reviewed recent work in the field and concluded that blockchain and physical protection methods are the main approaches proposed to diminish the possibility of cyberattacks in the design stage. Regarding the operation stage, various FDIAs detection and mitigation methods are proposed in the literature, and a comprehensive review of related papers was presented in this paper. We concluded that the application of data-driven algorithms including AI has a high potential in the domain of sensor measurement forecast and has been widely discussed in the recent literature. Likewise, these approaches are adapted to forecast battery SE such as SOC and SOH. In the future work, the reviewed methods are to be compared on the same dataset of a utility-scale BESS.

We also conclude that with no regard for the implementation, data preprocessing is necessary to form a reliable training set for ML algorithms. The integrity of training data is specifically important for ensuring the forecast accuracy. Thus, the algorithms for FDIA detection should be applied to the training dataset as well. According to the recent literature, we concluded that the clustering method for FDIA detection, residual-based method combined with the ML-based forecast, and distributed FDIA detection methods can be adapted for this purpose. According to the analyzed literature, the share of ML-based algorithms for BESS cyber defense is expected to enlarge. An additional research is required to define a more comprehensive cyber defense algorithm to ensure the reliable utilization of BESS along with the approaches that would be the most suitable for the applications in BESS cybersecurity. Nevertheless, based on the current literature review, it is suggested to apply clustering for the cyberattack detection since it might be able to identify the unknown attack along with deep learning utilized as a forecast tool to apply residual-based cyberattack detection mechanism. Due to cyber security domain being a safety-critical application, it is vital for the cyber defense algorithm to have a transparent decision-making process. The paper reviewed existing methods for improving AI transparency and detects the lack of the research related to the algorithm transparency connected to the particular method. This is another concern that is to be addressed in the future research to provide a list of tools for cyber defense strategy development.

It is worth mentioning that the majority of state-of-the-art papers in the field of BESS cybersecurity are focused on the cyberattacks on BMS communication channels or EV domain, and there is a lack of comprehensive research focusing on the unreliable command that can be sent from the SO or third parties to the BESS. Therefore, current solutions are not sufficient to ensure the cyber-secure operation of BESS in renewable energy systems.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work is supported by the Danish project “BOSS: Bornholm smartgrid secured by grid connected battery systems” co-founded by Danish Energy technology Development and Demonstration program (EUDP) contract no. 64018-0618.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.egyai.2021.100095.

References

[1] Hameed Z, Hashemi S, Traeholt C. Site selection criteria for battery energy storage in power systems. In: Canadian Conference on Electrical and Computer Engineering. 2020-August; Aug. 2020. https://doi.org/10.1109/CCECE47787.2020.9255678.
[2] Joubert CJ, Chokani N, Abhari RS. Impact of large scale battery energy storage on the 2030 central european transmission grid. In: International Conference on the European Energy Market, EEM. 2018-June; Sep. 2018. https://doi.org/10.1109/EEM.2018.8469789.
[3] Simmhan Y, Kumbhare AG, Cao B, Prasanna V. An analysis of security and privacy issues in smart grid software architectures on clouds. In: 2011 IEEE 4th International Conference on Cloud Computing; 2011. p. 582–9.
[4] Mhaisen N, Fetais N, Massoud A. Secure smart contract-enabled control of battery energy storage systems against cyber-attacks. Alexandria Eng. J. 2019;58(4):1291–300. https://doi.org/10.1016/j.aej.2019.11.001.
[5] Gunduz MZ, Das R. Cyber-security on smart grid: threats and potential solutions. Comput. Networks Mar. 2020;169:107094. https://doi.org/10.1016/j.comnet.2019.107094.
[6] Wu Y, Xue Q, Shen J, Lei Z, Chen Z, Liu Y. State of health estimation for lithium-ion batteries based on healthy features and long short-term memory. IEEE Access 2020;8:28533–47. https://doi.org/10.1109/ACCESS.2020.2972344.
[7] I. Nedyalkov and D. Arnaudov, “Attacks and security measures of the exchanged information in the charging infrastructure for electromobiles,” Sep. 2019, doi: 10.1109/ET.2019.8878500.
[8] Dey S, Khanra M. Cybersecurity of plug-in electric vehicles: cyber attack detection during charging. IEEE Trans. Ind. Electron. Jan. 2020:1. https://doi.org/10.1109/tie.2020.2965497.
[9] C. Niddodi, S. Lin, S. Mohan, and H. Zhu, “Secure integration of electric vehicles with the power grid,” Oct. 2019, doi: 10.1109/SmartGridComm.2019.8909774.
[10] Farmann A, Sauer D. A comprehensive review of on-board state-of-available-power prediction techniques for lithium-ion batteries in electric vehicles. J. Power Sources 2016;329:123–37. https://doi.org/10.1016/j.jpowsour.2016.08.031.
[11] Kim T, et al. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg. Sel. Top. Power Electron. Jan. 2020:1. https://doi.org/10.1109/jestpe.2020.2968490.
[12] Plett GL. Extended Kalman filtering for battery management systems of LiPB-based HEV battery packs. J. Power Sources 2004;134(2):277–92. https://doi.org/10.1016/j.jpowsour.2004.02.033.
[13] Kumbhar S, Faika T, Makwana D, Kim T, Lee Y. Cybersecurity for battery management systems in cyber-physical environments. In: 2018 IEEE Transportation Electrification Conference and Expo (ITEC); 2018. p. 934–8.
[14] Gundogdu B, Gladwin DT, Foster MP, Stone DA. A forecasting battery state of charge management strategy for frequency response in the UK system. In: Proceedings of the IEEE International Conference on Industrial Technology. 2018-Febru; Apr. 2018. p. 1726–31. https://doi.org/10.1109/ICIT.2018.8352443.
[15] Hong J, Wang Z, Chen W, Wang L-Y, Qu C. Online joint-prediction of multi-forward-step battery SOC using LSTM neural networks and multiple linear regression for real-world electric vehicles. J. Energy Storage 2020;30:101459. https://doi.org/10.1016/j.est.2020.101459.
[16] Zhang X, Cai M, Wang C, Gao L, Fan X. Research for SOC prediction of lithium battery based on GA-ESN. In: 2018 11th International Symposium on Computational Intelligence and Design (ISCID). 02; 2018. p. 165–8.
[17] Watrin N, Blunier B, Miraoui A. Review of adaptive systems for lithium batteries State-of-Charge and State-of-Health estimation. In: 2012 IEEE Transportation Electrification Conference and Expo (ITEC); 2012. p. 1–6.
[18] Ullah F, Edwards M, Ramdhany R, Chitchyan R, Babar MA, Rashid A. Data exfiltration: a review of external attack vectors and countermeasures. J. Netw. Comput. Appl. 2018;101:18–54. https://doi.org/10.1016/j.jnca.2017.10.016.
[19] Khan MA, Salah K. IoT security: review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. 2018;82:395–411. https://doi.org/10.1016/j.future.2017.11.022.
[20] Cui L, Qu Y, Gao L, Xie G, Yu S. Detecting false data attacks using machine learning techniques in smart grid: a survey. J. Netw. Comput. Appl. 2020;170:102808. https://doi.org/10.1016/j.jnca.2020.102808.
[21] Pasqualetti F, Dorfler F, Bullo F. Attack detection and identification in cyber-physical systems. IEEE Trans. Automat. Contr. 2013;58(11):2715–29. https://doi.org/10.1109/TAC.2013.2266831.
[22] Y. Wu, J. Weng, B. Qiu, Z. Wei, F. Qian, and R. H. Deng, “Random delay attack and its applications on load frequency control of power systems,” Nov. 2019, doi: 10.1109/DSC47296.2019.8937611.
[23] A. Greenburg, “Hackers remotely kill a Jeep on the highway - with me in it,” *Tech. Rep., [Online]*, 2015.
[24] “Cyber attacks in connected cars: what Tesla did differently to win,” *Tech. Rep., [Online]*, 2017.

[25] Guo L, Ye J, Du L. Cyber-Physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyber-attacks. IEEE Trans. Transp. Electrif. 2020:1.

[26] "Man-in-the-middle, ENISA glossary," [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/man-in-the-middle.

[27] Wu Y, Wei Z, Weng J, Li X, Deng RH. Resonance attacks on load frequency control of smart grids. IEEE Trans. Smart Grid Sep. 2018;9(5):4490–502. https://doi.org/10.1109/TSG.2017.2661307.

[28] Liu J, Gu Y, Zha L, Liu Y, Cao J. Event-triggered h∞ load frequency control for multiarea power systems under hybrid cyber attacks. IEEE Trans. Syst. Man, Cybern. Syst. Aug. 2019;49(8):1665–78. https://doi.org/10.1109/TSMC.2019.2895060.

[29] Di Lu K, Zeng GQ, Luo X, Weng J, Zhang Y, Li M. An Adaptive Resilient Load Frequency Controller for Smart Grids with DoS Attacks. IEEE Trans. Veh. Technol. May 2020;69(5):4689–99. https://doi.org/10.1109/TVT.2020.2983565.

[30] Liu S, Hu Z, Wang X, Wu L. Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks. IEEE Trans. Ind. Informatics Jul. 2019;15(7):4066–75. https://doi.org/10.1109/TII.2018.2885170.

[31] P. Srikantha and D. Kundur, "Denial of service attacks and mitigation for stability in cyber-enabled power grid," Jun. 2015, doi: 10.1109/ISGT.2015.7131827.

[32] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM Conference on Computer and Communications Security; 2009. p. 21–32. https://doi.org/10.1145/1653662.1653666.

[33] Li Y, Wang Y. Developing graphical detection techniques for maintaining state estimation integrity against false data injection attack in integrated electric cyber-physical system. J. Syst. Archit. May 2020;105:101705. https://doi.org/10.1016/j.sysarc.2019.101705.

[34] "Militant Attack Plunges Pakistan Into Darkness | World News | Sky News." https://news.sky.com/story/militant-attack-plunges-pakistan-into-darkness-10374055 (accessed Mar. 16, 2021).

[35] "U.S. government concludes cyber attack caused Ukraine power outage | Reuters." https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K (accessed Mar. 16, 2021).

[36] Nateghi S, Shtessel Y, Edwards C. Cyber-attacks and faults reconstruction using finite time convergent observation algorithms: Electric power network application. J. Franklin Inst. Jan. 2020;357(1):179–205. https://doi.org/10.1016/j.jfranklin.2019.10.002.

[37] Xiang Y, Wang L, Liu N. Coordinated attacks on electric power systems in a cyber-physical environment. Electr. Power Syst. Res. Aug. 2017;149:156–68. https://doi.org/10.1016/j.epsr.2017.04.023.

[38] Liang G, Zhao J, Luo F, Weller SR, Dong ZY. A Review of False Data Injection Attacks Against Modern Power Systems. IEEE Transactions on Smart Grid Jul. 01, 2017;8(4):1630–8. https://doi.org/10.1109/TSG.2015.2495133. Institute of Electrical and Electronics Engineers Inc.

[39] Deng R, Xiao G, Lu R, Liang H, Vasilakos AV. False data injection on state estimation in power systems-attacks, impacts, and defense: A survey. IEEE Trans. Ind. Informatics Apr. 2017;13(2):411–23. https://doi.org/10.1109/TII.2016.2614396.

[40] Li Z, Shahidehpour M, Alabdulwahab A, Abusorrah A. Analyzing locally coordinated cyber-physical attacks for undetectable line outages. IEEE Trans. Smart Grid Jan. 2018;9(1):35–47. https://doi.org/10.1109/TSG.2016.2542925.

[41] Li Z, Shahidehpour M, Alabdulwahab A, Abusorrah A. Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems. IEEE Trans. Smart Grid Sep. 2016;7(5):2260–72. https://doi.org/10.1109/TSG.2015.2456107.

[42] Azizi A, Peyghami S, Mokhtari H, Blaabjerg F. Autonomous and decentralized load sharing and energy management approach for DC microgrids. Electr. Power Syst. Res. Dec. 2019;177:106009. https://doi.org/10.1016/j.epsr.2019.106009.

[43] Naitmalek Y, Najib M, Bakhouya M, Essaaidi M. On the use of machine learning for state-of- charge forecasting in electric vehicles. In: 5th IEEE International Smart Cities Conference, ISC2 2019; Oct. 2019. p. 408–13. https://doi.org/10.1109/ISC246665.2019.9071705.

[44] Mejri MN, Ben-Othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. Apr. 2014;1(2):53–66. https://doi.org/10.1016/j.vehcom.2014.05.001.

[45] Xiaonan L, Zhiyi F, Lijun S. Securing vehicular ad hoc networks. In: 2007 2nd International Conference on Pervasive Computing and Applications, ICPCA'07; 2007. p. 424–9. https://doi.org/10.1109/ICPCA.2007.4365481.

[46] Khan SK, Shiwakoti N, Stasinopoulos P, Chen Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accid. Anal. Prev. Dec. 2020;148:105837. https://doi.org/10.1016/j.aap.2020.105837.

[47] *The Basics of Information Security*. Elsevier, 2014.

[48] *Eleventh Hour CISSP*. Elsevier, 2014.

[49] "Article: What is... Denial-of-Service (DoS) | F-Secure." .

[50] Dong C, Li X, Jiang W, Mu Y, Zhao J, Jia H. Cyber-physical modelling operator and multimodal vibration in the integrated local vehicle-grid electrical system. Appl. Energy Mar. 2021;286:116432. https://doi.org/10.1016/j.apenergy.2021.116432.

[51] *Machine-to-machine (M2M) Communications*. Elsevier, 2015.

[52] Wang L, Liang DH, Crossland AF, Taylor PC, Jones D, Wade NS. Coordination of multiple energy storage units in a low-voltage distribution network. IEEE Trans. Smart Grid 2015;6(6):2906–18.

[53] Mokhtari G, Nourbakhsh G, Ghosh A. Smart coordination of energy storage units (esus) for voltage and loading management in distribution networks. IEEE Trans. Power Syst. 2013;28(4):4812–20.

[54] McNeil P. Secure IoT deployment in the cement industry. In: 2017 IEEE-IAS/PCA Cement Industry Technical Conference; 2017. p. 1–12.

[55] Liu H, Ning H, Zhang Y, Xiong Q, Yang LT. Role-dependent privacy preservation for secure v2g networks in the smart grid. IEEE Trans. Inf. Forensics Secur. Feb. 2014;9(2):208–20. https://doi.org/10.1109/TIFS.2013.2295032.

[56] "WiFi Security: WEP, WPA, WPA2 And Their Differences." https://www.netspotapp.com/wifi-encryption-and-security.html (accessed Mar. 17, 2021).

[57] "What Is Symmetric Key Cryptography? | Binance Academy." https://academy.binance.com/en/articles/what-is-symmetric-key-cryptography (accessed Mar. 17, 2021).

[58] Makhdoom I, Abolhasan M, Abbas H, Ni W. Blockchain's adoption in IoT: the challenges, and a way forward. J. Netw. Comput. Appl. 2019;125:251–79. https://doi.org/10.1016/j.jnca.2018.10.019.

[59] Ajao LA, Agajo J, Adedokun EA, Karngong L. Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry. J Aug. 2019;2(3):300–25. https://doi.org/10.3390/j2030021.

[60] R. Bobba, K. Davis, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting False Data Injection Attacks on DC State Estimation," 2010.

[61] Aoufi S, Derhab A, Guerroumi M. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. J. Inf. Secur. Appl. 2020;54:102518. https://doi.org/10.1016/j.jisa.2020.102518.

[62] Lipu MSH, et al. Data-driven state of charge estimation of lithium-ion batteries: Algorithms, implementation factors, limitations and future trends. J. Clean. Prod. 2020:124110. https://doi.org/10.1016/j.jclepro.2020.124110.

[63] M. Scalas and G. Giacinto, "On the role of explainable machine learning for secure smart vehicles," Nov. 2020, doi: 10.23919/aeitautomotive50086.2020.9307431.

[64] M. Szczepanski, M. Choras, M. Pawlicki, and R. Kozik, "Achieving explainability of intrusion detection system by hybrid oracle-explainer approach," Jul. 2020, doi: 10.1109/IJCNN48605.2020.9207199.

[65] "8 Explainable AI Frameworks Driving A New Paradigm For Transparency." https://analyticsindiamag.com/8-explainable-ai-frameworks-driving-a-new-paradigm-for-transparency-in-ai/ (accessed Mar. 19, 2021).

[66] Guan Y, Ge X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. IEEE Trans. Signal Inf. Process. Over Networks Mar. 2018;4(1):48–59. https://doi.org/10.1109/TSIPN.2017.2749959.

[67] Zhu M, Martínez S. On distributed constrained formation control in operator-vehicle adversarial networks. Automatica Dec. 2013;49(12):3571–82. https://doi.org/10.1016/j.automatica.2013.09.031.

[68] Pasqualetti F, Carli R, Bullo F. A distributed method for state estimation and false data detection in power networks. In: 2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011; 2011. p. 469–74. https://doi.org/10.1109/SmartGridComm.2011.6102368.

[69] Mashlakov A, Honkapuro S, Tikka V, Kaarna A, Lensu L. Multi-timescale forecasting of battery energy storage state-of-charge under frequency containment reserve for normal operation. In: International Conference on the European Energy Market, EEM. 2019-September; Sep. 2019. https://doi.org/10.1109/EEM.2019.8916335.

[70] Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. J. Inf. Secur. Appl. Feb. 2020;50:102419. https://doi.org/10.1016/j.jisa.2019.102419.

[71] Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. Futur. Gener. Comput. Syst. May 2018;82:761–8. https://doi.org/10.1016/j.future.2017.08.043.

[72] B. Yang, L. Guo, and J. Ye, "Real-time simulation of electric vehicle powertrain: hardware-in-the-loop (HIL) testbed for cyber-physical security," Aug. 2020, pp. 63–68, doi: 10.1109/itec48692.2020.9161525.

[73] Gahrooei YR, Khodabakhshian A, Hooshmand R. A new pseudo load profile determination approach in low voltage distribution networks. IEEE Trans. Power Syst. 2018;33(1):463–72.

[74] Gerbec D, Gasperic S, Smon I, Gubina F. Allocation of the load profiles to consumers using probabilistic neural networks. IEEE Trans. Power Syst. 2005;20(2):548–55.

[75] Niyato D, Hoang DT, Wang P, Han Z. Cyber Insurance for Plug-In Electric Vehicle Charging in Vehicle-To-Grid Systems. IEEE Netw Mar. 2017;31(2):38–46. https://doi.org/10.1109/MNET.2017.1600321NM.

[76] Manitsas E, Singh R, Pal BC, Strbac G. Distribution system state estimation using an artificial neural network approach for pseudo measurement modeling. IEEE Trans. Power Syst. 2012;27(4):1888–96.

[77] Wu J, He Y, Jenkins N. A robust state estimator for medium voltage distribution networks. IEEE Trans. Power Syst. 2013;28(2):1008–16.

[78] Dehghanpour K, Wang Z, Wang J, Yuan Y, Bu F. A survey on state estimation techniques and challenges in smart distribution systems. IEEE Trans. Smart Grid 2019;10(2):2312–22.

[79] Diao W, Naqvi IH, Pecht M. Early detection of anomalous degradation behavior in lithium-ion batteries. J. Energy Storage 2020;32:101710. https://doi.org/10.1016/j.est.2020.101710.