Cyber-attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review

Sriranga Suprabhath Koduru , Venkata siva Prasad Machina , Sreedhar Madichetty *

Posted Date: 21 April 2023

doi: 10.20944/preprints202304.0691.v1

Keywords: Cyber physical systems ; Cyber attacks ; Artificial Intelligence ; Machine learning ; Deep learning

Article

Cyber-Attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review

Sriranga Suprabhath Koduru, Venkata siva Prasad Machina and Sreedhar Madichetty *

Department of Electrical and Computer Engineering, Ecole Centrale School of Engineering, Mahindra University, India

* Correspondence: sreedhar.803@gmail.com;

Abstract: Importance and need for cyber security have increased in folds since a decade. Indirectly, the country's security depends on the country's cyber-physical systems. Attackers are becoming more innovative, and attacks are becoming undetectable, causing huge risks to the systems. In this scenario, intelligent and evolving detection methods should be introduced to replace the basic and outworn ones. This article discusses about new-age intelligence and smart techniques dealing with artificial intelligence (AI) models. Artificial intelligence for cyber security is reviewed, and the performance of machine learning models (ML) and deep learning (DL) models are analysed. A real-time case study of stealthy local covert attacks with false data injection attacks is implemented on the DC-DC converter. A deep learning model is designed to mitigate cyber attacks, and its performance is evaluated.

Keywords: cyber physical systems; cyber attacks; artificial Intelligence; machine learning; deep learning

1. Introduction

Microgrid, the new age power grid architecture, is gaining more attention from researchers and industry. The possibility of integrating renewable generations, electric vehicles, energy storage and distributed energy resources into the power grid and coupling them with effective communication links will improve the efficiency of the power grid [1]. Also, the microgrids are capable of powering the localized loads by operating in isolated mode [2].

With the aim of reducing carbon emissions, renewable energy generation is encouraged in the power sector, and the transportation sector is moving towards the electrification of vehicles. To achieve the sustainable development goals, by 2030, it is targeted to integrate $8000GW$ of renewables compared to $2800GW$ at present. By 2025 at least 100 countries should be targeting 100% working with renewable generation. At present Norway stands first in renewable power integration with 99%, Newzealand (81%) , Brazil (79%), Colombia (74%), Canada (68%), Sweden (67%), Portugal (65.5%) and saudi arabia with least integration of (0.1%).

The renewable energy share globally increased from 26.30% to 28.1%from 2020 to 2021. It is observed that 17% of the global CO_2 emissions are due to the transport sector; the global EV market is receiving huge support, which leads to over 16.5 million EVs on the road. By 2030, 2% of the global electrical demand is expected to be due to EVs. Therefore microgrid is the best alternative for the conventional grid in terms of grid integration with RES and EVs [3], the variety of sources and loads that can be integrated into a microgrid is shown in Figure 1.

With a variety of intermittent distributed energy resources, the information of load availability and demand on the grid should be continuously monitored and communicated to the controller for effective operation and control. The communication network is established based on the OSI model, TCP/IP model, EAP protocol and microgrid communication [4,5]. Figure 2 denotes the different protocol structures. The development of IoT devices and architectures makes it viable to utilise the services of smart meters, smart health, smart transport and smart grid [6]. IoT architecture is preferred on the demand side, whereas the EPA model is implemented on the supply side.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

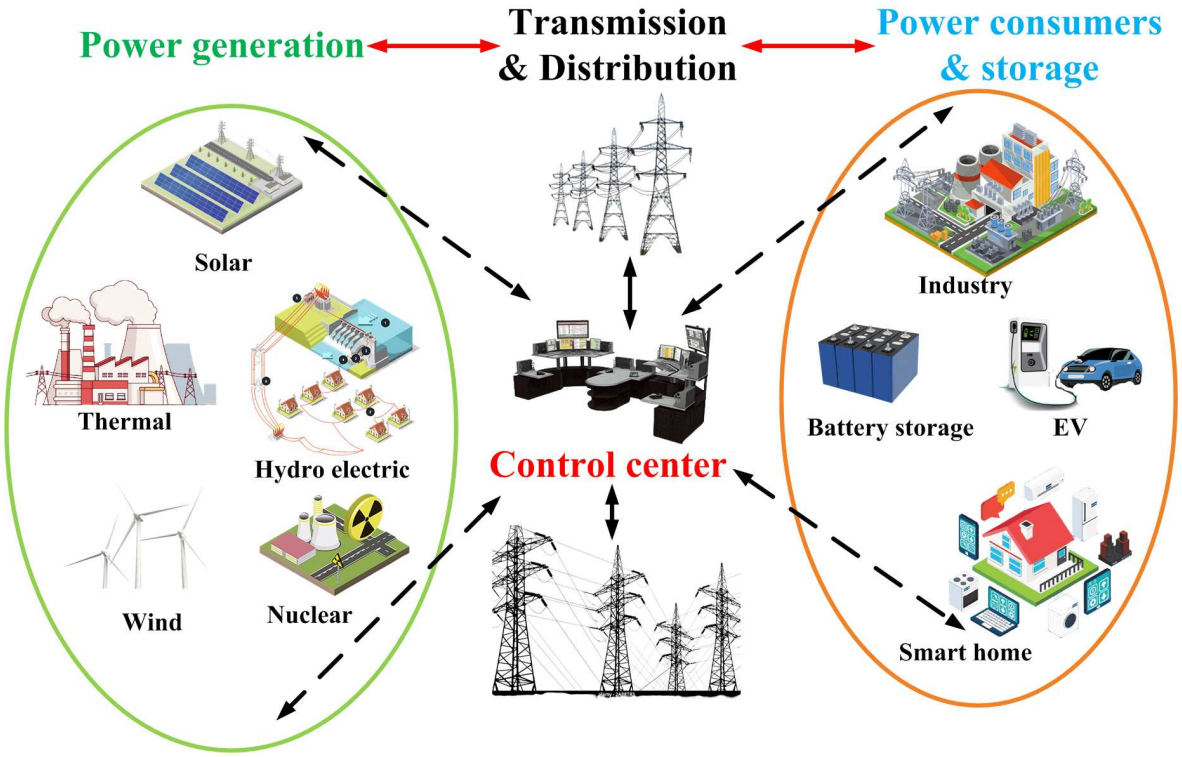

Figure 1. Overview of microgrid .

The battlegrounds between the countries have constantly been shifting. Intruding their cyberspace and attacking the communication channels of the enemy, thereby interrupting their information transfer, is the war strategy followed in the near future. This kind of war strategy is termed cyber warfare [7], and even the strongest and most developed countries are vulnerable to this strategy.

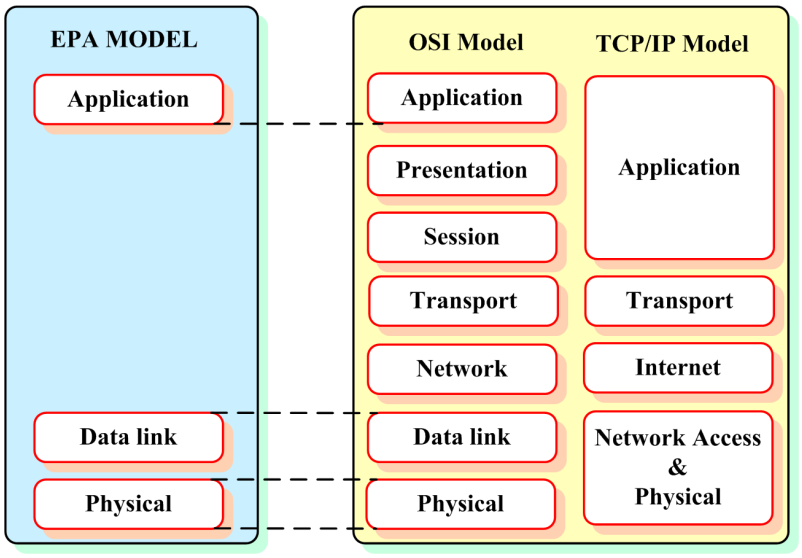

Figure 2. Communication models for microgrid communication .

To overcome this, countries are focusing on building cyber security and creating cyber awareness [8–10]. According to the crunch base cyber security report [11], over a decade, there has been an almost 700% increase towards cyber security funding. USA holds the king share of 76% in global cyber security funding and Israel and the UK stand next with 13% and 3%, all the other countries accounting

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

for 8%. There are seven different types of attacks as shown in Figure 3 where an attacker can create havoc in the country.

Espionage is a form of gentle cyber attack, where an attacking country tries to monitor and steal sensitive information by phishing attacks or botnets [12]. Sabotage attacks or cyber sabotage deliberately destroy critical infrastructure by introducing a malfunction into the system [13]. These attacks are frequently observed, introducing a software update bug. Flooding the communication channel with multiple requests causing the channel to be irresponsive to legitimate users, is defined as a denial of service attack [14]. This attack is dangerous and causes communication delays or interruptions, affecting military bodies and research bodies. Cyber attack on power grids is the most dangerous and impactful phenomenon. It can cause interruption information sharing, cause disruption in critical services and cause huge economic losses [15].

Propaganda attacks are largely used to influence the audience and their perspective by spreading false news that makes people lose faith and create agitations in the country; these kinds of attacks look simple but effective [16]. Economic disruption attacks target the economic pillars of the country; these attacks try to take down the financial systems like the stock market and the banking sector by stealing money or blocking people to access the funds available [17]. Surprise attacks are performed to create a massive impact in less time, weakening the country's defence systems.

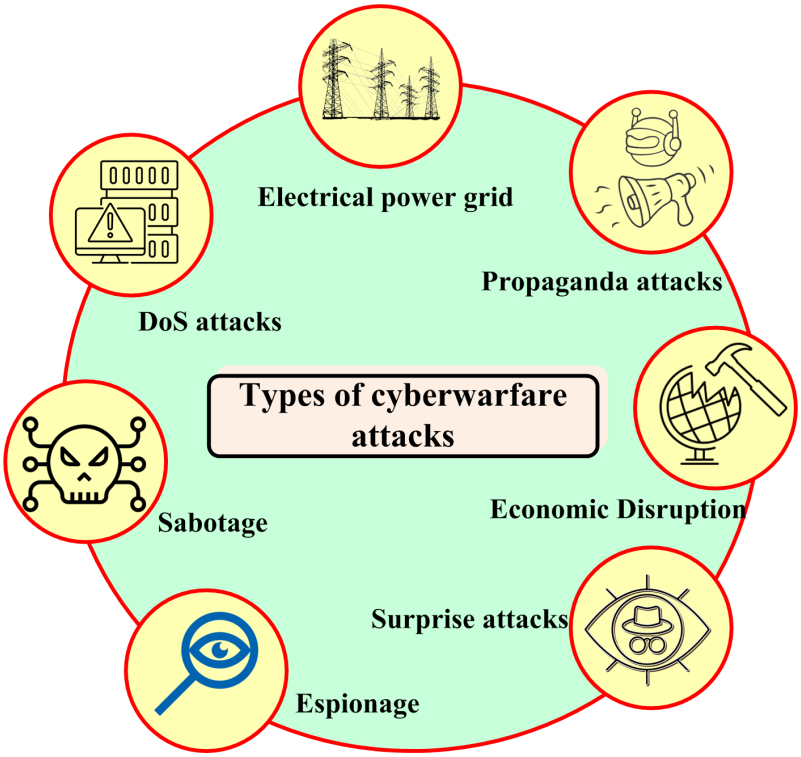

Figure 3. Different attack methodologies used for cyber warfare.

2. Real-world cyber attack scenarios

The most notable and successful cyber-attack was the 2010 Iran nuclear plant attack; this attack targeted the PLCs in the nuclear plant. Stuxnet virus introduced for this attack has its impact on 2,00,000 computers and nearly caused damage to 1000 machines [18]. 2012 Aramco cyber-attack uses shamoon virus; this attack is intended to delete some confidential files in the Aramco workstations. 30,000 Saudi Aramco workstations are affected by this attack [19].

The best examples of cyber warfare are the attacks that took place in the context of the Russia-Ukraine war. These cyber-attacks have made the world realise the importance of cyber security. 2015 cyber-attack on Ukraine's power grid has caused a blackout and led to a power outage for 2,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

30,000 people [20]. The attack group known as Sandworm used black energy 3 malware to compromise the information systems of energy distribution companies [21]. Spear phishing [22] method is used to implement the attack. Followed by the 2015 attack, in less than a year, one more attack was targeted by Russia towards Ukraine's capital Kyiv. Industroyer malware [23] used this attack maloperate the protective relays, where the data packets of the relays are diverted to the wrong IP address. This attack caused a blackout for 1 hr.

One of the biggest cyber-attacks on oil resources took place in the US on 7 May 2021. This ransomware cyber-attack has halted the working of oil pipelines in nearly 17 states of the USA. Darkside malware is used in this attack [24]. A similar attack happened in Iran in 2021, where 4300 gas stations could not process the payment. The 2021 Natanz cyber-attack is one more example of cyber warfare, where it is speculated that Israel is responsible for the attack on nuclear power plant as a part of the Iran and Israel war [25].

These cyber-attacks on the cyber-physical systems are implemented by accessing the information from the communication links. Depending on the protocol used for communication, there are possible different attacks that are shown in Figure 4

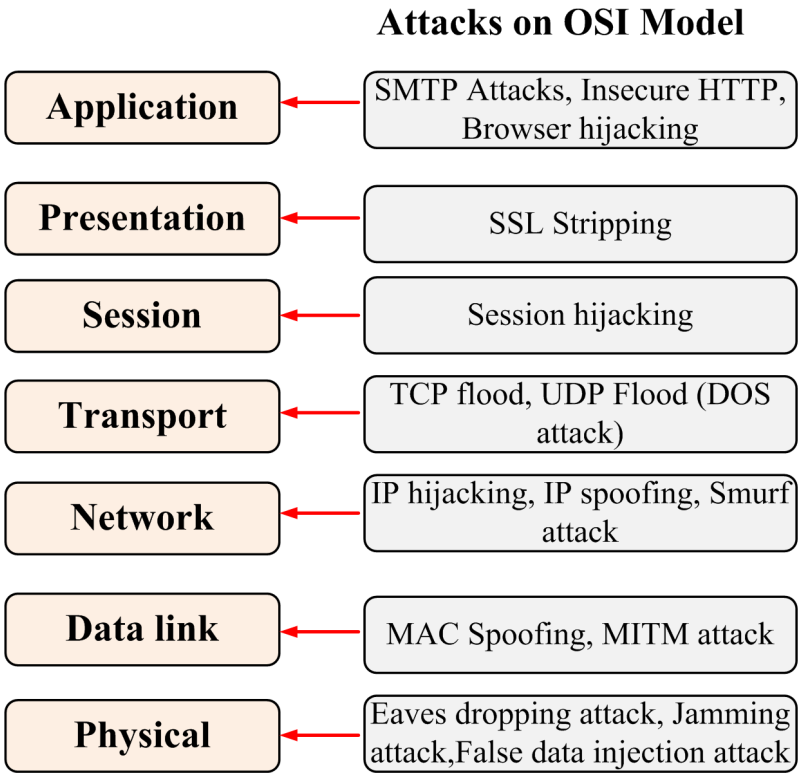

Figure 4. Cyber attacks in different layers of OSI model.

3. DC microgrid control and architecture

DC microgrid, an example of a cyber-physical system, is considered to examine the communication in CPS and the possibility of cyber-attacks in communication links. Figure 5 shows the control architecture of the distributed control DC microgrid [26,27]. This architecture consists of three nodes, which communicate with neighbouring nodes. There are two control layers: the primary control layer and the secondary control layer. The sensor value information from the neighbouring converters is transferred to the particular converter through the secondary control layer. The received information is processed and passed through the control algorithm, and the control outputs are sent to the plant; the control outputs are sent to the plant through the primary layer communication [28]. The secondary and primary layers, which carry critical sensor information, are prone to cyber-attacks. The

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

attack on the communication layers leads to the disruption in the control technique and causes the maloperation of the DC microgrid.

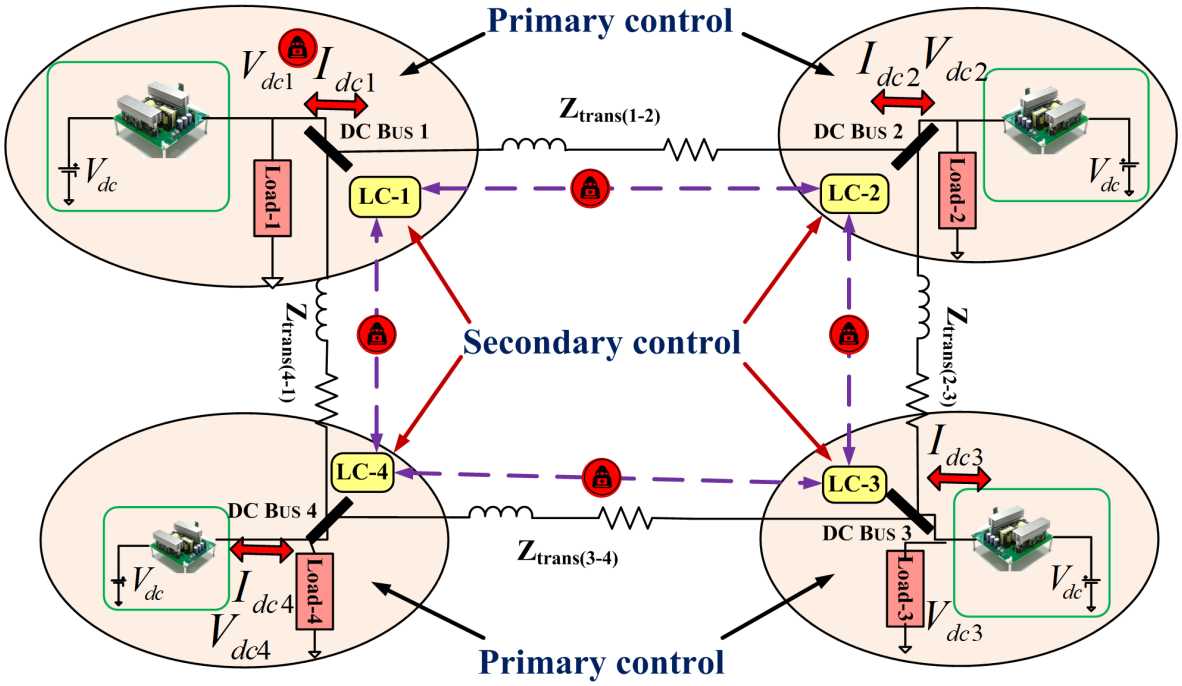

Figure 5. Control architecture of distributed DC microgrid.

There are various cyber-attacks targeted towards CPS, the most prominent, frequent and effective cyber-attacks preferred by the attackers are false data injection (FDI) attacks, Man in the middle (MITM) attacks and Denial of service (DoS) attacks.

3.1. False data injection attacks

The primary aim of false data injection attacks is to modify the sensor values transmitted through the communication links [29]. FDI attacks increase the computational burden on the controllers, cause revenue losses, mismanagement of control devices, and lead to load dysfunction and power imbalance. Adversary targets the vulnerabilities in the communication links and injects false data into the existing sensor values using different injection techniques. Structured query language (SQL) injection and cross-site scripting attacks are the most common and popular. In SQL injection attacks, the attacker tries to inject the commands that exploit the authenticity and authorization of the application [30]. The attacker can read, modify and delete the data using this injection technique. Cross-site scripting technique inserts malicious code into the web application; this attack tries to manage the cookies, hijack the sessions and change the user settings [31]. Some other types of injection techniques are code injection, command injection and CCS injection. Figure 6 represents the FDI attack on the sensor values.

Depending upon the knowledge and accessibility of the attacker, FDI attacks are further classified into two types, internal FDI attacks and external FDI attacks. If the attacker possesses complete knowledge of the system and has access to the critical infrastructure, the FDI attack in this scenario is considered an internal FDI attack. Internal FDI attacks are considered as most effective and dangerous attacks. As the attacker is aware of the system working, FDI attacks designed are more constructive and stealthy, which makes it difficult to identify. External FDI attacks are performed by the external agent who has mere knowledge of the system working; in this scenario, the attacker completely depends on the vulnerabilities in the communication network.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

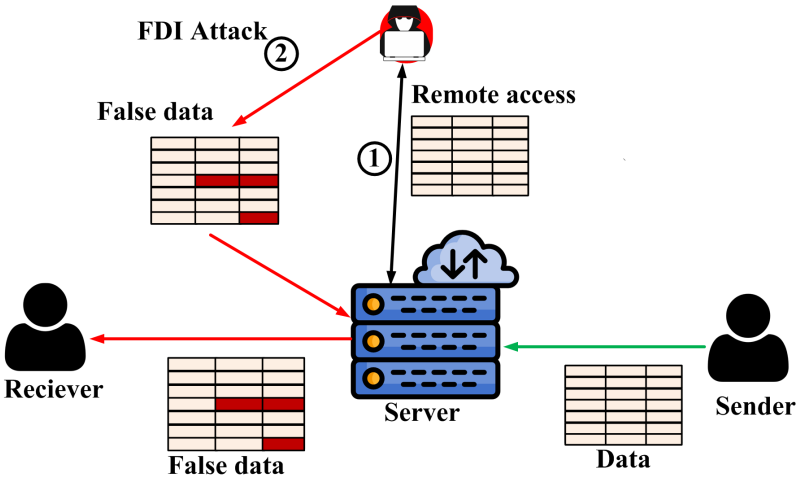

Figure 6. False data injection attack representation.

3.2. Man in the middle attack

In man in a middle attack, the attacker tries to steal the information between two parties that should be secure and private. A man-in-the-middle attack has two steps, step 1 is intruding into the communication channel or intercepting the data traffic, and step 2 is decrypting the information that is transmitted through the channel [32] as shown in Figure 7. The motive for a MITM attack can be anything, such as stealing the authorized parties' identity, modifying the parties' login credentials, taking control of financial transactions, etc.

There are certain methods through which attacker tries to intrude into the network. IP spoofing [33], ARP spoofing [34] and DNS spoofing [35]. In IP spoofing, the attacker who stands in the middle of the communication between the authorized parties, the attacker spoofs the IP address of the sender and receiver. For the sender, the attacker spoofs the IP address of the receiver, and he appears as the receiver to the sender and vice versa, making the operation look legitimate. ARP is the address resolution protocol used to map the device's IP address into the MAC address.

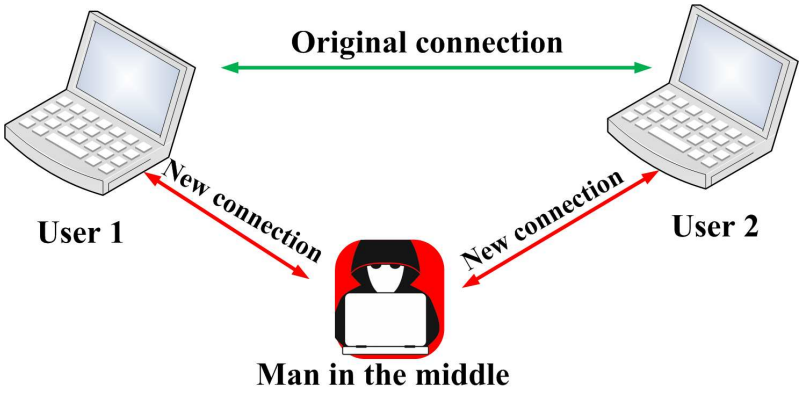

Figure 7. Man in the middle attack representation.

When an ARP request is sent by one device, an ARP response is obtained by the device matching the request, these responses and requests are formed as an ARP cache. When the attacker gets access to the ARP cache, the attacker tries to match his MAC address with the device's IP address in the network. This makes the attacker to access the data transfer between the parties. DNS spoofing is the type of attack technique in which the user is directed to the fake account intended by the attacker; this happens due to the altered domain names in the server. When the user tries to enter confidential information such as login credentials, the information gets stolen by the attacker.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

After intruding into the network by using any of the methods mentioned above, the attacker should find a way to decrypt the messages transmitted between the parties. HTTPS spoofing, SSL hijacking, SSL stripping and SSL beast are the methods often used to decrypt the messages [36].

3.3. Denial of service attack

A denial of service attack aims to make the service unavailable to the authorized user by flooding the server with false requests [37,38]. This attack causes disruption in the availability factor in the CIA triad. CIA stands for confidentiality, integrity and availability; these are the guidelines and policies followed to ensure information security. Disruption in any one of the factors indicates a cyber-attack on the system. However Dos attack doesn't cause a breach of confidentiality or integrity, but it causes a loss of time and computational resources. Attackers often aim DoS to halt the system's performance and cause financial losses. Sometimes this attack is also performed to expose the vulnerability of the system. DoS attack is pictorially represented in Figure 8, where an attacker gains access to multiple devices and floods the server with requests.

DoS attack is distinguished based on the point of attack in the communication system. If the attack targets a specific application, it is defined as an application layer attack. In this attack, the application is flooded with multiple HTTP requests; this attack is measured in requests per second (RPS). If a DoS attack is performed by exploiting the vulnerabilities in communication protocols, it is defined as a network layer attack; this attack disrupts the entire network and is measured in bits per second (BPS). Finally, the most common form of DoS attack is the volumetric attack, which targets the bandwidth of the communication channel. The bandwidth of the communication channel is flooded, creating congestion in network traffic; this attack is measured in BPS. Different techniques for implementing DoS attacks are SYN scan, smurf attack, teardrop attack, ARP attack and Fraggle attack. Another variant of the DoS attack is the distributed denial of service (DDoS) attack [39]. In this attack, a group of devices are used to attack the network, whereas in the DoS attack attacker uses a single device.

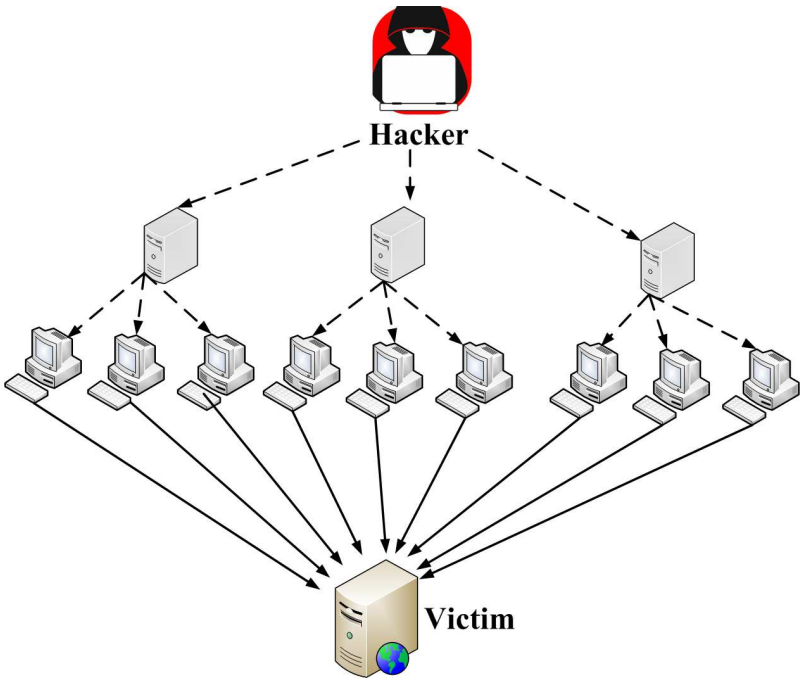

Figure 8. Denial of Service attack representation.

4. Defense mechanisms

To address cyber-attacks, every organisation or system follows some basic security measures. User authentications, Firewall [40], Anti-virus, data encryption and Cryptography are the basic

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

security measure implemented, but these security systems are not strong enough to address the present cyber-attacks that are rapidly evolving and innovative. Intrusion detection systems (IDS) and Intrusion prevention systems are used in addition to the basic security measures. IDS monitors the information flow in the network continuously and detects the attack packets [41,42]. IDS is classified into network intrusion detection system (NIDS) and host intrusion detection system (HIDS). NIDS is a software-defined system it monitors, captures and analyses network traffic. It detects malicious data packets by comparing them with the already known attack patterns. But the operation of NIDS is very difficult in busy and complex networks. HIDS is a host-based system installed on individual devices; it monitors the information received on the particular device and generates alerts for any malicious packets found. Depending on the operation, IDS is classified into signature-based IDS [43], and anomaly-based IDS [44].

Signature-based IDS works on detecting the patterns in the data packets. Signature IDS searches the database for attack patterns; if there is any similarity with the attack patterns, it sends an alert. The drawback of the system is it detects only known attack patterns, and there is a possibility of false negatives for new and unknown attacks. Anomaly-based IDS monitors the deviation from the normal, and a confidence interval creates a boundary that it marks as an anomaly. The disadvantage of this method is the high possibility of false positives for policy changes and new authentic intrusions. Hybrid IDS is introduced to overcome the disadvantage of the signature and anomaly-based IDS, which uses both techniques. Signature-based IDS detects known attacks, and anomaly-based IDS detects unknown attacks. Intrusion prevention system (IPS) is the extension of IDS, which not only detects intrusions but is also capable of blocking malicious data from entering the network [45].

4.1. Artificial intelligence for cyber security

AI's broad scope and capabilities made it possible to penetrate various fields. Cyber security is also enhanced with the application of AI into it [46]. There are different levels of algorithms applied in cyber security, and with the increase in complexities of real-world systems, AI has also evolved.

Initially, basic machine learning algorithms, also called shallow models, are used for cyber security, later deep learning techniques are introduced that are capable of dealing with complex networks, and further reinforcement learning methods are proposed that are futuristic and claimed to be self-learning methods. Figure 9 gives the classification of various ML models used for cyber security.

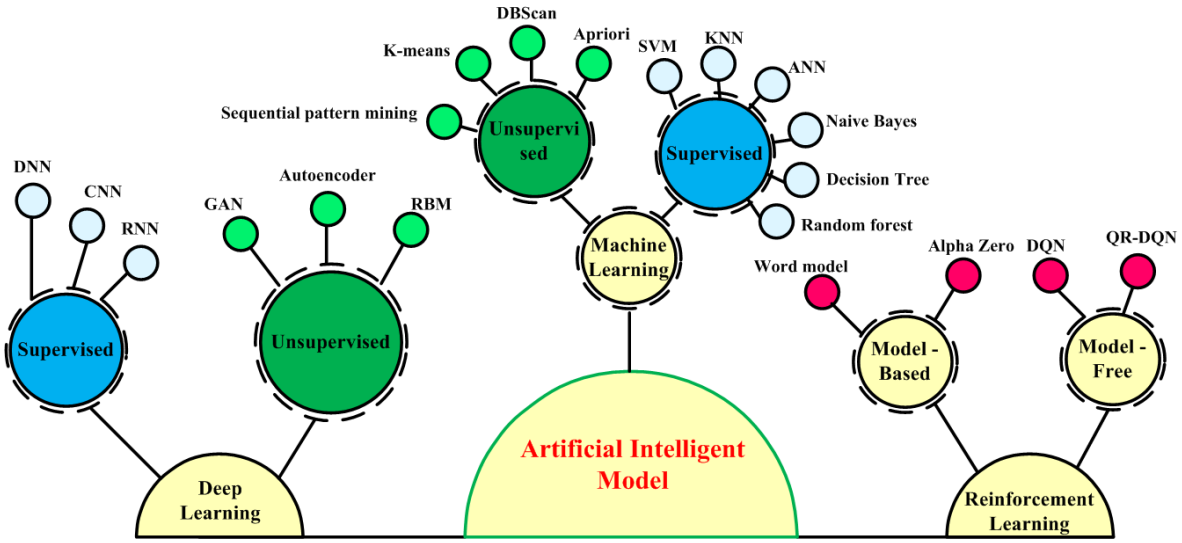

Figure 9. Taxonomy of artificial intelligence models for cyber security

Machine learning models, referred to as shallow models, are further classified into supervised learning and unsupervised learning based on their learning procedure. In unsupervised learning, the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

classified outputs are formed into clusters; these algorithms mostly depend on the internal pattern of the data. The k-means algorithm is used to detect malicious entries into the network [47]; the k-means algorithm groups the unlabelled data into clusters. The value of K indicates the no.of clusters. This technique divides the data into different groups, which gives insights for data analysis about unknown and known attack patterns. Sequential pattern mining [48], a subset of data mining, is also a data analytic method that gives the knowledge of the attack patterns; this method will send an alert if any malicious activity or abnormal activity is registered. Another data mining method used to detect web intrusion is the apriori algorithm [49]; the apriori method that runs on the specific rule set will keep track of frequently occurring data patterns and indicate if any new pattern is detected.

Supervised learning methods are already specified with the class labels to verify model classification or predictions. The k-nearest neighbours (KNN) method is used to classify the incoming entry as normal or malicious entry [50]. Naïve Bayes is a statistical method that uses a probabilistic method based on the Bayesian theory; the probability of a field prone to attack can be calculated [51]. Support vector machine (SVM) is a classification method that separates the intrusions and normal entries from the dataset. SVM uses a kernel that facilitates the classification of even complex and nonlinear data; SVMs can transform the data into the next dimension if the decision boundary cannot be determined in this dimension [52]. Decision trees and random forests are tree-based classifiers [53]. Based on the training data, a tree-like structure is created in a decision tree, predictions can be made based on the tree's structure, and any unknown entities can be sorted out [54,55]. The random forest also follows a similar method, but instead of a single tree, a large group of trees are created, and the final structure of the tree for classification is decided by voting process[56–58].

Deep learning (DL) models are designed to handle complex and non-linear systems; DL models are considered superior to ML models in system handling capability. The architecture of DL models also differs from ML models; there is no fixed algorithm for this model [59]. DL model consists of neurons placed in different layers; the working of neurons in the DL model is inspired by the working of the human brain, and neurons of each layer are interconnected. Information transmits from the input layer to the output through multiple hidden layers. DL model consists of two stages, the training state and the testing stage. The training stage consists of the modification of weights for each connection during multiple iterations; this process makes the DL model learn the patterns of the data feeding to the network.

Later the efficiency of the trained model is tested on the testing data. Deep neural networks (DNN) have the structure discussed above with multiple hidden layers, an increase in the depth of the network gives the model the ability to classify the nonlinear data [60,61]. Convolution neural networks (CNN) is widely used for image classification, the data to be classified is converted into image format, and the malicious data is identified [62,63]. Recurrent neural networks (RNN) are used for time series data; this network model predicts the occurrence of the next data sample based on the previous output and the present inputs [64]. But this model suffers from memory issues; often the outliers and extreme cases are considered as the attack vectors.

To overcome this, the models like Long-Short Term Memory (LSTM) and Gated Recurrent Unit (GRU) are introduced that contain the memory element, and the network architecture also differs from the classical RNN [65]. Generative adversarial networks (GaN) and autoencoders are unsupervised techniques in deep learning where the outputs are not specified. The GaN model consists of two networks, namely the generator and discriminator. The generator takes the input data sample and generates a sample of data; the generated sample is compared with the training data or real sample using a discriminator. Discriminator, after comparison, decides whether the incoming data sample is real or fake [66,67]. Autoencoders is a neural network architecture, and this technique often uses for video and image classification [68]. The input data is compressed to the lower dimension called as latent space; the latent space consists of data containing the most prominent features. From the latent space, the auto-encoder tries to recreate the input data at the output; by comparing the output of the autoencoder, normal and fake data are classified. During the training phase, autoencoders are trained

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

to recreate the input near the output; higher variation in the output and input indicates the attacked data.

Reinforcement learning is the advanced and futuristic architecture proposed to practice self-learning [69]. RL, also known as reward-based learning, works on the reward obtained by the action it performed in the previous iteration. The agent is present in a customized environment with predefined rules, goals and reward criteria. The model reaching the goal with high reward points is considered the optimized model; RL model continuously updates its decision-making or policy based on the rewards.

Popular real-time datasets like KDD99 and DARPA are considered to evaluate the deep learning and machine learning algorithms' performance. Initially, machine learning algorithms are implemented on the KDD99 dataset and the performance obtained is as follows naïve bayes with 97% accuracy [70], SVM with 93% accuracy [71], Decision tree with 94.3% accuracy [72], Random forest with 99% accuracy [73] and Deep belief networks with 96.5% [74]. Further, the same KDD99 dataset is classified using deep learning models, and performance is as follows, GRU with 98.64% [75], CNN-LSTM with 99.7% [76–78].

5. Case study of stealth FDI attack on DC-DC converter

From the looming threat of cyber attacks, researchers and engineers have built efficient detection and mitigation strategies to protect the CPS from attackers [79]. But the covert attack strategy implemented by attackers makes it difficult to find the presence of the attack in the system. The adversary tries to mimic the system's behaviour and tries to hide the effect of the attack reaching the controller; this makes the controller assume normal operation. These attack types demand the adversary to know the system working, making it even more difficult to detect and mitigate. This article proposes a strategy to detect and mitigate the covert attack on the DC-DC converter, the major component in the CPS, like microgrids and smart grids.

Covert attacks or stealth attacks are studied in literature based on the type of attack and their criticality. In [80], authors discussed the stealth attack and their effects on the critical infrastructure; a taxonomy is proposed to discuss the risk possessed by the stealth attack at each stage of the system. Stealthy covert attacks in cyber-physical systems are discussed in [81], where it discusses modelling different types of stealth attacks from an adversary perspective. The decoupling method and zero dynamics methods are discussed, which makes attacks completely stealthy. In [82], a steal attack methodology for a smart grid is proposed in which the attack detection probability is reduced by minimizing the Kulback Leibler (KL) divergence. The KL divergence term is reduced by obtaining a proper tradeoff between the loss of mutual information and the reduction in attack detection. An attack index is introduced in [83] to detect the stealth attack on current sensor information in distributed controlled DC Microgrid. In [84] a man-in-the-middle stealth attack is performed on battery energy storage systems with the help of an artificial neural network. Two ANNs are used, one to estimate the power of BESS and the other to estimate the state of charge of the BESS for the adversary. The above-discussed literature discusses the effective implementation of stealth attacks with various techniques, and some detection mechanisms are proposed. This article performs a false data injection-based stealth attack on the artificial intelligence-controlled DC-DC converter.

5.1. Proposed Methodology

The criticality and the level of stealthiness of the covert attacks depend on the knowledge of the adversary. If the adversary has complete knowledge and access to the system, the attack is very dangerous, but this is usually not the case. An adversary will have limited knowledge of the system and tries to attack the nodes which are more vulnerable and critical to the system, but not every node. This type of attack is referred to in the literature as local covert attacks. The impact of a local covert attack depends on the amount of stealthiness in the attack.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

The proposed DC-DC converter contains an input voltage sensor (V_{in}), an output voltage sensor (V_o), an input current sensor (I_{in}) and the output current sensor (I_o). These sensor values are fed to the controller through the communication channel. An adversary who is located in the communication layer tries to gain access to the output variables. As shown in Figure 10, the controller receives the plant input variables (V_{in}, I_{in}) and plant output variables (V_o, I_o).

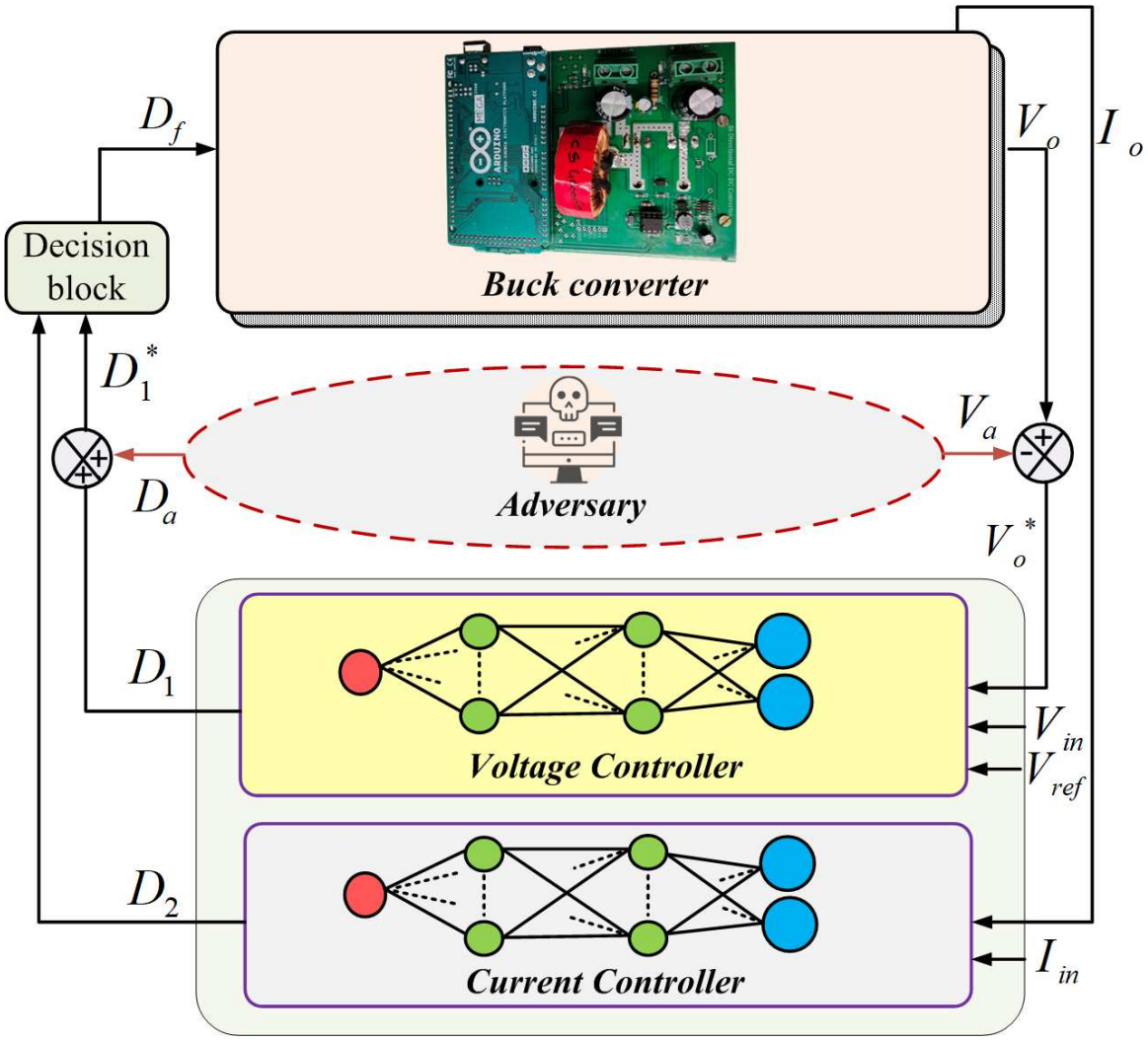

Figure 10. Proposed control mechanism for stealthy local covert FDI attack on buck converter

5.1.1. Modelling of stealth local covert FDI attack (SLCA-FDIA)

Adversary tends to inject FDI attacks on the plant output sensors and finely tune their action, so detecting the attack is difficult for the protection devices. Stealth local covert attack is modelled such that the adversary has partial writing access to the output variables and partial writing access to the control inputs. The adversary designs the plant model $B_a(s)$ that is similar to the actual plant model $B(s)$. The modified output vector and the control input vector after the SLCA are shown in (1) and (2).

$$y^*(t) = \begin{bmatrix} V_o(t) \\ I_o(t) \end{bmatrix} \rightarrow \begin{bmatrix} V_o(t) - V_a(t) \\ I_o(t) \end{bmatrix} \tag{1}$$

$$D^* = \begin{bmatrix} D_1 \\ D_2 \end{bmatrix} \rightarrow \begin{bmatrix} D_1 + D_a \\ D_2 \end{bmatrix} \tag{2}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

If there is no SLCA on the converter i.e. D_a=0 the output vector is given as (3)

$$y^*(t) = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \begin{bmatrix} D_1 \\ D_2 \end{bmatrix} \tag{3}$$

B_{11}, B_{12}, B_{21} and B_{22} are the plant transfer function matrices If there is SLCA on the converter I.e. $D_a \neq 0$ the output vector is given as (4) and (5).

$$y_s^*(t) = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \begin{bmatrix} D_1 + D_a \\ D_2 \end{bmatrix} - \begin{bmatrix} V_a(t) \\ 0 \end{bmatrix} \tag{4}$$

$$y_s^*(t) = \begin{bmatrix} y^*(t) + B_{11}D_a - V_a(t) \\ y^*(t) + B_{21}D_a \end{bmatrix} \tag{5}$$

For an attack to be completely stealthy

$$\begin{gathered} B_{21}D_a = 0 \\ and\ B_{11}D_a = V_a(t) \end{gathered} \tag{6}$$

(6) indicates that the adversary plant design should be such that the attack should not propagate to the controller.

5.1.2. Deep Learning Controller Design

An artificial neural network-based controller using deep learning is designed to control the DC-DC converter and detect and mitigate the SLCA. The proposed SLCA mitigation controller consists of two controllers a voltage controller and a current controller. Voltage Controller is the deep learning controller taking the inputs as V_{in}, V_o and V_{ref}, giving the output as duty D_1. Similarly, the current controller also consists of a deep learning controller with inputs as I_{in} and I_o, giving the output as duty D_2.

A stepwise detailed explanation of deep learning workflow is given below:

1. A set of training examples d_t is collected.
2. Design the deep learning model architecture by determining the hyperparameters such as the number of hidden layers, the number of hidden neurons in each layer and the learning rate.
3. Initialization of weights and biases.
4. Determining the training parameters of the model such as activation function, optimizer and loss function.
5. Train the model with training data.
6. Evaluate the deep learning model with testing data.
7. Deploy the trained deep learning model.

A generalised working model of the deep neural network is explained below. A set of training samples of d_t is considered. After applying the random search algorithm using the Keras tuner, the structure of the neural network with x_n input nodes and 2 hidden layers α_i^1, α_i^2 and output node $\widehat{y}$ is considered. Each hidden layer consists of 10 neurons each, and the learning rate (η) 0.1 is taken for training the deep learning model. To initialize the weights ad biases, Xavier uniform method is implemented and its mathematical representation is given in (7).

$$w_{i,j} \sim U\left[\frac{-\sqrt{6}}{\sqrt{n_{in}+n_{out}}}, \frac{\sqrt{6}}{\sqrt{n_{in}+n_{out}}}\right] \tag{7}$$

n_{in} are the no.of input connections to the neuron and n_{out} are the no.of output connections of the neuron. Root mean square, as shown in (8), is the evaluation metric considered for model training as well as evaluation.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

$$RMSE = \left[\frac{1}{2d_t}\sum_{i=1}^{d_t}|\widehat{y} - y|^2\right]^{\frac{1}{2}} \tag{8}$$

Various combinations of training parameters are applied to the deep learning model to finalize the best fit for the model. RMSE is the evaluation metric used for training parameter optimization. The sigmoid activation function with Adam optimizer run for 100 epochs gives the desirable RMSE value. The deep learning model's training process is shown below in (9)-(11).

$$\begin{gathered}\phi_1 = \omega^1 * x + \beta^1 \\ \alpha^1 = f(\phi_1)\end{gathered} \tag{9}$$

$$\begin{gathered}\phi_2 = \omega^2 * \alpha^1 + \beta^2 \\ \alpha^2 = f(\phi_2)\end{gathered} \tag{10}$$

$$\begin{gathered}\phi_3 = \omega^3 * \alpha^2 + \beta^3 \\ \alpha^3 = f(\phi_3) = \widehat{y}\end{gathered} \tag{11}$$

Here ϕ denotes the weighted sum of inputs and bias, α denotes the output of the neuron, f denotes the activation function. The training process continues until the error value converges to the performance goal specified or the model reaches the specified epochs.

In this article, it is considered that the adversary is attacking the duty D_1 obtained from the voltage controller, and to make the attack stealthy, the output voltage of the plant is modified to remove the effect of FDI attack on the control input.

5.1.3. Detection and mitigation of SLCA-FDIA

The decision block is placed before the plant, where it takes the control inputs generated from the controller. If there is no SLCA, the decision block receives D1 and D2. If there is SLCA the decision block recieves D_1^* and D_2. In the decision block, the control logic is built to detect and mitigate the FDI attack. The duty D1 is compared with D_2 with some threshold value ε, ε value accounts for small noises and errors that occurred controller. It is made sure that the ε value will not destabilize the system. (12) denotes the decision block logic.

$$D_2 - \epsilon < D_1 < D_2 + \epsilon \tag{12}$$

During no SLCA $D_1^* = D_1$ and the condition (12) satisfies if there is SLCA $D_1^* > D_1$ and the condition (12) fails. If (12) fails it indicates the attack on the voltage controller input, during this case D_2 is sent as the control input to the plant. In normal scenarios if (12) satisfies, D_1 is considered as the control input.

5.2. Simulation results

The proposed methodology for detection and mitigation of stealthy local covert FDI attacks is primarily implemented in MATLAB Simulink and further evaluated using a real-time hardware setup. DC-DC buck converter is simulated in MATLAB 2022a, and control logic is designed using a deep learning toolbox. DC-DC converter specifications are given in the Table 1

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

Table 1. Buck Converter Component Ratings

Component	Rating
Inductor L	$100\mu H$
Capacitor C	$10\mu F$
Input voltage V_{in}	$50V$
Output voltage V_o	$20V - 40V$
Voltage ripple	1% of V_o
Current ripple	15% of I_o(peak)
Load range	50W of 200W

Deep learning controller taking the plant input variables V_{in} and I_{in}, plant output variables V_o and Io as its inputs provides the output D_1 and D_2. During no attack condition, the DL controller output is shown in Figure 11 , where the input voltage is given as 50 V, and the reference voltage considered as 25 V. Output duty generated by both the voltage controller and the current controller is 0.5.

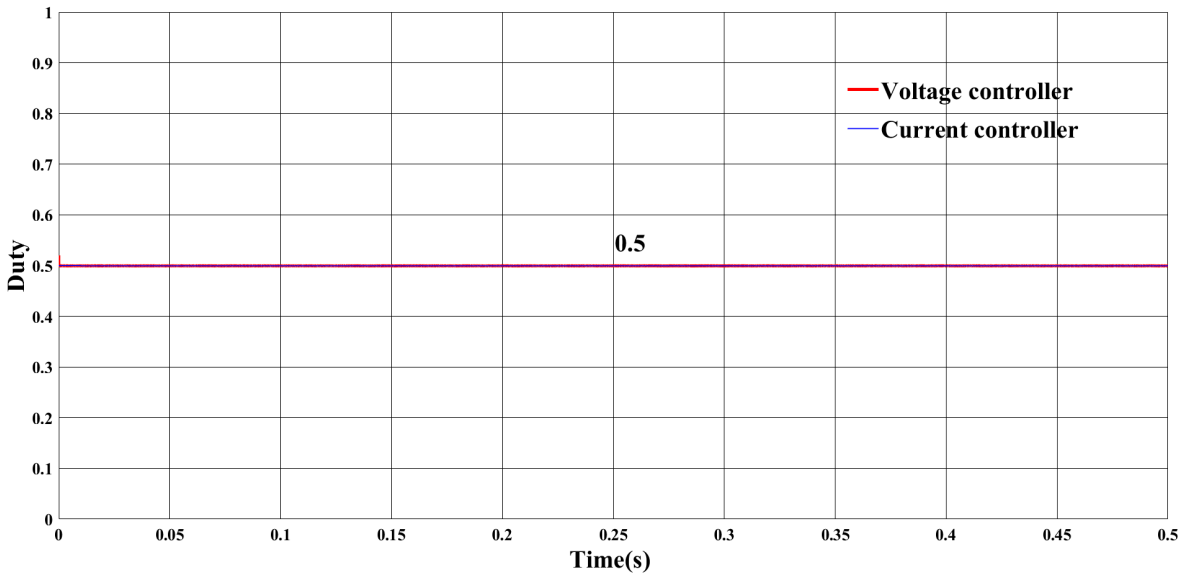

Figure 11. Deep learning controller outputs during no attack condition

An FDI attack is performed on the output of the voltage controller before reaching the decision block. False data D_a is injected into the voltage controller output D_1. Figure 12 shows the voltage controller output, and current controller output, at 0.25 s false data of 0.2 is injected. It is seen that the output of the current controller is not affected by the FDI attack on the voltage controller output; it is constant at 0.5, whereas the voltage controller output is increased to 0.7.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

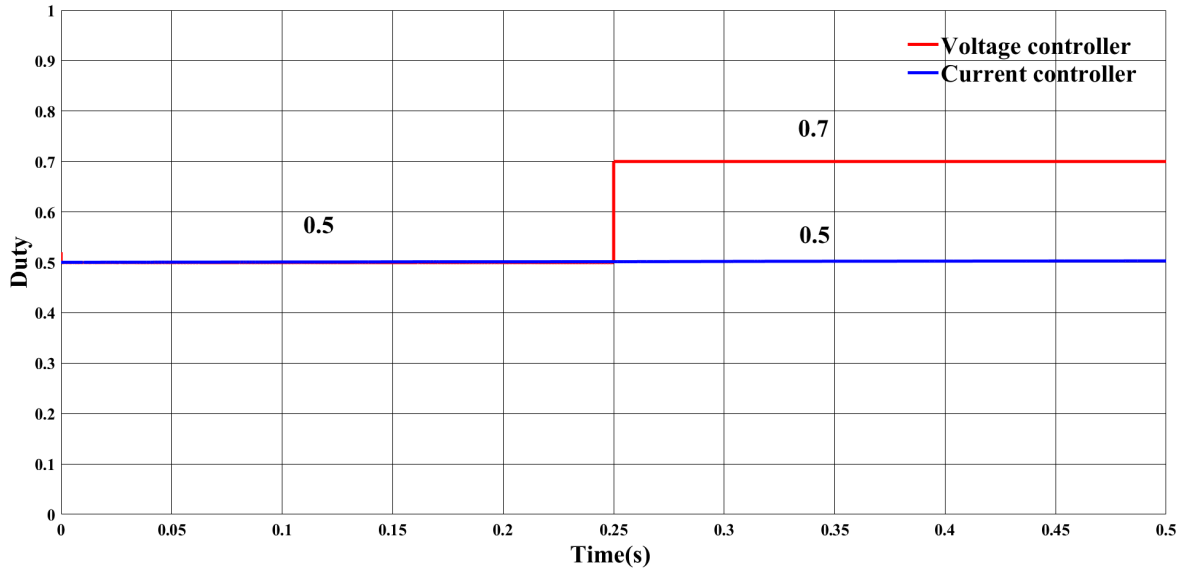

Figure 12. Deep learning controller outputs during FDI attack condition

Figure 13 shows the attack on voltage controller duty, Figure 13(a) indicates voltage controller duty, Figure 13(b) indicates the FDI attack on the duty at 0.25s. Figure 13(c) shows the final duty D_1^* sent to the decision block.

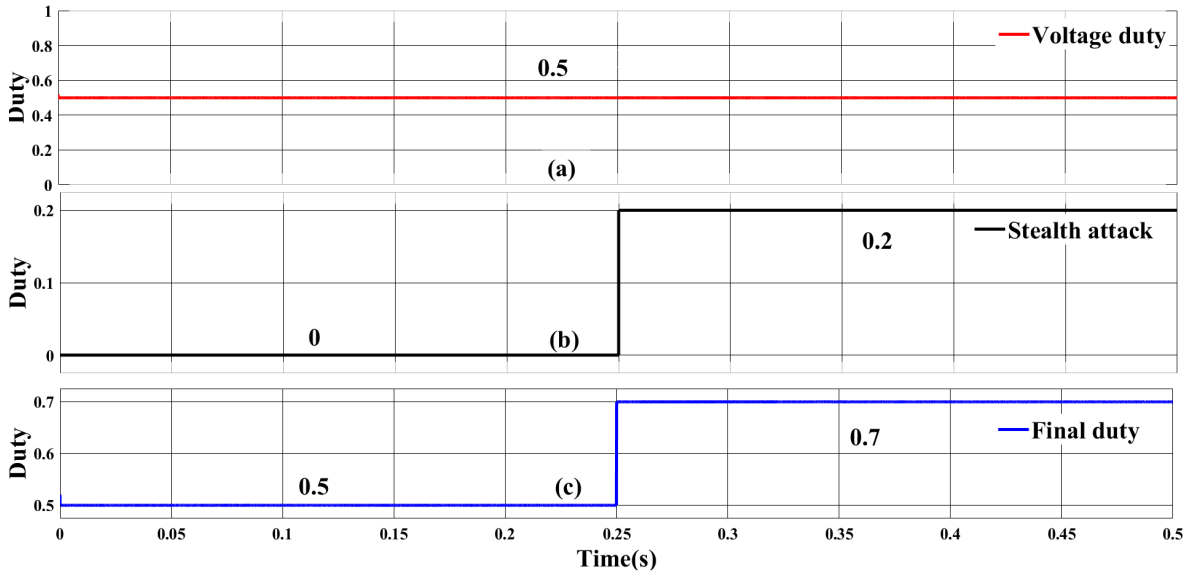

Figure 13. FDI attack on voltage controller output

After performing the FDI attack on the voltage controller output adversary tries to hide the attack by performing a stealth local covert attack and making the controller assume it is a normal operating condition. Figure 14(a) shows the output voltage of the converter at 2.5 s; when the FDI attack is made, an increase in output voltage is observed from 25 V to 35 V. To hide this attack, -10 V, a calculated value from the adversary plant model, is added to the output voltage at 2.5 s, as shown in Figure 14(b). It is observed from Figure 14(c) that the controller receives an unattacked and steady-state reference value of 25 V.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

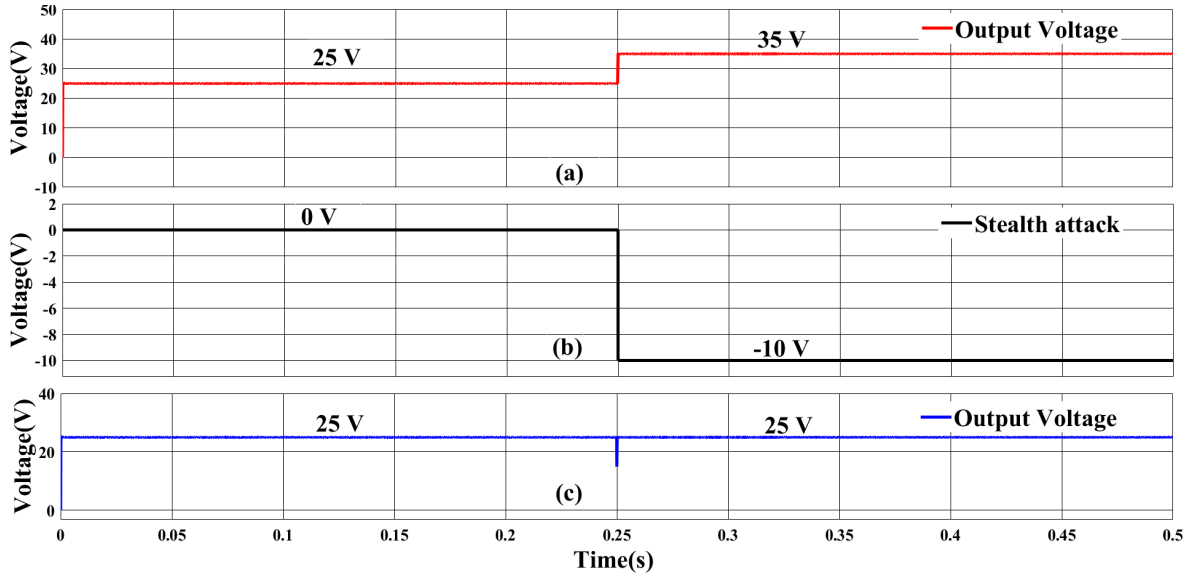

Figure 14. Stealthy local covert attack on FDI attack

To overcome the SLCA of an FDI attack, the generated control inputs are passed through the decision block. As shown in Figure 15(a), the attacked voltage controller output and current controller output are passed through the decision block. The decision block gives the output of 0.5, as shown in Figure 15(b), the final duty, which is the current controller output that corresponds to the reference voltage. The duty received from the decision block is given to the DC-DC buck converter to obtain the reference value of 25 V.

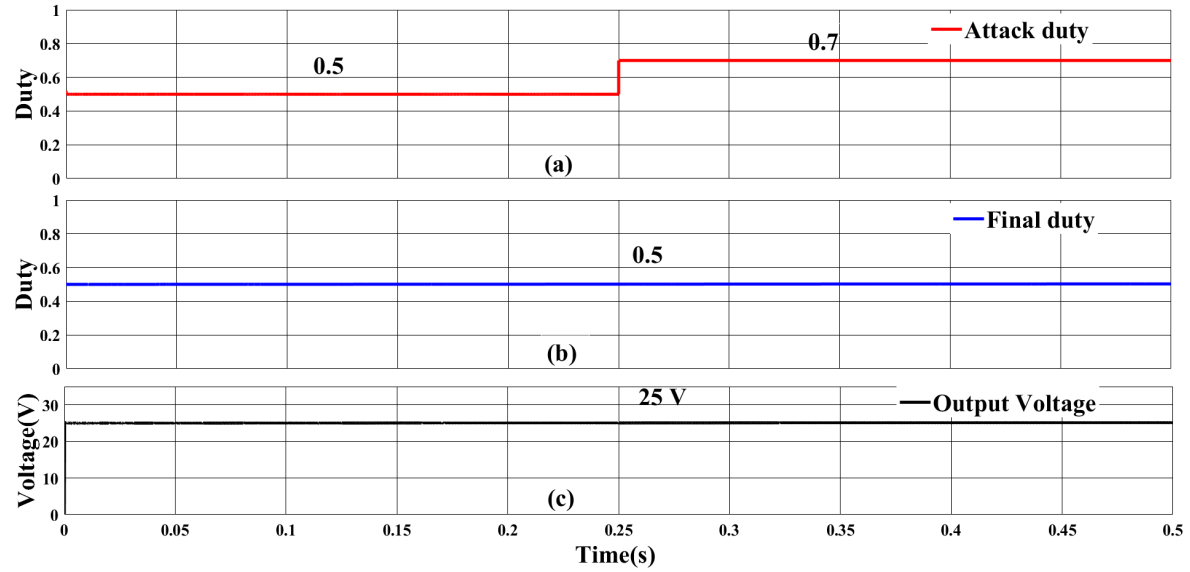

Figure 15. Overcoming stealth attack

5.2.1. FDI attack on output voltage sensor

In this case, the performance of the proposed algorithm is evaluated when there is an FDI attack on the output voltage sensor. Figure 16(a) shows the FDI attack on the output voltage sensor, where the adversary tries to manipulate the sensor data by changing the values from 25 V to 35 V at 0.22 s, 35 V to 40 V at 0.41 s, 40 V to 45 V at 0.62 s, 45 V to 35 V at 0.73 s and back to 25 V at 0.85 s. During all these sensor data manipulations, the actual output voltage of the converter remains stable at the reference value.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

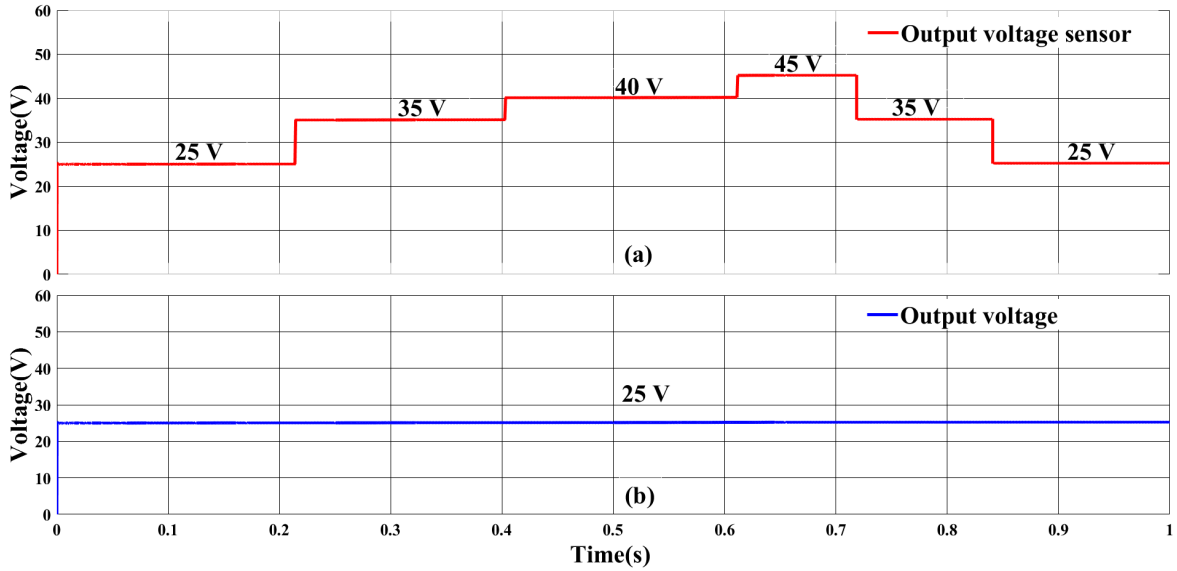

Figure 16. FDI attack on output voltage sensor

5.2.2. *FDI attack on input voltage sensor*

FDI attack is performed on the input voltage sensor by injecting the false data into the sensor values. Input voltage is changed from 50 V to 65 V at 0.35s and back to 50 V at 0.7s as shown in Figure 17(a). The designed control scheme efficiently mitigates the attack and maintains the output voltage constant at a reference value of 25 V as shown in Figure 17(b).

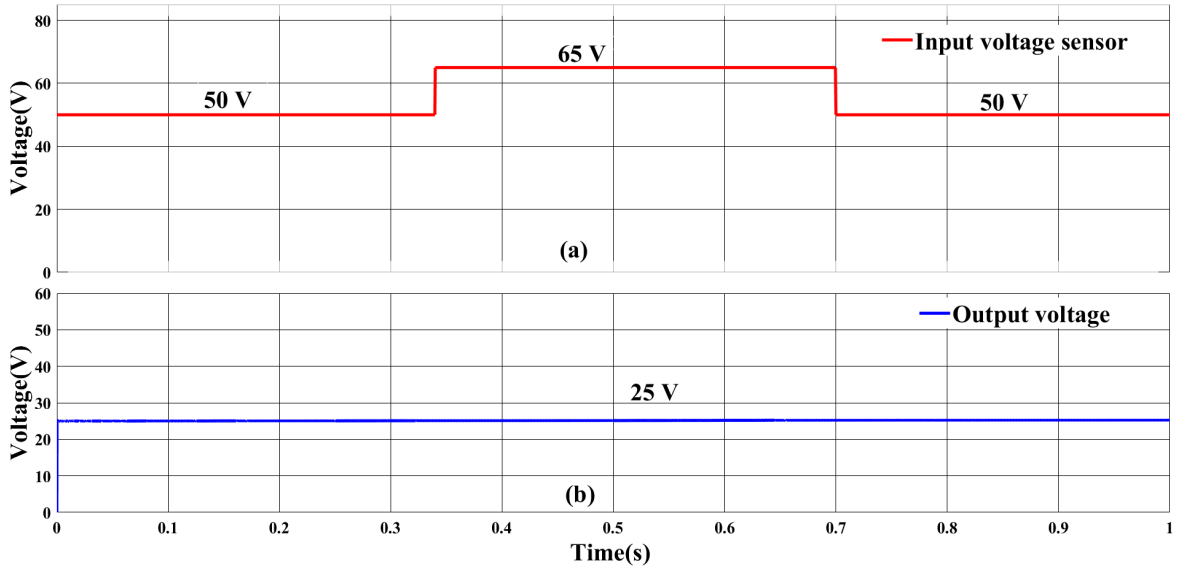

Figure 17. FDI attack on input voltage sensor

5.2.3. *FDI attack on input voltage sensor and Stealth attack*

In this case, a complex scenario, where the adversary tries to perform a stealth FDI attack on the voltage controller output and an FDI attack on the input voltage sensor is considered. The robustness of the designed control mechanism is verified by implementing both attacks simultaneously. From Figure 18(a) it is observed that the D_1 is manipulated by injecting false data and changing the value from 0.5 to 0.39 at 0.35 s, 0.39 to 0.6 at 0.5 s and finally settling to 0.7 at 0.7 s. At the same time, the input voltage sensor data is also falsified by changing the value from 50 V to 65 V at 0.35 s and back to 50 V at 0.7 s as shown in Figure 18(b). Figure 18(c) shows the output voltage of the converter which

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

remains unchanged and maintained at a reference level of 25 V. This shows that the designed control scheme is effectively designed to handle multiple attacks with a wide range of false data values.

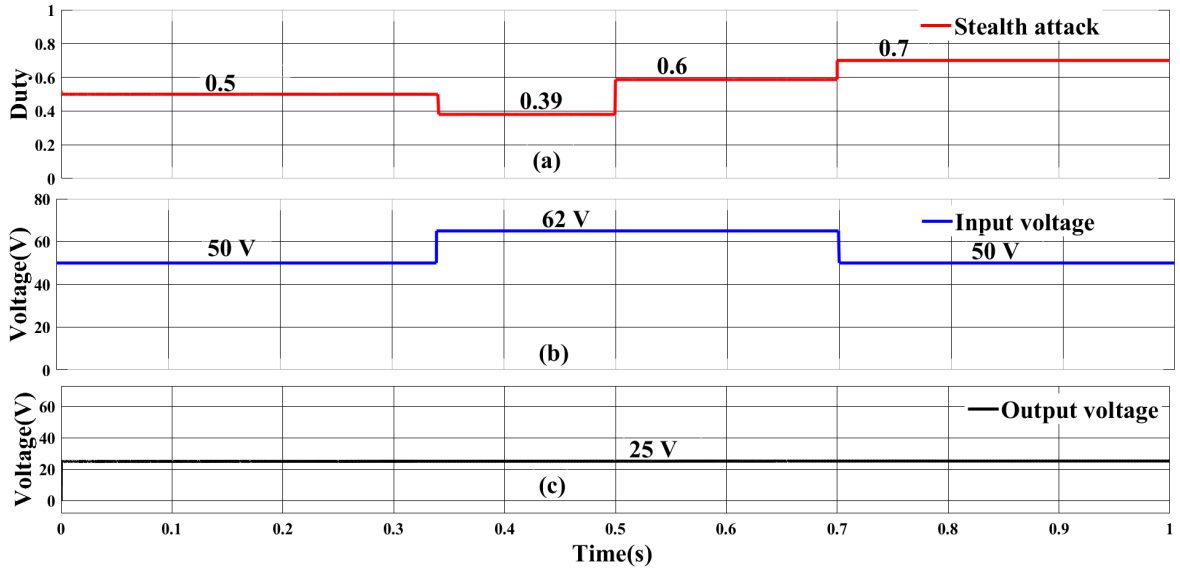

Figure 18. FDI attack on input voltage sensor and Stealth attack

5.3. Hardware Implementation

To test the applicability and accuracy of the proposed control scheme in real-world scenarios, a real-time hardware setup is built in a laboratory environment as shown in Figure 19

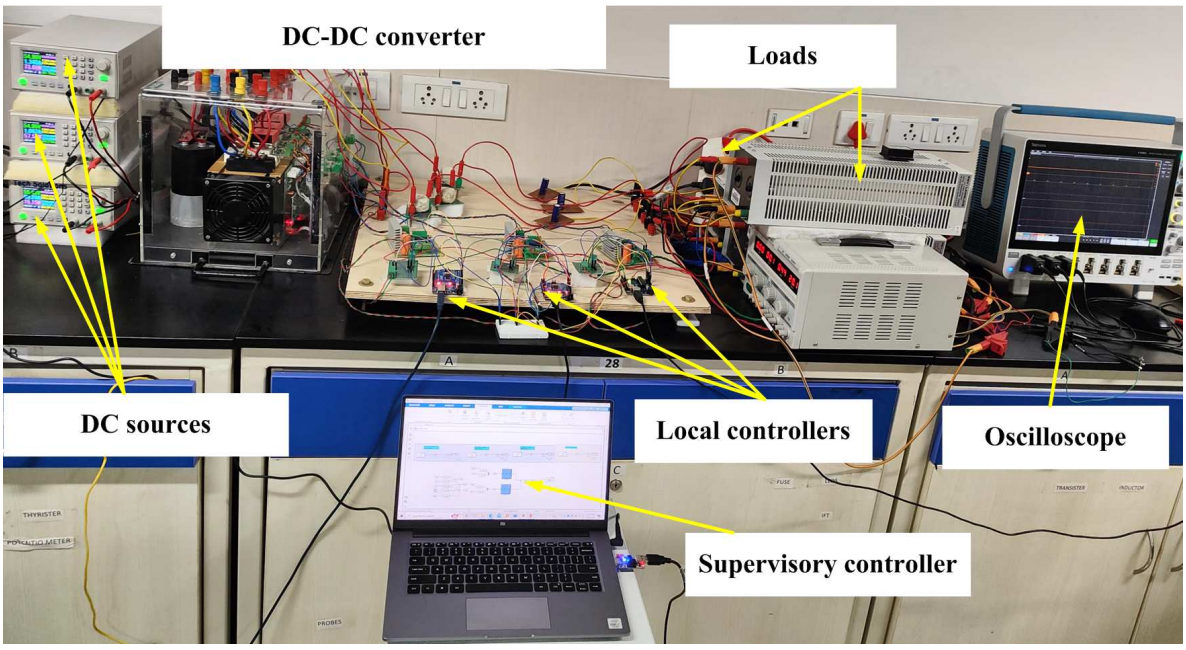

Figure 19. Realtime hardware setup of DC-DC buck converter

Initially, the designed control scheme's ability to control the DC-DC buck converter is analysed. The converter's reference voltage is varied from 25 V to 35 V, Figure 20(a) shows the change in the pulse width corresponding to the change in output of the control algorithm. From Figure 20(b), it is observed that the converter's output voltage is changing from 25 V to 35 V, and it takes approximately 10 ms for the transition.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

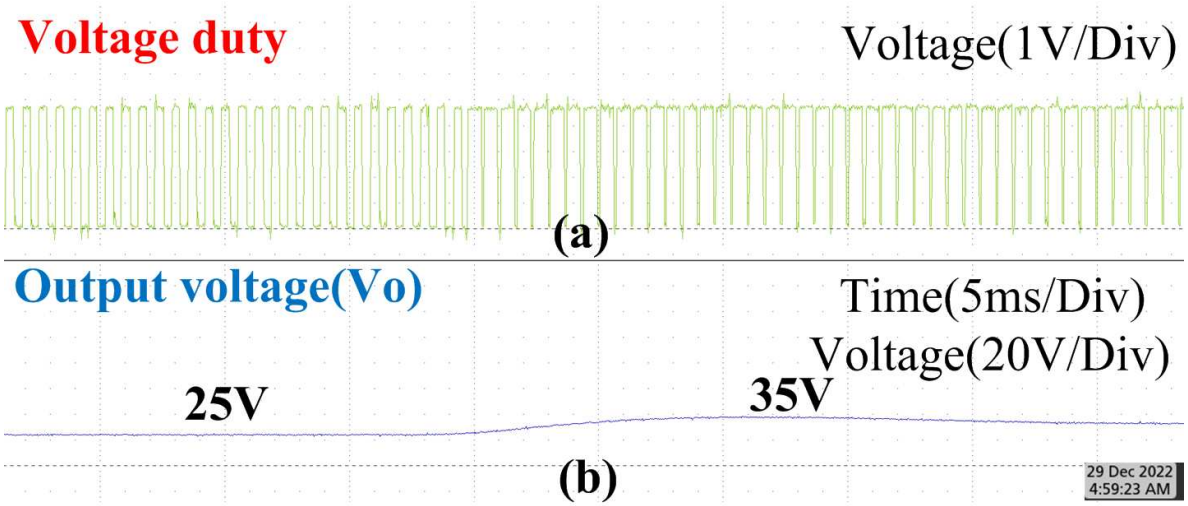

Figure 20. Reference change on DC-DC converter

Figure 21) gives information on the control inputs generated from the controller and the FDI attack on the voltage controller output. Figure 21(a) shows the pulses generated from the duty obtained from the voltage controller. When the adversary performs the FDI attack on the voltage controller data, the pulse width changes as shown in Figure 21(b), and an attacked duty of 0.2 is injected. Figure 21(c) denotes the duty generated from the current controller; it is observed that the voltage duty and current duty are the same.

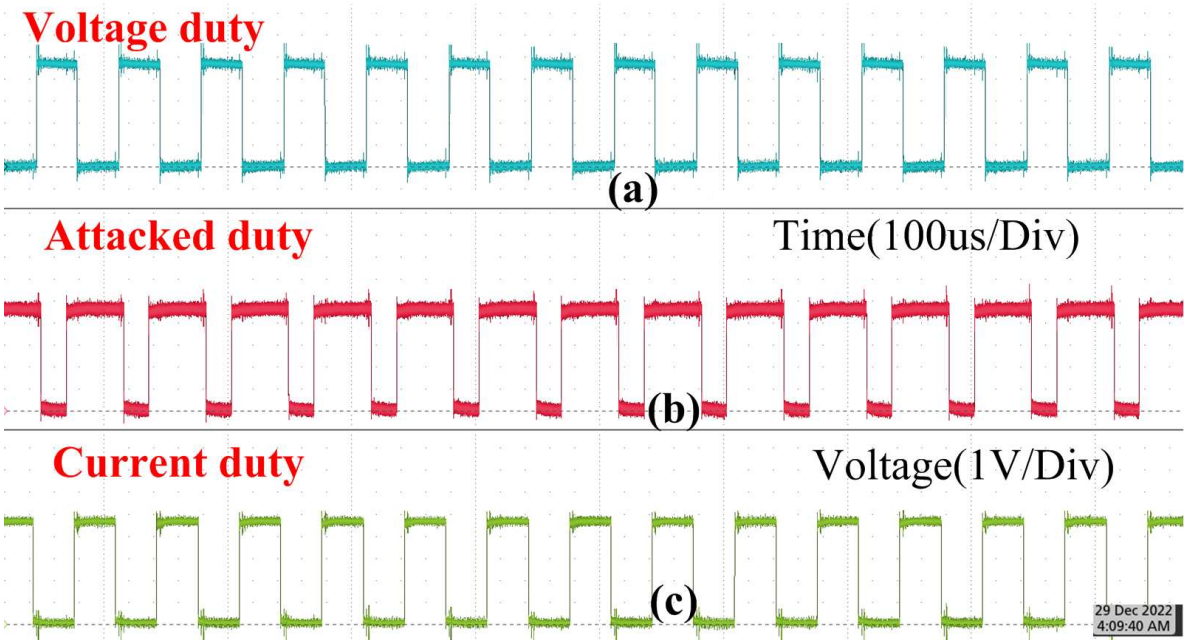

Figure 21. Deep learning controller output with FDI attack

The performance of the designed control algorithm during the SLCA of the FDIA attack can be observed in Figure 22. Figure 22(a) gives the output voltage controller duty and Figure 22(b) shows the FDI attack. Even though a stealth attack is performed by manipulating the output voltage sensor before reaching the controller, the proposed technique mitigates the attack. Figure 22(c) shows the output voltage of the converter which Is the desired reference value.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 April 2023 doi:10.20944/preprints202304.0691.v1

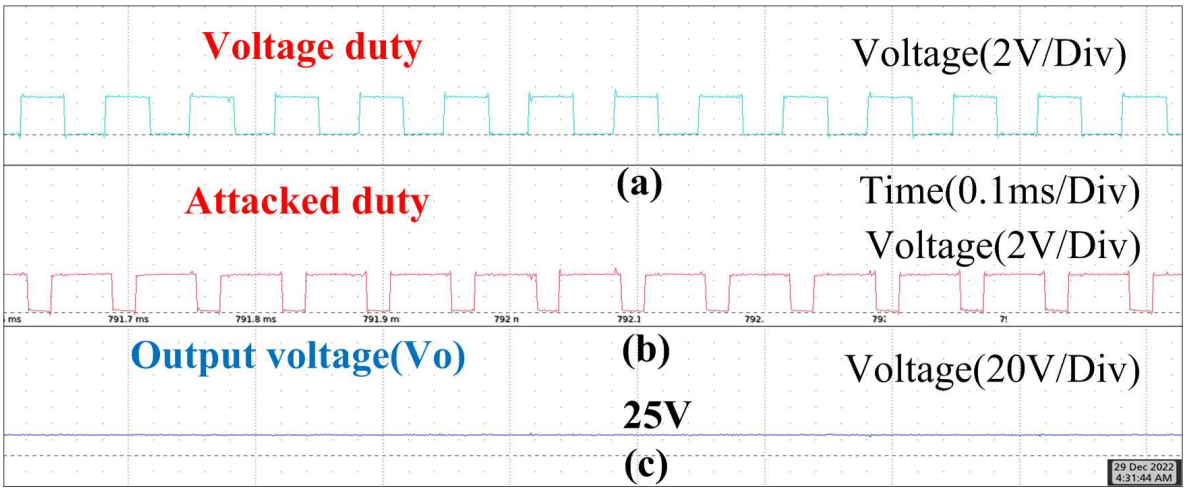

Figure 22. SLCA-FDIA attack mitigation

6. Conclusion

In this article, cyber-attacks on cyber-physical systems and their detection and mitigation methods using deep learning are discussed in detail. The importance of cyber security is discussed in the context of cyber warfare, and a brief discussion on cyber warfare methods is performed. Multiple cyber-attacks to which cyber-physical systems are most vulnerable are discussed in detail. Most common defence mechanisms implemented in network security are examined, and their inability to handle present-day cyberattacks is observed. The advanced and new-age detection techniques for cyber security and artificial intelligence-based cyber security are discussed elaborately, and different methods used in detecting the attacks and their success rates towards attack detection are analysed. A real-time case study is implemented on a DC-DC converter using deep learning to detect and mitigate stealthy false data injection attacks. Further, AI techniques can be implemented on the most complicated CPS for mitigating different types of cyber attacks.

Funding: This work is supported by Science and Engineering Research Board (SERB) under start-up research grant SRG/2020/000269 sponsored to Dr. Sreedhar Madichetty

Abbreviations

The abbreviations used in this article are given below:

ARP	Address resolution protocol
CCS	Change cipher spec
CPS	Cyber-physical systems
DARPA	Defense advanced research projects agency
DNS	Domain name server
EAP	Extensible authentication protocol
EV	Electric vehicle
HTTP	Hypertext transfer protocol
HTTPS	Hypertext transfer protocol secure
IP	Internet protocol

KDD99	Knowledge discovery in databases 1999
MAC	Media access control
OSI	open system interconnection
PLC	Programmable logical controller
RES	Renewable energy sources
SSL	Secure socket layer
TCP	Transfer control protocol
FDI	False data injection
SLCA	Stealthy local covert attack

References

1. Bong, C.P.; Hashim, H.; Ho, W.S.; Ab Muis, Z.B.; Yunus, N.A.B.; Demoral, A.; Tirta, A.; Kresnawan, M.R.; Safrina, R.; Rosalia, S.A. Integration of Variable Renewable Energy, Electric Vehicle, and Smart Microgrid in ASEAN: A Focus Group Discussion Approach. In Proceedings of the IOP Conference Series: Earth and Environmental Science. IOP Publishing, 2022, Vol. 997, p. 012013.
2. Kulkarni, S.V.; Gaonkar, D.N. Operation and control of a microgrid in isolated mode with multiple distributed generation systems. In Proceedings of the 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), 2017, pp. 1–6. https://doi.org/10.1109/TAPENERGY.2017.8397210.
3. Hossain, E.; Kabalcı, E.; Bayindir, R.; Perez, R. A comprehensive study on microgrid technology. *International Journal of Renewable Energy Research* **2014**, *4*, 1094–1104.
4. Bani-Ahmed, S.; Weber, L.; Nasiri, A.; Hosseini, H. Microgrid communications: State of the art and future trends. 2015, pp. 780–785. https://doi.org/10.1109/ICRERA.2014.7016491.
5. Kumar, S.; Islam, S.; Jolfaei, A., Microgrid communications - protocols and standards; 2019; pp. 291–326. https://doi.org/10.1049/PBPO139E_ch9.
6. Serban, I.; Céspedes, S.; Marinescu, C.; Azurdia-Meza, C.A.; Gómez, J.S.; Hueichapan, D.S. Communication Requirements in Microgrids: A Practical Survey. *IEEE Access* **2020**, *8*, 47694–47712. https://doi.org/10.1109/ACCESS.2020.2977928.
7. Robinson, M.; Jones, K.; Janicke, H. Cyber warfare: Issues and challenges. *Computers & Security* **2015**, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007.
8. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems* **2022**, *62*, 82–97.
9. Chasanah, B.; Candiwan, C. Analysis of College Students' Cybersecurity Awareness In Indonesia. *SISFORMA* **2020**, *7*, 49. https://doi.org/10.24167/sisforma.v7i2.2706.
10. Hong, W.C.H.; Chi, C.; Liu, J.; Zhang, Y.; Lei, V.N.L.; Xu, X. The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies* **2022**, pp. 1–32.
11. Cyber security research report 2020, 2021.
12. Freet, D.; Agrawal, R., Cyber Espionage; 2017. https://doi.org/10.1007/978-3-319-32001-4_51-1.
13. Schaefer, T.; Brown, B.; Graessle, F.; Salzsieder, L. Cybersecurity: common risks: a dynamic set of internal and external threats includes loss of data and revenue, sabotage at the hands of current or former employees, and a PR nightmare. *Strategic Finance* **2017**, *99*, 54–62.
14. Hamid, A. Denial of Service Attacks: Tools and Categories. *International Journal of Engineering Research and* **2020**, *V9*. https://doi.org/10.17577/IJERTV9IS030289.
15. Nguyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebsari, A.; Dehghanian, P. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access* **2020**, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2020.2993233.
16. Goswami, M., Fake News and Cyber Propaganda: A Study of Manipulation and Abuses on Social Media; 2018; pp. 535–544.
17. Eling, M.; Elvedi, M.; Falco, G. The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal* **2022**, pp. 1–15.
18. Collins, S.; McCombie, S. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism* **2012**, *7*, 80–91.

19. Dehlawi, Z.; Abokhodair, N. Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. 2013, pp. 73–75. https://doi.org/10.1109/ISI.2013.6578789.
20. Guo, Q.; Xin, S.; Wang, J. Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout. *Dianli Xitong Zidonghua/Automation of Electric Power Systems* **2016**, *40*, 145–147. https://doi.org/10.7500/AEPS20160113101.
21. Cherepanov, A.; Lipovsky, R. Blackenergy–what we really know about the notorious cyber attacks. *Virus Bulletin October* **2016**.
22. Halevi, T.; Memon, N.; Nov, O. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electronic Journal* **2015**. https://doi.org/10.2139/ssrn.2544742.
23. Cherepanov, A.; Lipovsky, R. Industroyer: Biggest threat to industrial control systems since Stuxnet. *WeLiveSecurity, ESET* **2017**, *12*.
24. Dudley, R.; Golden, D. The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms. *MIT Technology Review and ProPublica* **2021**.
25. Khoshnood, A. The Attack on Natanz and the JCPOA. *BESA Center Perspectives Paper* **2021**.
26. Espina, E.; Llanos, J.; Burgos-Mellado, C.; Cárdenas-Dobson, R.; Martínez-Gómez, M.; Sáez, D. Distributed Control Strategies for Microgrids: An Overview. *IEEE Access* **2020**, *8*, 193412–193448. https://doi.org/10.1109/ACCESS.2020.3032378.
27. Nasirian, V.; Moayedi, S.; Davoudi, A.; Lewis, F.L. Distributed Cooperative Control of DC Microgrids. *IEEE Transactions on Power Electronics* **2015**, *30*, 2288–2303. https://doi.org/10.1109/TPEL.2014.2324579.
28. Tan, S.; Wu, Y.; Xie, P.; Guerrero, J.M.; Vasquez, J.C.; Abusorrah, A. New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience. *IEEE Electrification Magazine* **2020**, *8*, 98–106.
29. Liang, G.; Zhao, J.; Luo, F.; Weller, S.; Dong, Z. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Transactions on Smart Grid* **2016**, *8*, 1–1. https://doi.org/10.1109/TSG.2015.2495133.
30. Halfond, W.G.; Viegas, J.; Orso, A.; et al. A classification of SQL-injection attacks and countermeasures. In Proceedings of the Proceedings of the IEEE international symposium on secure software engineering. IEEE, 2006, Vol. 1, pp. 13–15.
31. Endler, D. The evolution of cross site scripting attacks. Technical report, Technical report, iDEFENSE Labs, 2002.
32. Wlazlo, P.; Sahu, A.; Mao, Z.; Huang, H.; Goulart, A.; Davis, K.; Zonouz, S. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *IET Cyber-Physical Systems: Theory & Applications* **2021**, *6*, 164–177.
33. Ali, F. IP spoofing. *The Internet Protocol Journal* **2007**, *10*, 1–9.
34. Whalen, S. An introduction to arp spoofing. *Node99 [Online Document]* **2001**.
35. Steinhoff, U.; Wiesmaier, A.; Araújo, R. The state of the art in DNS spoofing. In Proceedings of the Proc. 4th Intl. Conf. Applied Cryptography and Network Security (ACNS), 2006.
36. Gangan, S. A review of man-in-the-middle attacks. *arXiv preprint arXiv:1504.02115* **2015**.
37. Elleithy, K.M.; Blagovic, D.; Cheng, W.K.; Sideleau, P. Denial of service attack techniques: analysis, implementation and comparison **2005**.
38. Long, N.; Thomas, R. Trends in denial of service attack technology. *CERT Coordination Center* **2001**, *648*, 651.
39. Lau, F.; Rubin, S.H.; Smith, M.H.; Trajkovic, L. Distributed denial of service attacks. In Proceedings of the Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0. IEEE, 2000, Vol. 3, pp. 2275–2280.
40. Neupane, K.; Haddad, R.; Chen, L. Next generation firewall for network security: a survey. In Proceedings of the SoutheastCon 2018. IEEE, 2018, pp. 1–6.
41. Liao, H.J.; Lin, C.H.R.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications* **2013**, *36*, 16–24.
42. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 1–22.
43. Ioulianou, P.; Vasilakis, V.; Moscholios, I.; Logothetis, M. A signature-based intrusion detection system for the internet of things. *Information and Communication Technology Form* **2018**.

44. Gyanchandani, M.; Rana, J.; Yadav, R. Taxonomy of anomaly based intrusion detection system: a review. *International Journal of Scientific and Research Publications* **2012**, *2*, 1–13.
45. Wang, Z.; Li, X. Intrusion prevention system design. In Proceedings of the Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012: Volume 3. Springer, 2013, pp. 375–382.
46. Zhang, Z.; Ning, H.; Shi, F.; Farha, F.; Xu, Y.; Xu, J.; Zhang, F.; Choo, K.K.R. Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review* **2022**, pp. 1–25.
47. Shrestha Chitrakar, A.; Petrović, S. Efficient k-means using triangle inequality on spark for cyber security analytics. In Proceedings of the Proceedings of the ACM international workshop on security and privacy analytics, 2019, pp. 37–45.
48. Husák, M.; Kašpar, J.; Bou-Harb, E.; Čeleda, P. On the sequential pattern and rule mining in the analysis of cyber security alerts. In Proceedings of the Proceedings of the 12th International Conference on Availability, Reliability and Security, 2017, pp. 1–10.
49. Azeez, N.A.; Ayemobola, T.J.; Misra, S.; Maskeliūnas, R.; Damaševičius, R. Network intrusion detection with a hashing based apriori algorithm using Hadoop MapReduce. *Computers* **2019**, *8*, 86.
50. Aung, Y.Y.; Min, M.M. Hybrid intrusion detection system using K-means and K-nearest neighbors algorithms. In Proceedings of the 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS). IEEE, 2018, pp. 34–38.
51. Majeed, R.; Abdullah, N.A.; Mushtaq, M.F. IoT-based Cyber-security of Drones using the Naïve Bayes Algorithm. *International Journal of Advanced Computer Science and Applications* **2021**, *12*.
52. Meyer, D.; Wien, F. Support vector machines. *The Interface to libsvm in package e1071* **2015**, *28*, 20.
53. Al-Omari, M.; Rawashdeh, M.; Qutaishat, F.; Alshira'H, M.; Ababneh, N. An intelligent tree-based intrusion detection model for cyber security. *Journal of Network and Systems Management* **2021**, *29*, 1–18.
54. Rahman, C.M.; Farid, D.M.; Harbi, N.; Bahri, E.; Rahman, M.Z. Attacks classification in adaptive intrusion detection using decision tree **2010**.
55. Ferrag, M.A.; Maglaras, L.; Ahmim, A.; Derdour, M.; Janicke, H. Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. *Future internet* **2020**, *12*, 44.
56. Choubisa, M.; Doshi, R.; Khatri, N.; Hiran, K.K. A simple and robust approach of random forest for intrusion detection system in cyber security. In Proceedings of the 2022 International Conference on IoT and Blockchain Technology (ICIBT). IEEE, 2022, pp. 1–5.
57. Chen, Z.; Zhou, L.; Yu, W. ADASYN- Random Forest Based Intrusion Detection Model. In Proceedings of the 2021 4th International Conference on Signal Processing and Machine Learning, 2021, pp. 152–159.
58. Apruzzese, G.; Andreolini, M.; Colajanni, M.; Marchetti, M. Hardening random forest cyber detectors against adversarial attacks. *IEEE Transactions on Emerging Topics in Computational Intelligence* **2020**, *4*, 427–439.
59. Shrestha, A.; Mahmood, A. Review of deep learning algorithms and architectures. *IEEE access* **2019**, *7*, 53040–53065.
60. Bapiyev, I.M.; Aitchanov, B.H.; Tereikovskyi, I.A.; Tereikovska, L.A.; Korchenko, A.A. Deep neural networks in cyber attack detection systems. *International Journal of Civil Engineering and Technology (IJCIET)* **2017**, *8*, 1086–1092.
61. Zhou, L.; Ouyang, X.; Ying, H.; Han, L.; Cheng, Y.; Zhang, T. Cyber-attack classification in smart grid via deep neural network. In Proceedings of the Proceedings of the 2nd international conference on computer science and application engineering, 2018, pp. 1–5.
62. Jemal, I.; Haddar, M.A.; Cheikhrouhou, O.; Mahfoudhi, A. Performance evaluation of Convolutional Neural Network for web security. *Computer Communications* **2021**, *175*, 58–67.
63. Alabadi, M.; Celik, Y. Anomaly detection for cyber-security based on convolution neural network: A survey. In Proceedings of the 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2020, pp. 1–14.
64. Tang, T.A.; McLernon, D.; Mhamdi, L.; Zaidi, S.A.R.; Ghogho, M. Intrusion detection in sdn-based networks: Deep recurrent neural network approach. *Deep Learning Applications for Cyber Security* **2019**, pp. 175–195.
65. Feltus, C. Learning algorithm recommendation framework for IS and CPS security: Analysis of the RNN, LSTM, and GRU contributions. *International Journal of Systems and Software Security and Protection (IJSSSP)* **2022**, *13*, 1–23.
66. Tasneem, S.; Gupta, K.D.; Roy, A.; Dasgupta, D. Generative Adversarial Networks (GAN) for Cyber Security: Challenges and Opportunities.

67. Chen, D.; Wawrzynski, P.; Lv, Z. Cyber security in smart cities: a review of deep learning-based applications and case studies. *Sustainable Cities and Society* **2021**, *66*, 102655.
68. Yousefi-Azar, M.; Varadharajan, V.; Hamey, L.; Tupakula, U. Autoencoder-based feature learning for cyber security applications. In Proceedings of the 2017 International joint conference on neural networks (IJCNN). IEEE, 2017, pp. 3854–3861.
69. Li, C.; Qiu, M.; Li, C. Reinforcement Learning for Cybersecurity. *Reinf. Learn. Cyber-Phys. Syst* **2019**, pp. 155–168.
70. Amor, N.B.; Benferhat, S.; Elouedi, Z. Naive bayes vs decision trees in intrusion detection systems. In Proceedings of the Proceedings of the 2004 ACM symposium on Applied computing, 2004, pp. 420–424.
71. Amiri, F.; Yousefi, M.R.; Lucas, C.; Shakery, A.; Yazdani, N. Mutual information-based feature selection for intrusion detection systems. *Journal of Network and Computer Applications* **2011**, *34*, 1184–1199.
72. Zhang, J.; Zulkernine, M.; Haque, A. Random-forests-based network intrusion detection systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* **2008**, *38*, 649–659.
73. Ravipati, R.D.; Abualkibash, M. Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets-a review paper. *International Journal of Computer Science & Information Technology (IJCSIT) Vol* **2019**, *11*.
74. Gao, N.; Gao, L.; Gao, Q.; Wang, H. An intrusion detection model based on deep belief networks. In Proceedings of the 2014 Second international conference on advanced cloud and big data. IEEE, 2014, pp. 247–252.
75. Choudhary, S.; Kesswani, N. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. *Procedia Computer Science* **2020**, *167*, 1561–1573.
76. Ahsan, M.; Nygard, K.E. Convolutional Neural Networks with LSTM for Intrusion Detection. In Proceedings of the CATA, 2020, Vol. 69, pp. 69–79.
77. Gurung, S.; Ghose, M.K.; Subedi, A. Deep learning approach on network intrusion detection system using NSL-KDD dataset. *International Journal of Computer Network and Information Security* **2019**, *11*, 8–14.
78. Ding, Y.; Zhai, Y. Intrusion detection system for NSL-KDD dataset using convolutional neural networks. In Proceedings of the Proceedings of the 2018 2nd International conference on computer science and artificial intelligence, 2018, pp. 81–85.
79. Amin, M.; El-Sousy, F.F.; Aziz, G.A.A.; Gaber, K.; Mohammed, O.A. CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: a review. *IEEE Access* **2021**, *9*, 38571–38601.
80. Cazorla, L.; Alcaraz, C.; Lopez, J. Cyber stealth attacks in critical information infrastructures. *IEEE Systems Journal* **2016**, *12*, 1778–1792.
81. Mikhaylenko, D.; Zhang, P. Stealthy local covert attacks on cyber-physical systems. *IEEE Transactions on Automatic Control* **2021**.
82. Sun, K.; Esnaola, I.; Perlaza, S.M.; Poor, H.V. Stealth attacks on the smart grid. *IEEE Transactions on Smart Grid* **2019**, *11*, 1276–1285.
83. Annavaram, D.; Sahoo, S.; Mishra, S. Stealth Attacks in Microgrids: Modeling Principles and Detection. In Proceedings of the 2021 9th IEEE International Conference on Power Systems (ICPS). IEEE, 2021, pp. 1–6.
84. Pasetti, M.; Ferrari, P.; Bellagente, P.; Sisinni, E.; de Sá, A.O.; do Prado, C.B.; David, R.P.; Machado, R.C.S. Artificial neural network-based stealth attack on battery energy storage systems. *IEEE Transactions on Smart Grid* **2021**, *12*, 5310–5321.