sensors

MDPI

Article

Resilient Consensus Control Design for DC Microgrids against False Data Injection Attacks Using a Distributed Bank of Sliding Mode Observers

Yousof Barzegari [1], Jafar Zarei [1,2,*], Roozbeh Razavi-Far [2], Mehrdad Saif [2] and Vasile Palade [3,*]

[1] Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz 71557-13876, Iran; y.barzegari@sutech.ac.ir
[2] Department of Electrical and Computer Engineering, University of Windsor, Sunset Ave., Windsor, ON N9B 3P4, Canada; roozbeh@uwindsor.ca (R.R.-F.); msaif@uwindsor.ca (M.S.)
[3] Center for Computational Science and Mathematical Modeling, Coventry University, Coventry CV1 5FB, UK
* Correspondence: zarei@sutech.ac.ir (J.Z.); vasile.palade@coventry.ac.uk (V.P.)

Abstract: This paper investigates the problem of false data injection attack (FDIA) detection in microgrids. The grid under study is a DC microgrid with distributed boost converters, where the false data are injected into the voltage data so as to investigate the effect of attacks. The proposed algorithm uses a bank of sliding mode observers that estimates the states of the neighbor agents. Each agent estimates the neighboring states and, according to the estimation and communication data, the detection mechanism reveals the presence of FDIA. The proposed control scheme provides resiliency to the system by replacing the conventional consensus rule with attack-resilient ones. In order to evaluate the efficiency of the proposed method, a real-time simulation with eight agents has been performed. Moreover, a verification experimental test with three boost converters has been utilized to confirm the simulation results. It is shown that the proposed algorithm is able to detect FDI attacks and it protects the consensus deviation against FDI attacks.

Keywords: DC microgrid; attack-resilient control; boost converter; sliding mode observer; false data injection cyber attack

Citation: Barzegari, Y.; Zarei, J.; Razavi-Far, R.; Saif, M.; Palade, V. Resilient Consensus Control Design for DC Microgrids against False Data Injection Attacks Using a Distributed Bank of Sliding Mode Observers. *Sensors* **2022**, *22*, 2644. https://doi.org/10.3390/s22072644

Academic Editor: Antonino Laudani

Received: 4 February 2022
Accepted: 28 March 2022
Published: 30 March 2022

1. Introduction

In recent years, distributed control has received considerable attention due to its high efficiency, simplicity, and reliability. DC microgrids can be represented as a distributed system, and therefore, distributed control techniques are widely utilized to control these systems. However, due to the nature of distributed networks and also advances in cyber attack methods, these systems are vulnerable to malicious attacks. One of the positive points for these systems is the versatility of a wide range of DC sources, which allows these sources to be used simultaneously in a microgrid [1–4]. Small energy sources such as solar photovoltaics, fuel cells, batteries, and other renewable energy sources (RESes) [3] mainly have low output voltage and need to boost converters to increase the voltage levels up to the network reference. The most popular control techniques used to regulate the voltage are back stepping [5], sliding mode control (SMC) [6,7], model predictive control (MPC) [8,9], and passivity-based control [10]. These methods have the advantages of robustness, stability, optimality, and flexibility [11].

In a microgrid, for supply distributed and different types of loads, we need distributed networked RESes with two features; all must be grid-connected and operate autonomously [12]. In these cases, designing a distributed control law to reach an agreement between all nodes regarding certain constraints that depends on the state of all agents is named a consensus algorithm [13]. Decentralized and distributed controls are two main keys for consensus problems [14].

Decentralized consensus is not vulnerable at a breakdown point, and is considered as a scalable and efficient control for network management [12]. In general, the purpose of distributed control in a DC microgrid is to reach a voltage consensus and proportional current distribution [15]. In the microgrid, each RES is an agent which cooperates and communicates with the neighbors to reach a consensus. Consensus is possible if the cyber networks report the measurements correctly. Any violation of measurement or incorrect reporting will result in an incorrect voltage or current distribution. In communication-based distributed networks, one of the main threats to the network is cyber attacks [16–18].

Cyber attacks are very costly for distributed power systems depending on the type, time, and place of occurrence. It causes major economical and technical problems that may be irreparable [19,20]. The most important of these attacks can be categorized into replay attacks, in which transmitted data are stored and repeated periodically, denial of service attacks (DOSA) [21], false data injection attacks (FDIA), and stealth attacks, in which the attackers have sufficient knowledge about the system model, controller, and network architecture [22]. Stealth attacks can easily bypass the bad-data detection mechanisms [19]. These attacks occurs in microgrids by injecting false data to the communication packets over the communication cyber links. Due to the variety of attack categories, denial of service attacks lead to disconnection and are very easy to detect. Therefore, from the viewpoint of attackers, a false data injection attack has a better chance of winning. Therefore, one of the most important attacks is FDIA, which is studied in this article.

There are several data security methods, such as cryptography, user administration, etc.; these are necessary but not enough to protect the systems against all cyber attacks. This is because the attackers are smart and their methods and knowledge about the systems are growing. Prevention is the first step in countering attacks, and the next step is resiliency. In recent years, several strategies have been proposed to detect and reduce the disadvantageous effects of attacks in microgrids. Some approaches are Kalman-filter-based methods to estimate process variables [23], local observers for fault and field level attacks [24], resilient distributed strategies for detecting and isolating time-varying attacks [25], event-triggered strategies proposed to make the control tolerant and robust under DOSA [26], the game theory defense method for a hierarchical networked microgrid structure [27], secure distributed state estimation for the network under FDIA [28], and distributed cyber attack detection for linear large-scale systems by a bank of unknown input observers (UIO) [29]. In general, all these works can be summarized as two main categories, secure robust control, and secure state estimation.

Considering these issues, the main objective of the current work is to design a distributed consensus algorithm to be resilient against false data injection attacks in a DC microgrid. The proposed method is developed based on the distributed observer form of attack detection schemes to achieve a resilient strategy. In this structure, each agent is locally equipped with a detection mechanism and resilient consensus control that utilizes the information of neighbor agents' states. To regulate the output voltage of each agent, the sliding mode controller is employed while the reference voltage of the controller is generated by the consensus law. Moreover, it is assumed that the converter voltage and current value can be measured. In order to achieve a resilient control structure, the consensus control is designed so as to be resilient in the presence of the FDIAs. Therefore, when an attack is detected, the corresponding agent will be neglected from the agreement process. In order to detect an FDI attack, a bank of sliding mode observers is designed in each agent in such a way that each observer is related to one of the neighbors.

Using the proposed attack detection algorithm, the compliance of received data from the neighboring agents will be checked with the estimated data from the corresponding observer and so the presence of the attack will be detected. The performance of this method has been validated with simulation and experimental tests to conclude that the proposed mechanism is able to detect the presence of attacks effectively and it is resilient. Compared with the existing literature, the main contributions of this article can be summarized as follows.

1. Compared to previous studies such as [12,22], the proposed approach develops a bank of robust observers for each agent that makes the detection and isolation of the false data injection attacks feasible. Therefore, by eliminating the effect of the attack in the consensus law, a resilient control is achieved.
2. The controller and observers are designed based on robust approaches, which is very important in practical applications. It is shown that consensus is successfully achieved even in the presence of cyber attacks, while the modeling uncertainty is considered.
3. A resilient consensus law is proposed to remove the false data injection attacks from the agreement procedure.
4. The practical efficiency of the proposed method is evaluated in an experimental testbed that is close to real-world applications. To this aim, a complex real-time hardware test is performed by MATLAB, Simulink real-time (XPC-Target), LAN communication, FPGA and Microblaze coding, control board design, and three DC-DC boost converters.

The remaining structure of this article is as follows. In Section 2, the basic concepts for graph theory, consensus protocol, and the microgrid model are presented. A model for the communication link attacks is provided in Section 3. Sliding mode controller and observers are designed in Section 4. The proposed resilience consensus law is developed in Section 5. Simulations and experimental validation are presented in Sections 6 and 7. Finally, the paper is concluded in Section 8.

2. Background

2.1. Graph Theory

In this section, some basic definitions of graph theory are reviewed. A graph is a set of nodes that are connected to each other by several links. It is noted as $G = \{V, E, A\}$ that represents information flow between the nodes in the network; $V = \{v_1, \ldots, v_n\}$ is the set of network nodes, where n is the number of nodes, $E \subseteq V \times V$ is the set of network links, and $A = [a_{ij}]$ is the adjacency matrix that $a_{ii} = 0, 0 < \delta \leq a_{ij} < 1$, where δ is a lower bound for gain of adjacency matrix links. If node i has access to the states of node j, it means there is a link between them, which is denoted by $e_{ij} = (v_i, v_j) \in E$. The neighbors of node i are denoted by $N_i = \{j \in V : (i, j) \in E, i \neq j\}$, which can communicate with node i.

$\mathbf{L} = [l_{ij}]_{n \times n} \in \mathbb{R}^{n \times n}$ is the Laplacian matrix, where $l_{ii} = \sum_{j=1, i \neq j}^{n} a_{ij}$ and $(l_{ij} = -a_{ij}$ for $i \neq j)$. The eigenvalues of the Laplacian matrix can be ordered as $\lambda_1 < \lambda_2 < \ldots < \lambda_n$, where λ_2 is called the algebraic connectivity of the graph. A graph is connected if only its algebraic connectivity is positive: $\lambda_2 > 0$. In a connected graph, agreement will be met, if the condition $\lim_{t \to \infty} \|x_i(t) - x_j(t)\| = 0, \forall i, j = 1, \ldots, n$, is established [30,31].

2.2. Conventional Consensus Protocol

In a network of agents, reaching an agreement between nodes is called consensus. In general, each node is modeled as

$$x_i(t) = f(x_i(t), u_i(t)) \tag{1}$$

A dynamic graph is shown by (G, x), where G is the graph topology and x is agents' states that are described by (1). The consensus problem is described by finding a way to guide agents' states to an agreement. In a simple and ideal multi-agent system, $u_i(t)$ depends on the states of neighbors that are compared and gained. This is expressed as:

$$u_i(t) = f_c(x_i(t), x_{j_1}(t), \ldots, x_{j_m}(t)) \tag{2}$$

The neighbors of node v_i are denoted by $N_i = \{v_j \in V : (v_i, v_j) \in E\}$, in which m is the number of neighbors. The consensus protocol is using a function for $u_i = f_c(x_i, x_{j \in N_i})$, which causes asymptotically an stable agreement. It is the main goal in the consensus

problems. In general, a consensus rule with a variable topology graph, communication time delay, and asynchronous update for agreement is

$$u_i(t_i) = \sum_{v_j \in N_i} a_{ij}(t_i)[x_j(t_j - \tau_{ij}(t_i)) - x_i(t_i)] \tag{3}$$

where $a_{ij}(t_i)$ is an entry of the adjacency matrix A that may change by time and is related to the edge of E_{ij}, $\tau_{ij} < \tau$ is the bounded delay related to the edge E_{ij} at time t_i, $t_j \leq t_i$ is the update time for Agent j , which shows that the update time for any agent may be different. By (3), each agent state goes to the neighbors' states and the graph reaches consensus $\lim_{t\to\infty} \sum_{j\in N_i} \|x_i(t) - x_j(t)\| = 0$.

2.3. DC-Microgrid Dynamic

The aim of this section is to introduce a typical model for a DC-DC boost converter in a state space approach. A typical DC-DC boost converter circuit is depicted in Figure 1.

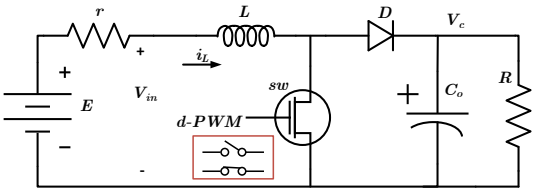

Figure 1. Generalized power model for DC-DC boost converters.

In this figure, V_{in} is the battery voltage, r is the sum of inductor resistance and battery resistor, L is an inductor, sw is an ideal switch, D is an ideal diode, C_o is the capacitor, and R is the load. The i_L is the inductance current that is considered as a state x_1 and V_c is the voltage of the capacitor or output voltage considered as a state x_2. Based on Kirchhoff's laws for the ON and OFF states of the switch, two models are given. These two models alternate with switching frequency periods.

Due to the fact that the switching frequency is very high and the rising time and falling time of the switch is very small, the average model for the converter can be used. According to the duty cycle of switch operation (switch is ON for d and OFF for $(1-d)$ in any period), the non-linear average model of the DC-DC boost converter is presented in (4) and the linear time-variant state space is presented in (5).

$$\begin{cases} \dot{x}_1 = -\dfrac{r}{L}x_1 - \dfrac{1-d}{L}x_2 + \dfrac{1}{L}V_{in} \\ \dot{x}_2 = \dfrac{-1}{RC_o}x_2 + \dfrac{1-d}{C_o}x_1 \\ y = x_2 \end{cases} \tag{4}$$

$$\begin{aligned} A_i &= \begin{bmatrix} \dfrac{-r}{L} & \dfrac{-(1-d)}{L} \\ \dfrac{(1-d)}{C_o} & \dfrac{-1}{RC_o} \end{bmatrix}, B_i = \begin{bmatrix} \dfrac{1}{L} \\ 0 \end{bmatrix} \\ C_i &= \begin{bmatrix} 0 & 1 \end{bmatrix} \end{aligned} \tag{5}$$

where $x \in \mathbb{R}^n$ is the state vector, $y \in \mathbb{R}^p$ is the output vector, $u \in \mathbb{R}^q$ represents the known inputs, and the r term is intended to take into account the voltage drop that is caused by the battery current. It is assumed that A_i, B_i, and C_i are known matrices with appropriate dimensions. For power balance in the steady state, it is:

$$\begin{aligned} &\begin{cases} sw = 0 \\ Q_{in} = Q_{out} \end{cases} \rightarrow i_L(1-d)T = I_{out}T \\ &\rightarrow i_L = \frac{I_{out}}{(1-d)} \rightarrow x_1 = \frac{x_2}{R(1-d)} \end{aligned} \tag{6}$$

3. Cyber-Physical Attack Model

In the microgrids, two features are very important; first, a global voltage reference exists, which must be followed by all the network nodes, and the second is that all the network nodes must follow the neighboring nodes. With these two requirements, the goal of the network, which is a uniform and homogeneous voltage distribution, is achieved. Because the microgrid consensus is based on interaction and communication within the network, the microgrid consensus is always under threat. Despite all the security and encryption in communications, there are always some attacks aimed at systems by destabilizing goals; thus, the agents must be sensitive to these attacks. In this case, it is assumed that attacks are performed by injecting false data into the output voltage information that transmits between agent neighbors in the network.

For cyber-link attacks in the ith controller, the attacked value can be modeled as

$$y_{ij}^{at}(t) = y_i(t) + k_{at}(t - T_{at}^{ij}) f_{ij}^{at}(t) \tag{7}$$

where k_{at} indicates the attack vector that expresses the existence of an attack, $f_{ij}^{at}(t)$ denotes the attack function in communication link ij, $T_{at}^{ij} > 0$ is the initial time of attack, y_i is the real voltage output of Agent i, and y_{ij}^{at} represents the attacked value that Agent j receives through the communication link about Agent i. For example, according to Figure 2, the communication data from Agent i to Agent j are attacked and the voltage data delivered to Agent j are false.

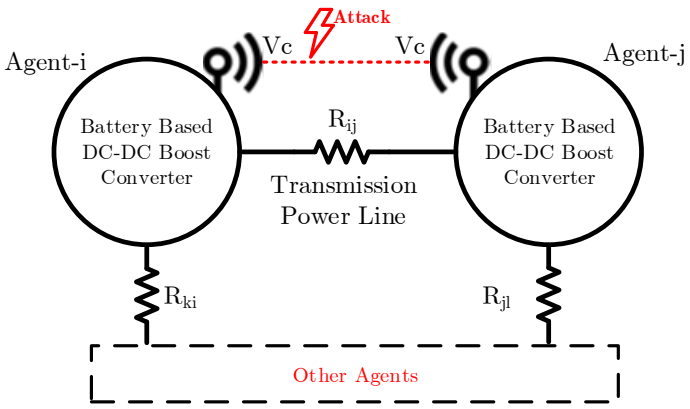

Figure 2. Physical cyber layer and communication link false data injection attack for a DC microgrid.

This malicious data lead to an incorrect consensus for the microgrid. For different types of attacks, the $f_{ij}^{at}(t)$ can take different functions [32]: for FDIA, $f_{ij}^{at}(t)$ can take any function of time; for a reply attack, it can be $f_{ij}^{at}(t) = -y_i(t) + y_i(t - nT)$, where T is a period of time; in a denial of service attack, it is $f_{ij}^{at}(t) = -y_i(t)$, which blocks the link by preventing some or all data transmission over the communication link, and for a stealth attack, all data vectors may be replaced with malicious data in such a way that observers cannot find any deviation compared to the system model.

4. Observer-Based Attack Detection

To reach a correct consensus in a DC microgrid network, the communication data between the neighboring agents must be correct. If only one piece of the communication data within the network is attacked, the network will reach a false consensus around this value. Therefore, each agent must prevent the influence of defective data. Moreover, because of model parameters' uncertainty due to factory tolerance, derating, temperature sensitivity, and others, the model is not accurate and control needs to implement a robust strategy. In this paper, a sliding mode controller is proposed to control the converter, and a sliding mode observer (SMO) is proposed to detect the presence of the attack in the received

data. To reach consensus in the proposed method, in addition to the conditions mentioned in the graph theory, each agent must be connected to the $n+1$ neighbors, where n is the maximum number of attacks in time. This is because, if n attack occurs at the same time, at least a healthy link is needed to achieve consensus.

4.1. Sliding Mode Control

The challenge for the boost converter is to design a control law for the duty cycle $u(t) \in [0,1]$ to regulate the output voltage $\lim_{t\to\infty} x_2(t) = x_2^d$ (x_2^d is the desired output voltage), while the battery voltage E is uncertain and bounded with $\Delta E < \zeta$. For this goal, a sliding mode control is designed. The boost converters represent non-linear dynamics with non-minimum phase characteristics [6]. Therefore, the voltage regulation using the switching function $S = x_2 - x_2^d$ is not acceptable, though it causes the output voltage to be equal to the desired value. This voltage sliding surface results in an unstable zero dynamic in the inductor current in the sliding motion [33]. According to the relation between position and velocity control, the dynamic of the current is much faster than the output voltage.

Theorem 1. *Consider the system defined in Equation (4). For this system, there exists a distributed sliding mode controller that keeps the microgrid voltages in an asymptotically stable agreement.*

Proof. Design the distributed sliding mode controller for each agent

$$\begin{aligned} u &= u_{eq} + u_n = u_{eq} + k\mathrm{sgn}(S) \\ \mathrm{sgn}(S) &= \begin{cases} 1 & S > 0 \\ -1 & S < 0 \end{cases} \end{aligned} \tag{8}$$

where S is the sliding surface that is shown in Equation (9), sgn is the sign function, k is the gain for sign function, and u_{eq} is the equal control law that is derived in Equation (11).

To improve the stability of the mentioned sliding mode control, S is the state variable trajectory and is described as

$$S = \lambda_1 \tilde{x}_2 + \lambda_2 \int \tilde{x}_2 + \lambda_3 x_1 \tag{9}$$

where the voltage error has been defined as $\tilde{x}_2 = x_2 - x_2^d$ and $\lambda_1, \lambda_2, \lambda_3$ are sliding coefficients. The time derivative of the switching function is

$$\begin{aligned} \dot{S} &= \lambda_1 \dot{\tilde{x}}_2 + \lambda_2 \tilde{x}_2 + \lambda_3 \dot{x}_1 \\ &= \lambda_1 \left(\frac{-1}{RC} x_2 + \frac{1-u}{C} x_1 - \dot{x}_2^d\right) + \lambda_2 \tilde{x}_2 + \lambda_3 \left(-\frac{1-u}{L} x_2 - \frac{r}{L} x_1 + \frac{1}{L} E\right) \\ &= (1-u)\left(\frac{\lambda_1}{C} x_1 - \frac{\lambda_3}{L} x_2\right) + \left(-\frac{\lambda_1}{RC} x_2 + \lambda_2 \tilde{x}_2 - \frac{\lambda_3 r}{L} x_1 + \frac{\lambda_3}{L} E\right) \end{aligned} \tag{10}$$

where x_2^d is assumed to be constant, which is calculated by the consensus algorithm in Equation (3). In order to attend to the dynamics of the sliding surface, the time derivative of the sliding surface is investigated. The purpose of this rule is to ensure that, for any initial values, the states will reach the sliding surface. This equation expresses that if we are not on the sliding surface, the path S is an absorbing path to the sliding surface. It is found from $\dot{S} = 0$ that

$$\begin{aligned} (1-u_{eq}) &= -\frac{\left(-\frac{\lambda_1}{RC} x_2 + \lambda_2 \tilde{x}_2 - \frac{\lambda_3 r}{L} x_1 + \frac{\lambda_3}{L} E\right)}{\left(\frac{\lambda_1}{C} x_1 - \frac{\lambda_3}{L} x_2\right)} \\ u_{eq} &= \frac{\left(\frac{\lambda_1}{C} x_1 - \frac{\lambda_3}{L} x_2\right) + \left(-\frac{\lambda_1}{RC} x_2 + \lambda_2 \tilde{x}_2 - \frac{\lambda_3 r}{L} x_1 + \frac{\lambda_3}{L} E\right)}{\left(\frac{\lambda_1}{C} x_1 - \frac{\lambda_3}{L} x_2\right)} \end{aligned} \tag{11}$$

The u_{eq} value is calculated for the nominal parameters of the model, and according to the uncertainties of the model, another component must be added to the input to be robust. According to Equation (8), for finding the range of k values, the stability condition of the sliding mode controller is $S\dot{S} \leq -\eta|S|$. For achieving finite-time convergence,

$$\begin{aligned}
&S\dot{S} \leq -\eta|S|, \quad \eta > 0 \rightarrow t_r = \frac{|S(0)|}{\eta} \\
&S\left[(-\frac{\lambda_1}{RC}x_2 + \lambda_2\tilde{x}_2 - \frac{\lambda_3 r}{L}x_1 + \frac{\lambda_3}{L}E + \frac{\lambda_3}{L}\Delta E) + (1 - u_{eq} - k\text{sgn}(S))(\frac{\lambda_1}{C}x_1 - \frac{\lambda_3}{L}x_2)\right] = \\
&S\left[\frac{\lambda_3}{L}\Delta E + (-k\text{sgn}(S)(\frac{\lambda_1}{C}x_1 - \frac{\lambda_3}{L}x_2)\right] \leq \\
&|S|\left[\frac{\lambda_3}{L}\zeta + -k(\frac{\lambda_1}{C}x_1 - \frac{\lambda_3}{L}x_2)\right] \leq -\eta|S| \\
&\frac{\lambda_3}{L}\zeta - k(\frac{\lambda_1}{C}x_1 - \frac{\lambda_3}{L}x_2) \leq -\eta \\
&k \geq \frac{\eta}{|\frac{\lambda_1}{C}x_1 - \frac{\lambda_3}{L}x_2|} + \frac{\lambda_3}{L}\zeta \\
&\square
\end{aligned} \tag{12}$$

4.2. Sliding Mode Observer Attack Detector

Observers are dynamic systems that are used to estimate the system states based on the measurements of system inputs and outputs [34]. The estimation occurs when we do not have access to some state variables or we face a fault detection problem. In order to design an observer for the non-linear systems or with parametric uncertainty and perturbation, the sliding mode observers are proposed. It is appropriate for robust estimation, accurate tracking, limited time convergence, and fault detection. In this paper, we convert a non-linear DC-DC boost converter problem to a time-varying linear problem by the assumption that we know the duty cycle values. According to Figure 3, if we have access to the duty cycle d, the non-linear model for the boost converter can be replaced with a linear time-varying model. By this definition, nothing changes for the system dynamics, and we can use a linear sliding mode observer for this problem.

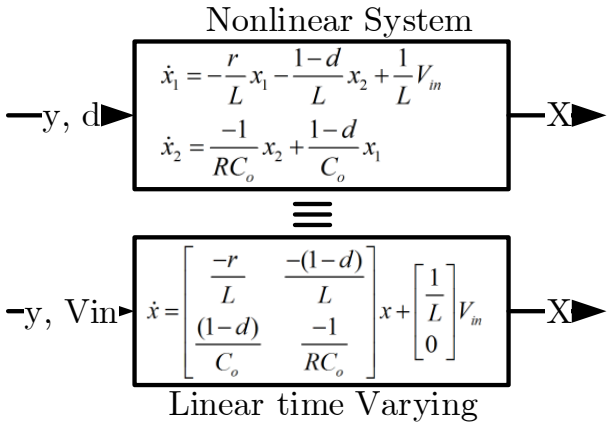

Figure 3. In order to estimate the state vector X, two explanations for boost converter modeling from the viewpoint of observer design exist. The first is a non-linear model where y and d are observer inputs, and the second is a linear time-varying model where y and V_{in} are observer inputs.

In the systems where software controls the process (usually, digital control systems execute some software), the safety of software cannot be measured and proven. In control and automation processes, due to the use of software, one of the approaches that is recommended to increase the safety of the systems is the use of different methods and algorithms for one process to increase the redundancy and security of the system. For this reason, with respect to matters of security and safety, it is recommended to use observers that have a

completely different structure from the controllers in order to diagnose attacks and faults; if possible, the implementation methods for controller and observer must be different. The difference in the structure of controller and observer results in the fact that the smallest incompatibilities can be easily detected and catastrophic failures can be prevented.

For the observer, if we consider the system input as d, the system is modeled non-linearly, and if we consider the system input as $v_{in} = E$, the system becomes a linear system whose dynamic varies with time. This assumption is correct because the values of these two parameters are always available. Considering these cases, the system state equations can be written as (5).

In order to design an observer, the pairs (A,C) must be observable. Therefore, we form the visibility matrix as

$$Q = \begin{bmatrix} C \\ CA \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ \frac{1-d}{C_o} & \frac{-1}{RC_o} \end{bmatrix} \tag{13}$$

If the matrix Q is full rank, the system is fully observable. A matrix by dimension of 2×2 has full rank if its determinant is non zero. Thus,

$$\det(Q) = -\frac{1-d}{C_o} \tag{14}$$

This value for $d \neq 1$ is always the opposite of zero. Given that $0 < d < 1$ (in the simulation and experimental tests in this paper, d is about 0.3), this assumption holds. Therefore, the system is completely observable. In the following, we will estimate the system states by using the proposed observer structure.

$$\begin{aligned} &S = \hat{y}_{ij} - y_{ij} \\ &v = sgn(S) \\ &G = \begin{bmatrix} \beta \\ \gamma \end{bmatrix}, \begin{cases} \beta \in \mathbb{R}^{(np)\times p} \\ \gamma \in \mathbb{R}^{p\times p} \end{cases} \\ &\dot{\hat{x}}_{ij} = A_{ij}\hat{x}_{ij} + B_{ij}u_{ij} + Gv, \\ &\hat{y}_{ij} = C_{ij}\hat{x}_{ij} \end{aligned} \tag{15}$$

where S is the sliding surface, $\hat{x}_{ij}$ is an estimation for x_{ij}, A_{ij}, B_{ij}, C_{ij} are the observer matrix, u_{ij} is the input voltage for the boost converters (V_{in}). It describes the input voltage of the *ith* converter, which is used in the observer of Agent i, where this observer is located in Agent j, and Gv is a term for robustness. In this problem and for a new matrix definition, we have

$$y = Cx, \quad C = [0 \quad 1] \Rightarrow \quad \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ y \end{bmatrix} \tag{16}$$

and so

$$\dot{x}_i = A_i x_i + B_i u_i \Rightarrow \quad \begin{cases} \dot{x}_1 = A_{11}x_1 + A_{12}y + B_1 u \\ \dot{y} = A_{21}x_1 + A_{22}y + B_2 u \end{cases} \tag{17}$$

According to (15), for the observer, we have

$$Observer_{ij} : \begin{cases} \dot{\hat{x}}_{1_{ij}} = A_{11_{ij}}\hat{x}_1 + A_{12_{ij}}\hat{y}_{ij} + B_{1_{ij}}u_{ij} + \beta v \\ \dot{\hat{y}}_{ij} = A_{21_{ij}}\hat{x}_1 + A_{22_{ij}}\hat{y}_{ij} + B_{2_{ij}}u_{ij} + \gamma v \end{cases} \tag{18}$$

By calculation of estimation error as follows, we have

$$\begin{aligned} e(t) &= \begin{bmatrix} e_1(t) \\ e_y(t) \end{bmatrix} \\ \dot{e} &= \begin{bmatrix} \dot{e}_1 \\ \dot{e}_y \end{bmatrix} = \begin{bmatrix} \dot{\hat{x}}_{1_{ij}} - \dot{x}_1 \\ \dot{\hat{y}}_{ij} - \dot{y}_{ij} \end{bmatrix}, \quad \dot{y}_{ij} = \dot{y}_i + k_{at}\dot{f}_{ij}^{at} \\ &= \begin{bmatrix} A_{11_{ij}}\hat{x}_{1_{ij}} + A_{12_{ij}}\hat{y}_{ij} + B_{1_{ij}}u_{ij} + \beta v \\ A_{21_{ij}}\hat{x}_{1_{ij}} + A_{22_{ij}}\hat{y}_{ij} + B_{2_{ij}}u_{ij} + \gamma v \end{bmatrix} - \\ &\begin{bmatrix} (A_{11_{ij}}x_1 + A_{12_{ij}}y_{ij} + B_{1_{ij}}u_{ij}) \\ (A_{21_{ij}}x_1 + A_{22_{ij}}y_{ij} + B_{2_{ij}}u_{ij}) - k_{at}\dot{f}_{ij}^{at} \end{bmatrix} \end{aligned} \tag{19}$$

Thus, we have

$$\begin{aligned} \dot{e}_1 &= A_{11_{ij}}e_1 + A_{12_{ij}}e_y + \beta v \\ \dot{e}_y &= A_{21_{ij}}e_1 + A_{22_{ij}}e_y + \gamma v + k_{at}\dot{f}_{ij}^{at} \end{aligned} \tag{20}$$

There are two constraints for sliding mode control: first $\dot{e}_y = 0$ to stabilize the error dynamic, and when we are on the sliding surface, $e_y = 0$ must hold, so:

$$\begin{aligned} \dot{e}_y &= A_{21_{ij}}e_1 + A_{22_{ij}}e_y + \gamma v + k_{at}\dot{f}_{ij}^{at} = 0 \\ v &= \frac{-1}{\gamma}A_{21_{ij}}e_1 - \frac{k_{at}}{\gamma}\dot{f}_{ij}^{at} \end{aligned} \tag{21}$$

and

$$\begin{aligned} \dot{e}_1 &= A_{11_{ij}}e_1 + \frac{-\beta}{\gamma}A_{21_{ij}}e_1 - \frac{\beta k_{at}}{\gamma}\dot{f}_{ij}^{at} \\ \dot{e}_1 &= (A_{11_{ij}} - \frac{\beta}{\gamma}A_{21_{ij}})e_1 - \frac{\beta k_{at}}{\gamma}\dot{f}_{ij}^{at} \\ \dot{e}_1 &= F_{ij}e_1 + \dot{F}_{ij}^{at} \end{aligned} \tag{22}$$

In order for e_1 to be stable, $F_{ij} = A_{11_{ij}} - \frac{\beta}{\gamma}A_{21_{ij}} = \frac{-r}{L} - \frac{\beta}{\gamma}\frac{(1-d_i)}{C_o}$ must be stable, and then the error tends to zero. Therefore, by selection of β and γ, the error dynamics will be stable. The effect of an attack is $F_{ij}^{at} = -\frac{\beta k_{at}}{\gamma}f_{ij}^{at}$, where the derivation of it appears in the derivation error of state estimation.

5. Resilience Consensus Law

In order to achieve consensus when the system is faced with cyber attacks, the consensus law must be revised. The consensus law that is proposed in Equation (3) will be changed to the following equation. The outcomes of the attack observers are now incorporated into the consensus law as a result of this modification. Therefore, the attacked channels will be removed from the consensus protocol.

$$\begin{aligned} &\tilde{a}_{ij} = a_{ij}Tr(F_{ij}^{at}), \quad Tr(x) = \begin{cases} 0 & |x| > threshold \\ 1 & else \end{cases} \\ &x_{2i}^{d} = u_i(t_i) = \textstyle\sum_{v_j \in N_i} \tilde{a}_{ij}(t_i)[x_j(t_j - \tau_{ij}(t_i)) - x_i(t_i)] \end{aligned} \tag{23}$$

where x_{2i}^{d} is the desired output voltage for Agent i and $Tr(x)$ is a threshold function.

6. Simulation and Results

In this section, the efficiency of the proposed method has been validated via Simulink real-time (SLRT) simulations. The case study is a network of eight DC-DC boost converters with the non-linear dynamics that are linked as shown in Figure 4A. In this simulation, an

attempt is made to choose a graph that considers different modes of connection. In general, the consensus is achieved faster if there are few links between agents; however, it leads to lower reliability as well as more vulnerability to cyber attacks. The coordinating algorithm to achieve consensus becomes more complicated when a large number of communication links is devoted to the agreement process—that is, when the connectivity order of the graph is high, even though it results in greater reliability. Moreover, when the number of participating agents increases, a more complex coordinating algorithm is required. Different components, i.e., sensors and communication links, may be targeted by attackers. The speed of the attack propagation and the scale of the impact will differ; for example, aiming at agents with more connections will result in a faster and greater deviating effect on neighbors. To address this issue, in the proposed algorithm, the communication link that has been attacked is detected, and neglected from the agreement process. On the other hand, aiming at the input communication link of the agent with more neighbors has less effect on the overall graph since it has been removed from the agreement and there are still more inputs to achieve the goal. From a security viewpoint, a large number of connections is desirable because the attack impact is less and the attack is more likely detected. Therefore, for the proposed method, which is based on neglecting malicious input links, a large number of connections is more appropriate. To show the ability of the proposed method, a proper scenario is considered in which agents communicate with a maximum of four neighbor agents.

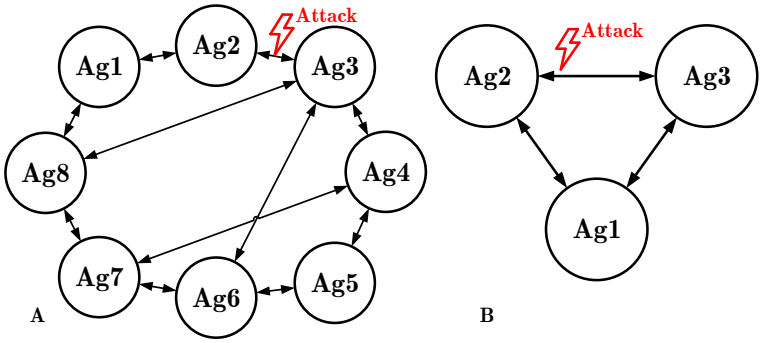

Figure 4. Graph topology: (**A**) eight boost agents for simulation scenario, and (**B**) three boost converters which communicate over the network for experimental test.

The goal of this paper is to achieve consensus in the output voltage of decentralized converters in the presence of FDIA. In the simulations, the parameters of converters are $E = 200$ V, $r = 1\ \Omega$, $C = 2.2$ mF, $L = 2.2$ mH, the load resistance $R = 60\ \Omega$ and the voltage reference is $V_{ref} = 315$ V. The parameters of the sliding mode controller are $\lambda_1 = 1$, $\lambda_2 = 2000$, $\lambda_3 = 0.5$ and the parameters of the observer are $\gamma = 1$ and the error pole is -600. To draw a comparison between conventional controllers and the proposed algorithm, two simulation scenarios are performed as follows.

First scenario: All the agents and communication links are healthy. The communication links are with $[1, 2, 3, 1, 1, 2, 1, 2]$ sample delay and they are synchronous. In the time stamp of 0.5 s, an FDIA occurs over the communication link from Agent 2 to Agent 3. As shown in Figure 5, the output voltage of Agent 2 which is delivered to Agent 3 is different from the real output voltage of Agent 2 due to a cyber attack that injects a false datum into the communication link L_{23}. Thus, the observer which is located in Agent 3, and estimates the states of Agent 2, follows the attacked voltage, which is different from the real output voltage of Agent 2. Figure 5 is shown for a better understanding of what is happening. This figure explains the attack effect on the communication data, which shows that when the output voltage of Agent 2 is at the steady state (blue color), an attack occurs at 0.5 s and the reported voltage over the communication link deviates from the output voltage of Agent 2 (red color). Therefore, the observer of Agent 2 that is located in Agent 3 follows the attacked value.

As shown in Figure 6, by the conventional consensus control law, agreement deviates from the normal condition and the FDIA cyber attack is successful. According to this figure, the output voltages of all agents will deviate because all of them are connected to each other by the communication links. In this scenario, when Agent 3 receives the wrong data, the controller regulates its output voltage to a false value, and this false value is sent to the other agents over the communication links.

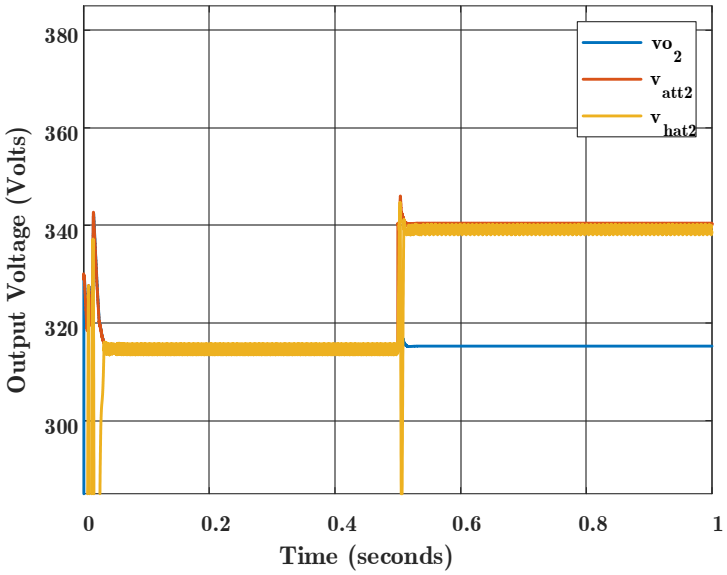

Figure 5. Voltage values for Agent 2, and the concept for what happens when an attack occurs; Vo_2 is the real output voltage for Agent 2, V_{att2} is the information about voltage of Agent 2 that is delivered over the communication link to Agent 3, which is manipulated by the false data injection attack, V_{hat2} is the voltage observer for Agent 2 that is located in Agent 3.

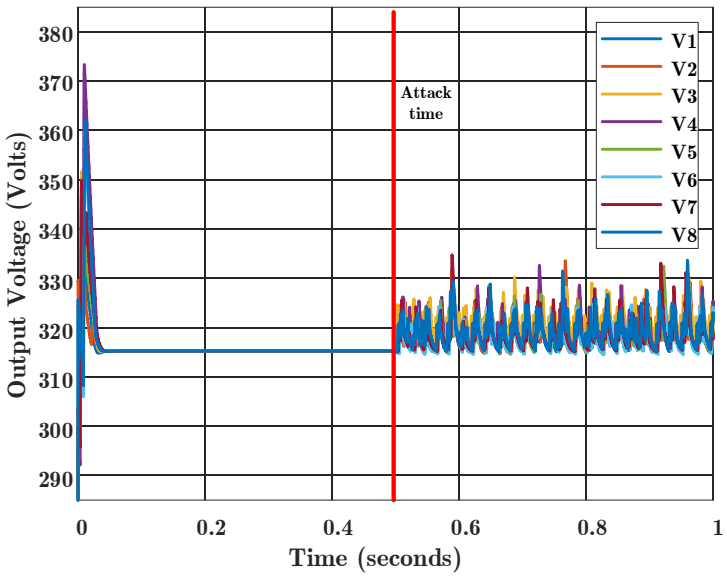

Figure 6. Output voltages of boost converters for conventional consensus algorithm in the presence of false data injection attack at time 0.5 s. The values of V_1 to V_8 are output voltages for Agent 1 to 8, respectively.

Second scenario: This scenario is the same as the first one, except that the consensus algorithm that is used to detect the attack is based on the developed algorithm in this paper. As shown in Figure 7, the voltages will reach consensus again immediately after the attack has occurred. Therefore, according to Figure 7, it is clear that the consensus will not deviate

from FDIA cyber attacks and the consensus process will be performed properly in the presence of this type of attack. As shown in this figure, the attack at Agent 3 affects the other agents. The proposed algorithm detects the source of the attack using residuals from the observer banks, and removes the attacked communication links from the consensus process. Therefore, it is shown that the proposed algorithm has resiliency or attack-tolerant control abilities.

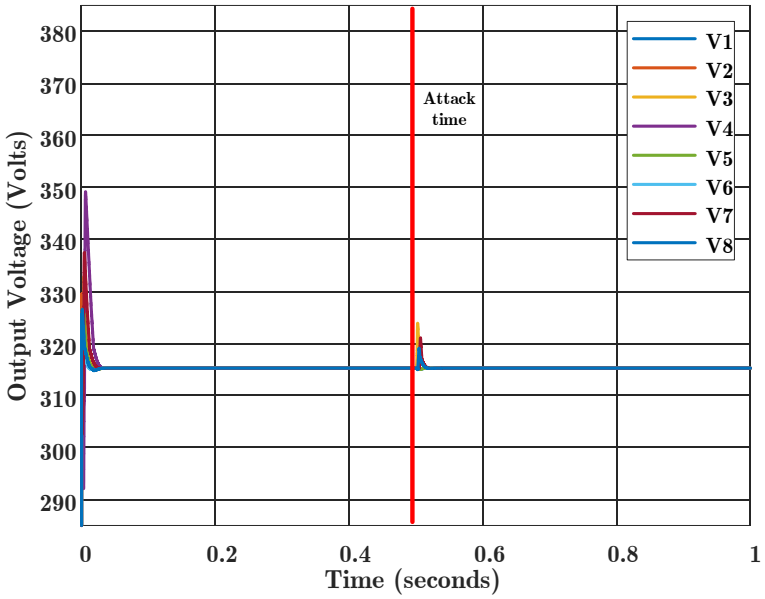

Figure 7. Proposed consensus algorithm results in the presence of false data injection attack at time 0.5 s. The values of V_1 to V_8 are output voltages for Agent 1 to 8, respectively.

7. Experimental Results

In order to validate the results, an experimental prototype with three agents is prepared according to the graph shown in Figure 4B and the hardware shown in Figure 8. Due to limited laboratory equipment, the number of agents is reduced to three, and the main reason is that the control board does not support more than three channels. However, a different control board with more channels can be utilized for practical implementation. Moreover, due to the fact that the laboratory power supplies have limited output voltages which are less than 30 volts, the operating voltage is reduced. However, it is worth noting that the nature of the experimental test is not different from the simulations.

This test-bench consists of: a development computer for FPGA and Microblaze programming by Xilinx-ISE and Xilinx-SDK softwares with a JTAG Xilinx programmer; a host computer to generate MATLAB codes, boot the target computer over the network, set-up and logging data from the target computer; a target computer that is booted by the Simulink real-time kernel and runs the tolerant consensus algorithm in real-time and communicates (Ethernet-UDP) with FPGA; a Spartan 6-based FPGA control board that is a controller and logger for the boost converters in an independent and very fast structure; three boost converters that are placed at the graph nodes and supply the hmic loads; three boost power supplies to supply the converters; three ohmic loads for three agents; three transmission ohmic loads between the agents to simulate the transmission power losses and a 100 Mbps Ethernet switch for connection between agents, host computer, and the target computer. In general, this testbed consists of three boost converters that are tied in a physical ring-bus network and a communication network. In order to implement three independent control loops for three agents, an FPGA Spartan 6 based board is used. This processor is connected to the target computer via a LAN-UDP connection link. For ease of programming and debugging, some local control loops are implemented in the Microblaze Xilinx-SDK environment. Boost converters are a 150 watt commercial type with a maximum operating voltage of 36 volts. Each agent consists of an ohmic load of

23 Ω, a boost converter with an efficiency of about 90%, a power supply with a voltage output about 17 volts, and 5 Ω transmission lines. The consensus control algorithm is implemented in the MATLAB software using Simulink real-time. Simulink and FPGA data are exchanging via the LAN connection link with 1 and 10 kHz times updates.

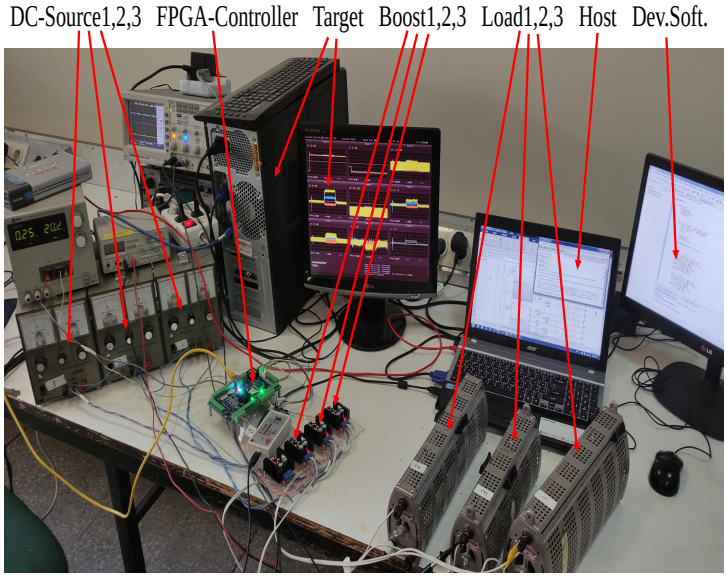

Figure 8. Experimental prototype for the validation of the proposed algorithm. This test-bench is composed of: development computer; host computer; target computer; Spartan 6 FPGA controller; three boost converters; three power supplies; three transmission loads, and a LAN switch.

According to Figure 9, the false data injection attack is aimed at the communication link L_{23} between $t = 1$ and $t = 2$ s. It is shown that for the conventional consensus algorithm, the output voltages of the converters deviate and consequently the consensus mechanism also is violated. Therefore, the conventional consensus algorithms are vulnerable in the presence of attacks. The attack occurs by injection of a fast ramp voltage from 24 to 28 volts into the L_{23} communication channel. Due to the fact that the converters are connected to each other through the 5 Ω power transmission lines, in practical applications, and in this experimental test, the output voltage measurement for each agent is affected by the other agents, and the voltage distribution is not ideally distorted. According to this figure, the maximum deviation is related to Agent 3, which is directly attacked. It is observed that after the end of the attack time, the consensus returned to its normal behavior.

Figure 10 also shows that with the proposed algorithm, the effect of the attack is eliminated and the consensus for the graph will occur correctly. This figure shows that the proposed tolerant consensus is resilient in the presence of the FDI attacks. It is shown that using the proposed algorithm after the attack has occurred, the attack is successfully detected and isolated, and then the attacked channel is removed from the consensus process to achieve the agreement. This amount of deviation at the start of the attack is shown in Figure 10, which is actually due to the fact that the detection process and the control loops are running in parallel. The cost that this method imposes on the system is the requirement of a larger computational burden compared to the conventional method, and also this method needs to know the model of each agent. It is worth noting that these costs are not comparable with the damages that may result due to cyber attacks.

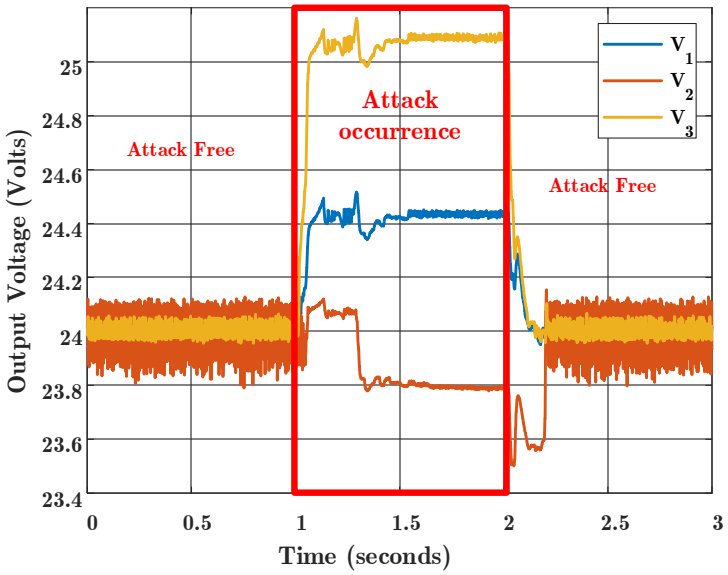

Figure 9. Experimental results for conventional consensus algorithm. FDI attack occurred at time 1 s and was removed at time 2 s.

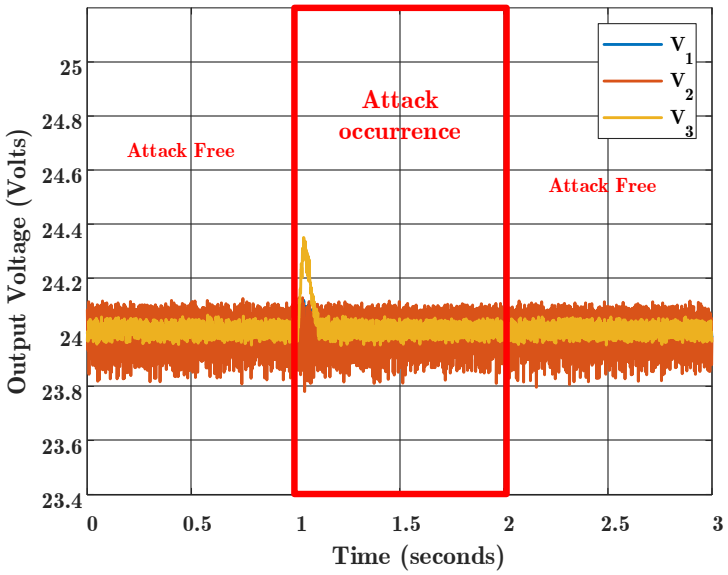

Figure 10. Experimental result for proposed consensus algorithm. FDI attack occurred at time 1 s and was removed at time 2 s.

8. Conclusions

In this study, an observer-based resilient control method was proposed to reach the consensus in a DC microgrid. In this microgrid, each agent is a battery-based boost converter and, at an unknown time, a false data injection attack appears. In order to control the voltage for each agent, the sliding mode control method has been used. To estimate the states of the neighboring agents, a bank of sliding mode observers has been proposed, which is organized to detect the attacks. If the states of the observers are not compatible with the communication data, the adjacency matrix will be modified with the correction values applied by the observers. The efficiency of the proposed method has been investigated by using simulations and experimental results. As a suggestion and continuation of the work in this paper, it is recommended that this method be extended for resiliency against stealth attacks. According to the results, it has been shown that by using the proposed method, the DC microgrid network will be resilient against false data injection attacks and the consensus will not deviate.

Author Contributions: Conceptualization, J.Z.; Formal analysis, R.R.-F., M.S. and V.P.; Investigation, Y.B.; Methodology, Y.B. and J.Z.; Project administration, R.R.-F. and M.S.; Resources, M.S.; Supervision, J.Z.; Visualization, V.P.; Writing—original draft, Y.B.; Writing—review & editing, R.R.-F. and V.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Sarrafan, N.; Rostami, M.A.; Zarei, J.; Razavi-Far, R.; Saif, M.; Dragicevic, T. Improved distributed prescribed finite-time secondary control of inverter-based microgrids: Design and real-time implementation. *IEEE Trans. Ind. Electron.* **2020**, *68*, 11135–11145. [CrossRef]
2. Saha, S.; Roy, T.K.; Mahmud, M.A.; Haque, M.E.; Islam, S.N. Sensor fault and cyber attack resilient operation of DC microgrids. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 540–554. [CrossRef]
3. Dragicevic, T.; Lu, X.; Vasquez, J.C.; Guerrero, J.M. DC Microgrids—Part I: A Review of Control Strategies and Stabilization Techniques. *IEEE Trans. Power Electron.* **2016**, *31*, 4876–4891. [CrossRef]
4. Vafamand, A.; Vafamand, N.; Zarei, J.; Razavi-Far, R.; Dragicevic, T. Intelligent Multi-objective NSBGA-II Control of Power Converters in DC Microgrids. *IEEE Trans. Ind. Electron.* **2021**, *68*, 10806–10814. [CrossRef]
5. Wu, J.; Lu, Y. Adaptive Backstepping Sliding Mode Control for Boost Converter With Constant Power Load. *IEEE Access* **2019**, *7*, 50797–50807. [CrossRef]
6. Chincholkar, S.H.; Jiang, W.; Chan, C.Y. An Improved PWM-Based Sliding-Mode Controller for a DC-DC Cascade Boost Converter. *IEEE Trans. Circuits Syst. II Express Briefs* **2018**, *65*, 1639–1643. [CrossRef]
7. Sarrafan, N.; Zarei, J.; Razavi-Far, R.; Saif, M.; Khooban, M.H. A Novel On-Board DC/DC Converter Controller Feeding Uncertain Constant Power Loads. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 1233–1240. [CrossRef]
8. Kowsari, E.; Zarei, J.; Razavi-Far, R.; Saif, M.; Dragičević, T.; Khooban, M.H. A Novel Stochastic Predictive Stabilizer for DC Microgrids Feeding CPLs. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *9*, 1222–1232. [CrossRef]
9. Andrés-Martínez, O.; Flores-Tlacuahuac, A.; Ruiz-Martinez, O.F.; Mayo-Maldonado, J.C. Nonlinear model predictive stabilization of DC–DC boost converters with constant power loads. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *9*, 822–830. [CrossRef]
10. Hernández-Márquez, E.; Silva-Ortigoza, R.; García-Sánchez, J.R.; Marcelino-Aranda, M.; Saldaña-González, G. A DC/DC Buck-Boost Converter-Inverter-DC Motor System: Sensorless Passivity-Based Control. *IEEE Access* **2018**, *6*, 31486–31492. [CrossRef]
11. Xu, Q.; Vafamand, N.; Chen, L.; Dragičević, T.; Xie, L.; Blaabjerg, F. Review on advanced control technologies for bidirectional DC/DC converters in DC microgrids. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *9*, 1205–1221. [CrossRef]
12. Sahoo, S.; Peng, J.C.H.; Devakumar, A.; Mishra, S.; Dragičević, T. On Detection of False Data in Cooperative DC Microgrids—A Discordant Element Approach. *IEEE Trans. Ind. Electron.* **2020**, *67*, 6562–6571. [CrossRef]
13. Olfati-Saber, R.; Fax, J.A.; Murray, R.M. Consensus and cooperation in networked multi-agent systems. *Proc. IEEE* **2007**, *95*, 215–233. [CrossRef]
14. Rahimi, N.; Binazadeh, T. Distributed robust consensus control for nonlinear leader–follower multi-agent systems based on adaptive observer-based sliding mode. *J. Vib. Control* **2019**, *25*, 109–121. [CrossRef]
15. Trip, S.; Cucuzzella, M.; Cheng, X.; Scherpen, J. Distributed averaging control for voltage regulation and current sharing in DC microgrids. *IEEE Control Syst. Lett.* **2019**, *3*, 174–179. [CrossRef]
16. Dibaji, S.M.; Pirani, M.; Flamholz, D.B.; Annaswamy, A.M.; Johansson, K.H.; Chakrabortty, A. A systems and control perspective of CPS security. *Annu. Rev. Control* **2019**, *47*, 394–411. [CrossRef]
17. Peng, C.; Sun, H.; Yang, M.; Wang, Y.L. A Survey on Security Communication and Control for Smart Grids under Malicious Cyber Attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1554–1569. [CrossRef]
18. Canaan, B.; Colicchio, B.; Abdeslam, D.O. Microgrid cyber-security: Review and challenges toward resilience. *Appl. Sci.* **2020**, *10*, 5649. [CrossRef]
19. Rana, M.M.; Li, L.; Su, S.W. Cyber attack protection and control of microgrids. *IEEE/CAA J. Autom. Sin.* **2018**, *5*, 602–609. [CrossRef]
20. Hassani, H.; Razavi-Far, R.; Saif, M.; Zarei, J.; Blaabjerg, F. Intelligent Decision Support and Fusion Models for Fault Detection and Location in Power Grids. *IEEE Trans. Emerg. Top. Comput. Intell.* **2021**. [CrossRef]
21. Saeedi, M.; Zarei, J.; Razavi-Far, R.; Saif, M. Event-Triggered Adaptive Optimal Fast Terminal Sliding Mode Control Under Denial-of-Service Attacks. *IEEE Syst. J.* **2021**. [CrossRef]

22. Sahoo, S.; Mishra, S.; Peng, J.C.H.; Dragicevic, T. A Stealth Cyber-Attack Detection Strategy for DC Microgrids. *IEEE Trans. Power Electron.* **2019**, *34*, 8162–8174. [CrossRef]
23. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans. Control Netw. Syst.* **2014**, *1*, 370–379. [CrossRef]
24. Barzegari, Y.; Zarei, J.; Razavi-Far, R.; Saif, M. Consensus of First Order Multi-agent Systems with Actuator or dynamic Fault by weighted adjacency matrix approach (WAMA). In Proceedings of the 2021 7th International Conference on Control, Instrumentation and Automation (ICCIA), Tabriz, Iran, 23–24 February 2021; pp. 1–6.
25. Zhou, Q.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids. *IEEE Trans. Smart Grid* **2020**, *11*, 3690–3701. [CrossRef]
26. Dolk, V.S.; Tesi, P.; De Persis, C.; Heemels, W.P. Event-triggered control systems under denial-of-service attacks. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 93–105. [CrossRef]
27. Nikmehr, N.; Moghadam, S.M. Game-theoretic cybersecurity analysis for false data injection attack on networked microgrids. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 365–373. [CrossRef]
28. Cintuglu, M.H.; Ishchenko, D. Secure distributed state estimation for networked microgrids. *IEEE Internet Things J.* **2019**, *6*, 8046–8055. [CrossRef]
29. Gallo, A.J.; Turan, M.S.; Boem, F.; Parisini, T.; Ferrari-Trecate, G. A Distributed Cyber-Attack Detection Scheme with Application to DC Microgrids. *IEEE Trans. Autom. Control* **2020**, *65*, 3800–3815. [CrossRef]
30. Diaconis, P.; Bollobas, B. *Modern Graph Theory; Graduate Texts in Mathematics*; Springer: New York, NY, USA, 2000; Volume 95, p. 1377. [CrossRef]
31. Dolk, V.S.; Postoyan, R.; Heemels, W.P. Event-Triggered Consensus for Multi-Agent Systems with Guaranteed Robust Positive Minimum Inter-Event Times. In Proceedings of the 2019 IEEE 58th Conference on Decision and Control (CDC), Nice, France, 11–13 December 2019; pp. 2604–2609.
32. Teixeira, A.; Pérez, D.; Sandberg, H.; Johansson, K.H. Attack models and scenarios for networked control systems. In Proceedings of the HiCoNS'12—1st ACM International Conference on High Confidence Networked Systems, Beijing China, 17–18 April 2012; ACM Press: New York, NY, USA, 2012; pp. 55–64. [CrossRef]
33. Utkin, V. Sliding mode control of DC/DC converters. *J. Frankl. Inst.* **2013**, *350*, 2146–2165. [CrossRef]
34. Askari, M.R.; Zarei, J.; Razavi-Far, R.; Saif, M. Robust Terminal Sliding Mode Observer-Based Sensor Fault Estimation for Uncertain Nonlinear Systems. In Proceedings of the 2020 IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 24 August–20 September 2020; pp. 1–6.