



AALBORG UNIVERSITY
DENMARK

Aalborg Universitet

Self-Healing Secure Blockchain Framework in Microgrids

Rath, Suman; Nguyen, Lam Duc; Sahoo, Subham; Popovski, Petar

Published in:

I E E E Transactions on Smart Grid

DOI (link to publication from Publisher):

[10.1109/TSG.2023.3253723](https://doi.org/10.1109/TSG.2023.3253723)

Publication date:

2023

Document Version

Accepted author manuscript, peer reviewed version

[Link to publication from Aalborg University](#)

Citation for published version (APA):

Rath, S., Nguyen, L. D., Sahoo, S., & Popovski, P. (2023). Self-Healing Secure Blockchain Framework in Microgrids. *I E E E Transactions on Smart Grid*, 14(6), 4729-4740. <https://doi.org/10.1109/TSG.2023.3253723>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy

If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Self-Healing Secure Blockchain Framework in Microgrids

Suman Rath, *Graduate Student Member, IEEE*, Lam Duc Nguyen, *Member, IEEE*,
Subham Sahoo, *Senior Member, IEEE* and Petar Popovski, *Fellow, IEEE*

Abstract—Blockchain has recently been depicted as a secure protocol for information exchange in cyber-physical microgrids. However, it is still found vulnerable to consensus manipulation attacks. These *stealth* attacks are often difficult to detect as they use kernel-level access to mask their actions. In this paper, we firstly build a trusted and secured peer-to-peer network mechanism for physical DC microgrids’ validation of transactions over Distributed Ledger. Secondly, we leverage from a physics-informed approach for detecting malware-infected nodes and then recovering from *stealth* attacks using a self-healing recovery scheme augmented into the microgrid Blockchain network. This scheme allows compromised nodes to adapt to a reconstructed trustworthy signal in a multi-hop manner using corresponding measurements from the reliable nodes in the network. Additionally, recognizing the possible threat of denial-of-service attacks and random time delays (where information sharing via communication channels is blocked), we also integrate a model-free predictive controller with the proposed system that can locally reconstruct an expected version of the attacked/delayed signals. This supplements the capabilities of Blockchain, enabling it to detect and mitigate consensus manipulation attempts, and network latencies.

Index Terms—Blockchain, Microgrids, Cybersecurity, Self-Healing Mechanism.

I. INTRODUCTION

RECENT attempts to develop more efficient DC microgrid systems can be attributed to their inherent cyber-physical capabilities that allow the smooth integration of renewable energy sources (RESs), multiple electronic devices (loads) and a variety of storage devices in both, the autonomous as well as the grid-connected mode of operation. Such systems can have three different types of control structures - centralized, distributed, and decentralized. The distributed control framework is generally preferred over the other control structures as it is resilient to single-point failures, thus enabling more reliability and better scalability [1]. Moreover, distributed control structures have a higher degree of tolerance to unavoidable cyber issues like network latency, packet losses, and communication link failures. However, these control structures can not be

considered fully *reliable* as the distributed framework can only enable partial information availability (limited to neighboring units), which in turn, makes the microgrid vulnerable to unauthorized manipulation of sensors and actuators [1]. Since cyber-physical DC microgrids are integral components of mission-critical systems (e.g., electric aircraft, hospitals, military bases, etc.), it is essential to protect them from adversarial cyber attacks.

Networked microgrids, which may function either in the independent mode or in collaboration with the rest of the network, can complicate the distribution system’s operation. Conventionally, through supervisory control and data acquisition (SCADA), microgrids are often controlled in a centralized manner [2]. In particular, the network data is gathered, recorded, and then processed at a centralized server. Considering the rapidly growing size and speed of the measurement data, collecting and processing such a wide-range network in real-time at a single server leads to overload for the centralized node and a single point of failure problem. Centralized networks would also be vulnerable to single-point attacks as hackers would only need to target the central host computer server to compromise the entire network, as this is the single point that issues control commands to all the other nodes [3]. In contrast, attacking a distributed network is more challenging for attackers, especially for the power grid that is distributed over a geographically wide-range area. Hence, the computation and the trust are distributed over the network, which can be useful for achieving a more secure power network.

In this regard, as the energy sector needs significant time reduction for the management of economic transactions and the possibility of getting rid of third-party authorities [4], the concept of *transactive energy* has appeared as one of the most interesting technologies since the 2017 Gartner Hype cycle [5]. There is a need to switch from a centralized energy system with intermediary components to a decentralized system that can detach the related financial transactions from the centralized energy control unit. For example, the authors in [6] introduced an approach using Blockchain technology for handling loss allocation and a timing mechanism for transacting intended energy exchanges and losses.

A type of Distributed Ledger Technology (DLT) known as Blockchain consists of blocks, which are lists of data items that are constantly growing. Transactions of all kinds, including those involving money, energy, transportation, data, logic, and even programs, can be recorded in blocks. Blocks are tied together in chronological order, timestamped, unchangeable, and verifiable. Every DLT node keeps a copy of the ledger,

This work is partly supported by the Baltic-Nordic Energy Research programme via Next-uGrid project and partly by the Villum Investigator Grant WATER from the Velux Foundation, Denmark.

Suman Rath is with the Department of Computer Science and Engineering, University of Nevada, Reno, NV 89557, USA (e-mail: srath@nevada.unr.edu)

Lam Duc Nguyen is with Software Systems Research Group, CSIRO’s Data61, Sydney 2015, Australia. (e-mail: lam.nguyen@data61.csiro.au)

Subham Sahoo is with the Department of Energy, Aalborg University, 9220 Aalborg, Denmark (e-mail: ssa@energy.aau.dk).

Petar Popovski is with the Department of Electronic Systems, Aalborg University, 9220 Aalborg, Denmark. (e-mail:petarp@es.aau.dk)

and any changes to the blocks' content or order are quickly detected by a check of the authenticity of the blocks. Among the concerned untrusted parties, Blockchain encourages immutable and transparent information sharing [7]. DLTs are viewed as a crucial enabler for trustworthy and dependable distributed observation systems in addition to their function in financial transactions. DLTs' authentication procedure depends on network consensus across numerous nodes. Blockchain technology is a noteworthy invention that can be applied in various microgrid domains.

Recently, Blockchain has become more popular in the integration with microgrids. There are several prominent applications of Blockchain technologies in microgrids, e.g., peer-to-peer energy trading [8], energy exchange [9], electric vehicle charging [10]. Besides, several start-ups and companies have applied Blockchain technologies in microgrids system for managing and sharing energy as well as building innovative products, e.g., the energy market of PowerLedger [11], a decentralized data exchange platform for energy sector GridSingularity [12]. More applications of Blockchain in microgrids can be found in [13]. The authors in [14] have discussed a Blockchain-based scheme for secure energy transactions. In conventional Blockchain-based schemes, the trustworthiness of each block is decided through a consensus-based mechanism where the majority of nodes in the system must agree on its validity. Such schemes are often vulnerable to 51% attacks [15]. In general, 51% attacks refer to an attack strategy where the hacker can access the system's internal mining capabilities and use this access to mine compromised blocks. Further, this access is also used to manipulate the consensus-based validation strategy by forcing individual nodes to stop the confirmation of authentic blocks and make them validate fabricated blocks generated by the attacker itself. 51% attacks can be executed using stealthy, kernel-level malware like rootkits [16].

Although the Blockchain¹ is being used in many power electronic applications, it is also essential to evaluate whether Blockchain could be a feasible tool for exchanging voltage/frequency control signals in the microgrid test system. This evaluation is essential because, even though the Blockchain is an essential tool for cyber-secure control, the time delay created as a consequence of mining new blocks may have a detrimental effect on microgrid stability [17]. Mahmud *et al.* in [18] have proposed the use of Blockchain for control in microgrids with distributed energy resources and presented results showing that the proposed framework can perform well even under time delays. However, the current studies have not addressed how to prevent stealth & hijacking attacks in their proposed control mechanism.

The conventional control framework in cyber-physical microgrids critically relies on a centralized database and communication channels, both of which are vulnerable to adversaries to manipulate the system operation. An effective solution for countermeasures is the detection and mitigation

of such threats. However, mitigation techniques may be vulnerable to adversarial attacks designed with knowledge of the system dynamics (e.g., adversarial attacks on learning-based anomaly detectors, reward poisoning attacks against reinforcement learning, etc.). Hence, a significantly better approach is the prevention of these threats in the first stage itself. Since the DLT technology offers great potential due to its advanced data protection and attack prevention capabilities based on the natural security strength of the cryptographic system and consensus mechanism [19], we propose to augment these salient features of the DLT into the dynamic physical properties of microgrids to enhance its resiliency against cyber-attacks (along with physics-informed attack detection metrics to identify any type of consensus-manipulating attack vector that tries to inject false data into the network). To recover from such attacks upon detection, we introduce a self-healing recovery mechanism for Blockchain-based microgrids that: i) provides a transparency and immutability microgrids system; ii) addresses the *garbage-in garbage-out* problem of the current Blockchain-based systems.

To summarize the key features, the contributions of this paper are as follows:

- Firstly, we formulate a general model of a DLT-based transactive DC microgrid system, including infrastructure and security mechanisms.
- Secondly, we evaluate the response of the general Blockchain model to stealth attacks and propose the addition of new physics-informed detection metrics based on the secondary control dynamics of each node to identify such attacks and alleviate the detection accuracy of DLT.
- Finally, we also present a self-healing recovery mechanism in the form of a reconstructed signal to compensate for any compromised data/signal at any node. This recovery mechanism is independent of the physical topology of multiple converters, and will always provide system resiliency, provided at least one node in the network is trustworthy. The presented strategy is resilient against several attack variants and potential network issues including FDIA, denial-of-service (DoS), and random communication delays.

The remainder of this paper is organized as follows. In Section II, we introduce the background knowledge of DLTs/Blockchain and the integration of Blockchain into microgrids. Section III highlights the operating principles and security issues in cyber-physical microgrids. Section IV presents the Blockchain-based strategy adopted for cyber-secure control in the DC microgrid. The effectiveness and robustness of the proposed strategy to illustrate its resilient behavior under different attack scenarios and physical topologies of microgrids are presented in Section V. Experimental results demonstrating the robustness of the proposed self-healing strategy are presented in Section VI. Finally, Section VII presents the conclusion of the paper.

¹Throughout this article, the words DLT and *Blockchain* will be used interchangeably. Blockchains are a particular sort of DLT where each node keeps a copy of the ledger, and chains of blocks are made up of digital pieces of information called transactions.

II. BACKGROUND KNOWLEDGE

A. DLTs/Blockchain Concept

A Distributed Ledger Technology (DLT) system provides a distributed, tamper-proof ledger that is spread throughout a network of interacting nodes, which share a common initial block of data known as the genesis block [20]. When publishing data to the ledger, each node adds data formatted in the form of transactions in a block that also contains a pointer to its preceding block. This produces a chain of blocks, or "Blockchain," referred to as the Blockchain. To receive a reward, a block that is generated by a particular node often needs to solve a mathematical crypto-puzzle [21] and provide the result as evidence of its effort. Mining is the name of this process. The network's overall computing or mining power changes the crypto-level puzzles of difficulty. Since every DLT node in the network maintains a copy of all committed transactions in the ledger, every transaction recorded in the distributed ledger is practically unchangeable [22]. Additionally, the integrity of the data blocks in the DLTs is ensured by cryptographic methods, including hash functions, asymmetric encryption algorithms, and digital signatures. As a result, the DLTs can guarantee transaction non-repudiation. Each transaction is also timestamped historically and given a unique ID, allowing each user to be assigned to it. The life cycle of a transaction in DLT-based networks is explained in detail in Fig. 1. Blockchain clients, e.g., physical devices and home alliances, generate or collect data, and transform it into Blockchain transaction format. The transactions are subsequently put into blocks, which are validated by peers via the mining process. In the distributed ledger, the transactions are finally immutably recorded and accessible to clients. After the transactions are recorded in the distributed ledger, they can be queried by clients.

B. Cyber Attacks on Microgrids

Blockchain is regarded as a typical distributed data storage system and encompasses a number of other technologies as well, including decentralization, distributed consensus procedures, and cryptography. Blockchain has been studied in both research and applications due to the benefit of creating safe, dependable, and decentralized autonomous ecosystems for a variety of scenarios [23]. Blockchain is suited for applications involving the security protection of cyber-physical systems (CPSs) because it is a novel and fundamental technical feature.

Recent cyber attacks against critical physical systems, for example, the attacks on the Ukrainian power grid in 2015-2016, have motivated multiple studies on security and privacy aspects for cyber-physical systems, particularly the power grid [24]. The work in [25] demonstrated that *false data injection* (FDI) could inject data measurements to induce error in the operation of the power system. A malicious attacker can also affect forecast systems, which are used to plan the operation and activities of power systems by exploiting vulnerabilities of artificial intelligence models [26]. In general, FDI attacks need to gather information about the current state of the system or the models used for making decisions, for example, the state of

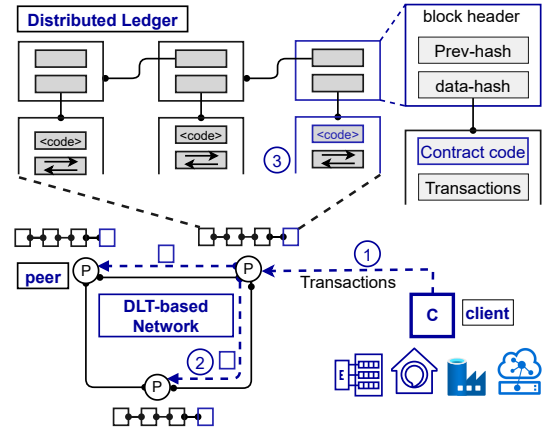


Fig. 1. Schematic of a DLT-based system.

the system, topology structure, or machine learning prediction models [27].

Besides, the attacker also exploits the lack of security mechanisms of embedded IoT sensors [16] to affect the operation of power grid systems. The target of adversaries could be embedded sensors such as environmental sensors, smart meters, appliances, or end-user systems to affect the power systems. The authors in [28] introduced a novel form of attack named manipulation of demand via IoT and documented that if an attacker compromised thousands of nodes, they could cause various problems to the power grid, including line failures, frequency instabilities, increased operating costs. In another aspect, the adversaries can compromise IoT devices responsible for communicating or exchanging data and payments with other power systems by changing their bids [29]. In the scope of this work, we propose to augment the physical properties, dynamics, and principles of microgrid operation into Blockchain-based attack detection and mitigation.

III. CYBER-PHYSICAL MICROGRIDS

A. Operating Principle

A single-line diagram depicting a cyber-physical DC microgrid network with $N = 4$ sources and corresponding DC/DC buck converters is shown in Fig. 2. Each source with the corresponding converter is called an *agent*. Further, the agents are connected to each other via transmission lines. Besides the physical interconnections, the agents are also connected to one another through a communication network that aids in the exchange of information between themselves. The information received from the communication network is fed as input to the local controller associated with each agent. As shown in Fig. 2, the local control framework consists of voltage and current controllers for the management of the DC/DC converter. Apart from that, the secondary control framework consists of an average voltage regulator for facilitating the regulation of global voltage, and a current regulator to achieve proportionate load sharing through the imposition of voltage offsets from each of the layers.

An undirected, interconnected graph of cyber elements is shown in Fig. 2. In this graph, the nodes represent the

agents, and are denoted by $\mathbf{x} = \{x_1, x_2, \dots, x_N\}$. The nodes are connected to each other using edges through an associated adjacency matrix, $\mathbf{A}_G = [a_{kj}] \in R^{N \times N}$, where the communication weight (represented by a_{kj} , i.e., from node j to node k) is formulated as: $a_{kj} > 0$, if $(\psi_k, \psi_j) \in \mathbf{E}$, where \mathbf{E} represents an edge connecting two different nodes, with ψ_k and ψ_j representing a local node and its neighboring node, respectively. If the cyber link connecting ψ_k and ψ_j is absent, $a_{kj} = 0$. In this framework, an agent (say at ψ_k node) shares local voltage and current measurements with its neighbors $N_k = \{j \mid (\psi_j, \psi_k) \in \mathbf{E}\}$. The matrix showing input and output information can be represented as $\mathbf{D}_{in} = \text{diag}\{d_k^{in}\}$ and $\mathbf{D}_{out} = \text{diag}\{d_k^{out}\}$ respectively, where, $d_k^{in} = \sum_{j \in N_k} a_{kj}$ and $d_k^{out} = \sum_{i \in N_j} a_{jk}$. Combining the transmitted and received information, a single Laplacian matrix can be obtained, which is denoted by $\mathbf{L} = [l_{kj}]$. The elements of the matrix are represented by l_{kj} and obtained using $\mathbf{L} = \mathbf{D}_{in} - \mathbf{A}_G$.

As previously mentioned, the role of the cooperative control framework is to achieve average global regulation and proportional sharing of load current. To fulfill these objectives, a reference value of the voltage setpoint is determined through the use of two voltage correction terms, as defined below:

$$\Delta V_{1k}(t) = K_P^{H1} (V_{dcref} - \bar{V}_i(t)) + K_I^{H1} \int (V_{ref} - \bar{V}_k(t)) dt \quad (1)$$

$$\Delta V_{2i}(t) = K_P^{H2} \delta_k(t) + K_I^{H2} \int \delta_k(t) dt \quad (2)$$

where \bar{V}_i represents the estimated average value of the voltage at the i^{th} agent; V_{ref} represents the nominal value of voltage; δ_k represents the current mismatch error (in (4)) for the k^{th} agent between the local per-unit output current and the neighbors' per-unit output current. The output from the voltage observer and power-sharing controller in Fig. 3 can be mathematically depicted as:

$$\bar{V}_k(t) = V_k(t) + \int \sum_{j \in N_k} a_{kj} (\bar{V}_j(t - \tau) - \bar{V}_k(t - \tau)) dt \quad (3)$$

$$\delta_k(t) = \sum_{j \in N_k} ca_{kj} \left(\frac{I_j(t - \tau)}{I_j^{max}} - \frac{I_k(t - \tau)}{I_k^{max}} \right) \quad (4)$$

where, τ is the communication delay between the k^{th} & the j^{th} agent and c represents the coupling gain. Further, I_k and I_j , I_k^{max} and I_j^{max} represent the measured and the maximum output currents for the k^{th} and the j^{th} agent, respectively.

The local reference value of voltage V_k^* for the k^{th} agent, determined by using the two voltage correction terms as depicted in (1)-(2) can be given by:

$$V_k^*(t) = V_{ref} + \Delta V_{1k}(t) + \Delta V_{2k}(t). \quad (5)$$

For a well-connected cyber graph in a networked DC microgrid, based on the cooperative consensus algorithm, the global control objectives can be given by:

$$\lim_{k \rightarrow \infty} \bar{V}_k(t) = V_{ref}, \quad \lim_{k \rightarrow \infty} \delta_k(t) = 0. \quad \forall k \in N \quad (6)$$

TABLE I
STEALTH ATTACKS IN DC MICROGRIDS IN [1] AND [30]

Affected Counterparts	Modeling
Voltage [1]	$\mathbf{W}x_{attack}^V = 0$
Current [30]	$\mathbf{W}x_{attack}^I = 0$

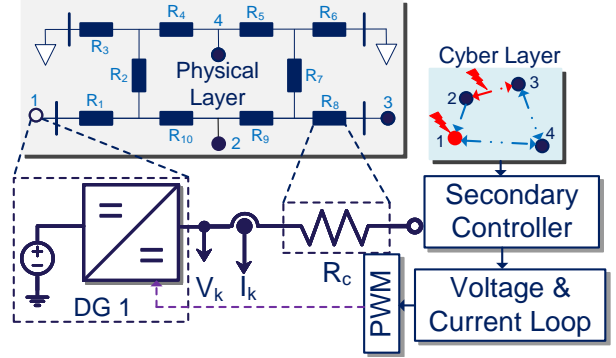


Fig. 2. Networked DC microgrid with $N = 4$ distributed generations (DGs) operating with a cooperative ring-based cyber graph.

B. Cybersecurity Issues

Fig. 2 shows how malicious attackers may inject false data into the sensors, actuators, controllers and other cyber devices in the DC microgrid system to disrupt the objectives depicted in (6). These attacks may also be performed in a coordinated fashion in order to deceive microgrid system operators and hide the actions of the attack vector by adding additional inputs in (3)-(4), as given by:

$$\mathbf{u}^a(t) = \mathbf{L}\mathbf{x}(t) + \mathbf{W}\mathbf{x}_{attack} \quad (7)$$

where, \mathbf{u}^a is the vector representation of the manipulated control input $u_k^a = \{u_k^{Va}, u_k^{Ia}\}$. Further, \mathbf{x}_{attack} and $\mathbf{x} = \{\bar{\mathbf{V}}, \mathbf{I}\}$ represent the attack elements $x_{attack_i} = [x_{attack_k}^V, x_{attack_k}^I]^T$ and the non-compromised measurements, respectively. Moreover, the attack distribution matrix $\mathbf{W} = [w_{kj}]$ represents row-stochasticity, where its elements can be given by:

$$w_{kj} = \begin{cases} \frac{1}{N_k + 1}, & j \in N_k \\ 1 - \sum_{j \in N_k} w_{kj}, & j = k \\ 0, & j \notin N_k, j \neq k \end{cases} \quad (8)$$

The detection strategies for both the stealth attacks (in Table I) are provided in Table II. More details on its formulation can be referred from [1] and [30]. As it can be seen in Table II that since the detection strategies primarily depend on local as well as neighboring measurements, this leaves a tactical opportunity for an attacker to infiltrate the communicated measurements used for the design of the detection strategies. As a result, such consecutive intrusion may affect the detectability of these attacks when the criteria in Table II are not met.

For more clarity, a case study is performed in a DC microgrid system with $N = 4$ agents, as shown in Fig. 4 to demonstrate the performance of detection criteria for a stealth attack on voltages and currents, respectively. In Fig. 4, after the stealth attack is initiated on currents, it can be seen that the output currents of each agent are anyway

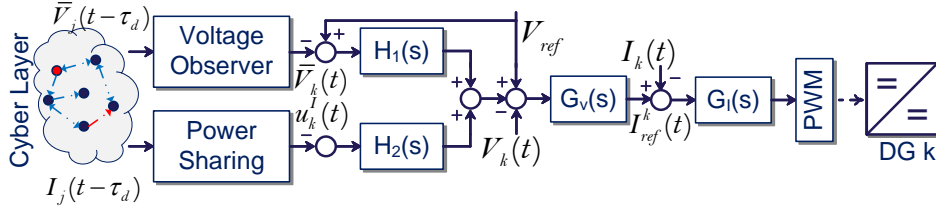


Fig. 3. Distributed controller for microgrids under consideration in k^{th} DG.

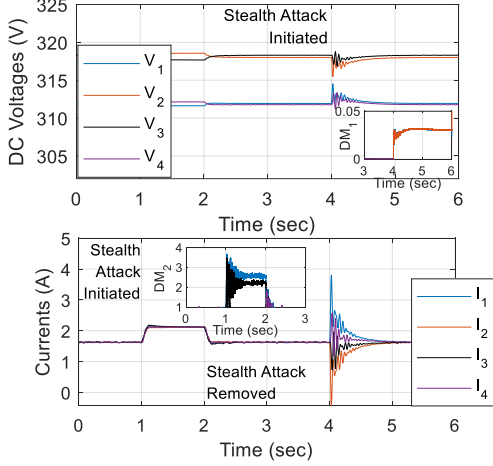


Fig. 4. Performance of detection strategies in response to stealth attack on current and voltages at $t = 1-2$ sec and 4 sec, respectively – the detection strategies can further be manipulated.

shared equally. However, the detection mechanism for current measurements suggests that DM_2^1 and DM_2^3 are positive, which indicate compromised current measurements for agent I and III. Further at $t = 4$ sec, a balanced set of attack elements $\{-15, 0, 15, 0\}$ V are introduced in the voltage control input values (as shown in Fig. 4) on the basis of the attack strategy depicted in [1]. Despite the presence of attack elements, the voltages return back to pre-attack set points. However, the corresponding detection metric DM_1 for agents I and II immediately goes positive. Under these circumstances, if the communicated measurements $x_j(t)$ in (1) are manipulated by the cyber-attacker with considerable knowledge of the detection strategy, there is a possibility that the cyber attack alarm might be disinforming. This mandates a secure mechanism of information exchange between each agent so that the communicated variables used in the proposed detection approach remain uncompromised. Following an accurate scanning of the compromised measurement, the corresponding countermeasures can be applied without any false alarms.

IV. BLOCKCHAIN FOR SECURITY OF MICROGRIDS

In this section, we present our self-healing Blockchain-based communication model for the cyber-physical microgrid shown in Fig. 2. We propose a distributed DLT, where the nodes can communicate and collaborate to identify attacked counterpart(s) in a reliable and trustworthy manner. The DLT-based network consists of nodes connected via the P2P model.

TABLE II
DETECTION CRITERIA FOR STEALTH ATTACKS IN TABLE I

Stealth Attack	Detection Criteria for k^{th} Agent	Terminology
Voltage [1]	$h_k^1 [\sum_{j \in N_k} a_{kj} (\Delta V_{1j} - \Delta V_{1k})]$ $[\sum_{j \in N_i} a_{kj} (\Delta V_{1j} + \Delta V_{1k})] > \Upsilon_1$	DM_1^k
Current [30]	$c_k [\sum_{j \in N_k} a_{kj} (I_{in_{ref}}^j - I_{in_{ref}}^k)]$ $[\sum_{j \in N_k} a_{kj} (I_{in_{ref}}^j + I_{in_{ref}}^k)] > \Upsilon_2$	DM_2^k

¹ h_k is a positive quantity used for i^{th} agent.

² c_k is another positive quantity. $I_{in_{ref}}^k$ represents the value of input current reference for the k^{th} agent.

Basically, nodes connect using a unique address and use the gossip protocol to exchange network information such as blocks, transactions, and addresses. In DLT-based networks, there are specific nodes called miners responsible for extending the Blockchain by creating new blocks [31]. In the scope of this research, each node aggregates sensor measurement values (in its area) and analyzes them. Further, each of them estimates the local update and exchanges signal values with the other nodes, engages in distributed consensus procedures, and publishes to the distributed ledger in its local memory.

A. System Model

We consider the DLT-based microgrid system with M communication channels and N physical agents. The system states have already been defined as $x_i(t) = \{V_k(t), I_k(t), DetV_k(t-1), DetI_k(t-1)\}$. The measurements $y_i(t) = \{V_k(t), I_k(t), DetV_k(t-1), DetI_k(t-1)\}$ can be measured from every agent. The microgrid is modeled as a discrete-time linear dynamic system, as given below:

$$x_t = \mathbf{A}x_{t-1} + v_t \quad (9)$$

$$y_t = \mathbf{H}x_t + w_t \quad (10)$$

where $\mathbf{A} \in R^{(2N-1) \times (2N-1)}$ and $\mathbf{H} \in R^{K \times 2N-1}$ represent the state transition and the measurement matrices respectively. Further, $v_t = [v_{1,t}, \dots, v_{2N-1,t}]^T$ and $w_t = [w_{1,t}, \dots, w_{K,t}]^T$ represent the process noise and the measurement noise vectors respectively. It is assumed that w_t and v_t are independent AWGN processes, where $w_t \sim \mathcal{N}(0, \sigma_w^2 I_K)$ and $v_t \sim (0, \sigma^2, I_{2N-1})$.

For a secure and reliable state update among DLT-based nodes, it is essential to guarantee that the previous values of the state estimate are not modified, the physical agent measurement is non-anomalous, and the operation of the DLT nodes adheres to the predefined agreements. In case

the network is attacked, the state estimate values can be recovered through the use of previous reliable state estimations that also require the protection of preceding state estimation values against tampering. On the one hand, in a DLT-based network, malicious adversaries can obtain illegitimate access to the system, for example, via trojan propagation, stealing the identity of involved nodes, leading the nodes to get faulty updates during the operation of the system. On the other hand, as the characteristic of DLT is completely distributed, there is no single trustworthy central entity to take control and verify whether the other nodes are reliable and safe, e.g., if the involved nodes are operating as per pre-defined roles. Hence, a distributed authentication mechanism is needed to detect misbehaving nodes.

B. Detection Model

In a DLT-based microgrid network, even though the whole system is fully distributed, attackers can still manipulate the system dynamics if they can achieve control of the majority of the individual nodes, which gives them access to more than half of the hashing/computational power. This scenario can be used to manipulate consensual query decisions to introduce false data into sensors/communication links in the system [15], [25]. In certain cases, the attackers may also create a *fork*, extracting specific transactions, tampering with them, and injecting them back as *True* packets. Since these attack vectors were designed to prey on the vulnerability of the conventional DLT framework, we integrate system-specific knowledge into the DLT setup enabling it to recognize violations in microgrid dynamics to identify false data disrupting the secondary controller synchronization among nodes. The generated data from individual nodes are formatted in Blockchain-based transactions and synchronized among them. The detection criteria as mentioned in Table II are in the form of mismatch error margins (represented by the metric DM^k) between parameter data (measurements) from the distributed nodes. When an attack vector stealthily manipulates transactions, the detection metric DM^k increases beyond the threshold value Υ predefined in the smart contract, enabling autonomous attack detection using the physics-informed attack detection metrics in Table II. A more elaborate explanation of the integrated setup including the self-healing process is depicted in the next subsection.

C. Self-healing recovery

The self-healing process designed to enable recovery of compromised nodes in the DLT-microgrid framework is part of an integrated setup including both attack detection and mitigation. Any transaction performed by a node, leading to the generation of a new block of data is broadcast to the rest of the network through a secure sharing scheme. The network uses the recipient node's ability to validate transactions using digital signatures in order to detect any malicious data in the system. This process is carried out through the determination of *events*, when an external agent attempts data alteration, leading to a modification of the hash index associated with the detection metrics in the corresponding block. All subsequent changes

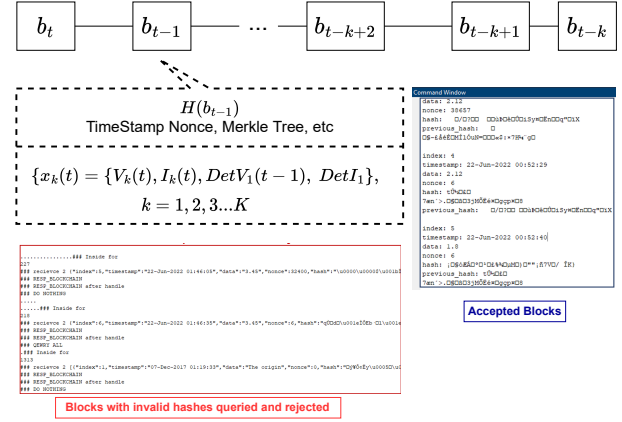


Fig. 5. Distributed Ledger and structure of b_t block at time t . Note that b_t is the block generated at time t and hash of the SHA $H(\cdot)$ algorithm. The block includes a block header and body of the local state vectors in corresponding time.

lead to further variation in the computed hash index, which is detected by the recipient node through comparison with the last trustworthy block received. In the event of a mismatch, the recipient queries the rest of the nodes for verification. As shown in Fig. 5, any hash which is declared *False* by the majority of the nodes is considered to be associated with a manipulated block of data and hence, rejected by the receiver. Thus, the general anomaly detection framework is based upon a mutual trust-based structure where a block is acceptable, if and only if it satisfies the following criteria:

$$N_a > N_r \quad (11)$$

where, N_a represents the number of approving nodes, and N_r is the number of rejecting nodes. Since this framework is vulnerable to consensus-deceiving hijacking attacks, an additional set of detection criteria as depicted in Table II is defined using smart contracts and utilized to detect such deceptive attacks. Any *event* resulting in the violation of the detection criterion in Table II leads to the labeling of the agent as a misbehaving node.

Detection of a misbehaving node triggers the activation of a self-healing strategy where:

- 1) firstly, the compromised transaction is canceled, stopping further communication of any manipulated signal to neighboring nodes to limit the attack propagation.
- 2) secondly, the malicious transaction is not recorded in the ledger and a trustworthy version of the manipulated signal is reconstructed for each compromised node (using pseudo-anonymous values of trustworthy sensor data stored in the irreversible ledger), to preserve system stability. This has been shown in Fig. 6.
- 3) finally, this trustworthy event-driven signal is sampled from measurements of the neighboring nodes (detailed philosophy can be found in [32]-[33]) and previous measurements from the same node obtained from the ledger as per the following equations:

$$\Delta V_{1j}(t_i) = f_1(\Delta V_{1k}(t), \Delta V_{1j}(t_{i-1})) \quad (12)$$

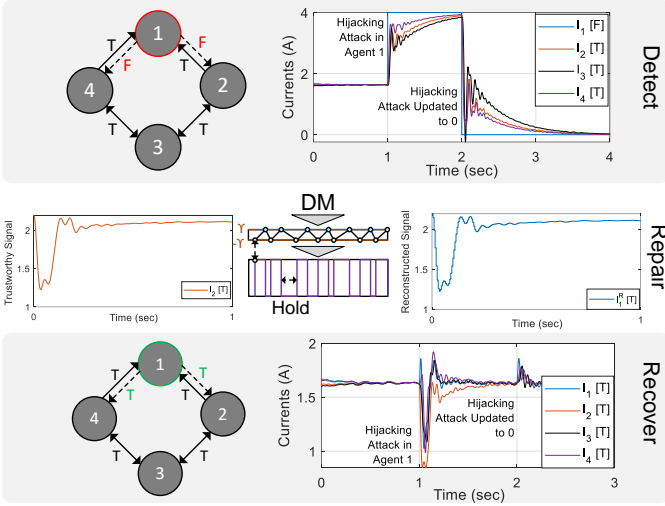


Fig. 6. Self-healing recovery scheme augmented into DLTs for microgrids – the detection metrics in Table II initiate the reconstruction process using trustworthy measurements from neighbors and then self-heal the system by transmitting back the reconstructed signal $I_1^R(t_i)$.

$$\Delta I_{dc_j}(t_i) = f_2(\Delta I_{dc_k}(t), \Delta I_{dc_j}(t_{i-1})) \quad (13)$$

where, i represents the instant at which the event occurs (also called the triggering instant), and $f(\circ)$ represents the triggering function as per which the reconstruction is performed. A major role of $f(\circ)$ is to hold the input value of the signal until the next triggering event. Hence, the recipient node is localized with no communication inputs from the malicious node. Ultimately, all the manipulated blocks are substituted with event-driven, secure reconstructed blocks. This strategy is followed to reconstruct the manipulated signal(s) at each compromised node. The presence of the terms, $\Delta V_{1_k}(t)$ and $\Delta I_{dc_k}(t)$ in (12) and (13) imply that the trustworthy reconstruction of a manipulated signal will always be possible if at least one of the nodes (here, represented as the k^{th} node) is reliable (i.e., not affected by the attack). In an event where even the k^{th} node is infected (i.e., 100% infection), the mitigation strategy will fail to reconstruct a trustworthy version of the signal. Hence, the resiliency scale of the proposed self-healing recovery scheme can be given by $N - 1$, with N given by the number of converters in the system. In simple terms, the above sentence implies that in a system comprising of N nodes, the proposed scheme will always provide secure and resilient behavior, even if there is only one trustworthy node to broadcast its information to self-heal the system.

D. Mitigation of DoS attacks and time delays

A significant advantage of the proposed set of physics-based detection metrics is their ability to also identify denial-of-service (DoS) attacks and network latencies as they would lead to mismatches in measurement values as well. However, the self-healing strategy as depicted in the preceding subsection may not be able to mitigate such network issues/attacks as the information sharing (via communication links) would be blocked in such cases. To mitigate these attacks a local compensation framework is established by integrating a

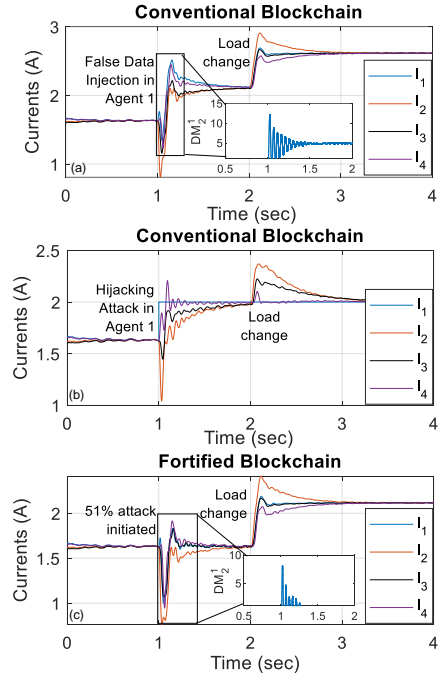


Fig. 7. Performance comparison of the microgrid-Blockchain network with and without additional fortifications as depicted in Table II. The conventional Blockchain fails to identify controller-level manipulations and accepts the attacker's manipulations as true data.

prediction policy with the self-healing strategy. This supplementary framework reconstructs an expected version of the attacked signal using a model-free compensatory mechanism as presented in [34] and depicted in Fig. 8.

In situations where DoS attacks and/or random time delays are encountered, the predictive policy exploits the recipient node's access to the last trustworthy measurement received (just before the occurrence of the *event*). In this case, the measurement not received/delayed (represented as $x(t - d)$) can be approximated using the proposed model-free prediction policy that uses the PI consensability law [35] to generate control signals in the presence of the attack vector. Since the vector seeks to manipulate the flow of measurement and control values in the secondary control layer, the signal representing the error margin $e_k^{Volt}(t)$ for the voltage control loop is downsampled to a reduced value $e_k^{down}(t)$ as per the following formula:

$$e_k^{down} = \sum_{b=0}^{B-1} e_k^{Volt} |nD - b| \cdot h|b| \quad (14)$$

where $h|b|$ represents an impulse response signal whose window length is B downsampling factor is D . Downsampling essentially reduces the resolution of the input error signal by decimating it by D samples. This ensures that the dynamic performance of the prior is appropriately matched. A pictorial representation of this process is shown in Fig. 9. In the figure, the resolution of the error signal e_k^{Volt} is scaled down by downsampling it into two different signals having resolutions of 2 and 4.

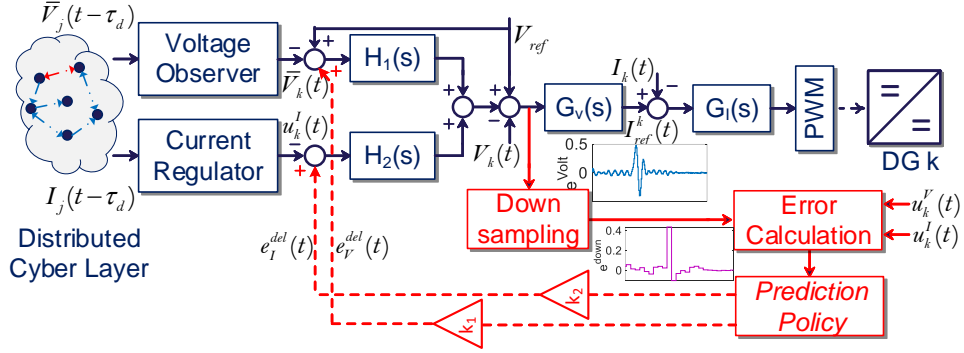


Fig. 8. A physics-based model-free predictive strategy that is augmented into the Blockchain-enabled DC microgrid to mitigate DoS attacks and potential time/computational delays [34].

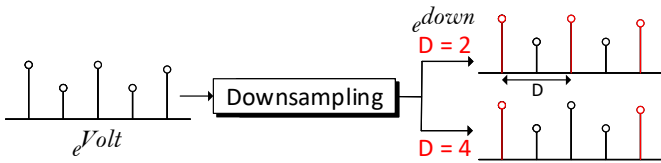


Fig. 9. Downsampling of an error signal into decimated output signals of lower resolution [34].

For an affirmation of the presence of the attack vector (and/or random time delays), local control, and measurement values are compared with the downsampled signal $e_k^{down}(t)$. Post-comparison, the proposed prediction strategy reconstructs the expected delay compensation signals $e_k(t_k) = e_k^V(t_k), e_k^I(t_k)$ at the local node side on the basis of the following condition:

$$e_k(t_k) = e_k^{down} \cdot [11] - u_k \quad (15)$$

After reconstruction, the error signal is sent to the prediction policy stage where signal reconstruction is performed again if the attack persists for an increased time period. A similar reconstruction is also performed in the case of large time delays. The overall prediction criterion is provided below.

$$\|e_k(t_k)\| > \alpha \|exp(-t/T) e_k^{Volt} \cdot [11]\| \quad (16)$$

where $T(= K_P/K_i)$ represents the time instant associated with the PI control loops, and represents a tunable parameter. If the condition defined above is satisfied, a trigger is generated that reconstructs $e_k(t_k)$ through a Sample and Hold process with the triggering instant t_k . After this, the reconstructed signals (compensators for the expected signal) are provided as inputs to the local secondary (voltage and current) control loops using a set of tunable gains, k_1 and k_2 . The inputs can be defined as follows.

$$e_V^{del}(t_k) = k_1 e_k(t_k) \quad (17)$$

$$e_I^{del}(t_k) = k_2 e_k(t_k) \quad (18)$$

As depicted in Fig. 8, these inputs are fed back into the secondary controller as per the following equations.

$$u_k^{Vf}(t) = u_k^V(t) + e_V^{del}(t_k) \quad (19)$$

$$u_k^{If}(t) = u_k^I(t) + e_I^{del}(t_k) \quad (20)$$

where u_k^{Vf} and u_k^{If} represent the final inputs to the secondary control loops as shown in Fig. 8. The proposed strategy effectively handles continued DoS attacks and large-magnitude time delays. Additionally, the error computation framework is used to validate the interruptions in a robust manner.

V. PERFORMANCE ANALYSIS & SIMULATION RESULTS

To demonstrate the action of the supplementary detection metric, we validate our results on the considered system in Fig. 2. The test system used for strategy validation is developed in the MATLAB R2020a environment. The model (as depicted in Fig. 2), has four converters (each of 10 kW rating) that are connected to each other through tie-lines R_i . The controller gains are also identical for each converter. The system and control parameters used for the simulation can be found in Table III. In the first case study, Fig. 7 presents the magnitude of current signals in a DC microgrid consisting of $N = 4$ agents (as shown in Fig. 2), where a malicious hacker with controller level access executes various types of consensus-disrupting attacks to perform: (i) hijacking, and (ii) false data injection. To perform the hijacking attack, the attacker activates an attack vector that impairs the iterative update rule leading to an arbitrary behavior. This is simulated through the swapping of a True measured signal with a new (False) constant value, which becomes the reference for other DGs in the system [36]. Consequently, all the DGs start operating erroneously resulting in a biased, arbitrary solution. To validate the replaced signal, the perpetrator interrupts the communication between a claimant (here, an incoming block of data) and the verifier (here, one or more nodes in the Blockchain network) in order to change the authentication decision. Thus, it cons the recipient into believing that a malicious, foreign block is authentic. The mathematical model of the hijacking attack can be formulated as

$$x_j^a(t) = (1 - \zeta)x_j(t) + c_j^a \quad (21)$$

where, x_j^a represents the final local measurement value from the neighboring nodes, and c_j^a is an attack element. ζ is a variable representing the presence of the attack vector which only accepts binary values 1 (during the attack), or 0

TABLE III
SYSTEM & CONTROL PARAMETERS OF SYSTEM IN FIG. 2

Parameter	Value	Parameter	Value	Parameter	Value
R_1	1.5 Ω	R_2	1.2 Ω	R_3	0.8 Ω
R_4	0.3 Ω	R_5	0.5 Ω	R_6, R_{10}	0.6 Ω
R_7	0.45 Ω	R_8, R_9	0.4 Ω	L_{se_i}	3 mH
C_{dc_i}	250 μF	$I_{dc_{min}}$	0 A	$I_{dc_{max}}$	28 A
$V_{dc_{min}}$	270 V	$V_{dc_{max}}$	360 V	V_{ref}	315
I_{ref}	0	K_P^v	5	K_I^v	100
K_P^i	2.5	K_I^i	0.05	h_i	2.5

TABLE IV
SYSTEM & CONTROL PARAMETERS OF SYSTEM IN FIG. 13

Parameter	Value	Parameter	Value	Parameter	Value
R_1	0.2 Ω	R_2	0.25 Ω	R_3	0.32 Ω
R_4	0.26 Ω	R_5	0.45 Ω	L_{se_i}	2 mH
C_{dc_i}	120 μF	$I_{dc_{min}}$	0 A	$I_{dc_{max}}$	10 A
$V_{dc_{min}}$	42 V	$V_{dc_{max}}$	54 V	V_{ref}	48
I_{ref}	0	K_P^v	5	K_I^v	100
K_P^i	2.5	K_I^i	0.05	h_i	2.5

(otherwise). This leads to a disruption in the behavior of the consensus theory imposing a restriction on $x_j^a(t)$ that can only update during future iterations. This results in the creation of a random steady-state signal value for each individual node that ceases to follow the consensus theory. To perform the false data injection attack, the attacker activates an attack vector that adds an additional (exogenic) signal to the general consensus-based control update during each iteration. This leads to the iterations converging to a feasible but manipulated (False) value, where all the operational states remain confined to their general bounds. To validate the manipulated measurement/control signals, the attacker internally overwrites any unfavorable decision from the verifier to mask malicious injections into the communication channel. The mathematical model of the FDI attack can be described as:

$$x_j^a(t) = x_j(t) + c_j^a \quad (22)$$

The above-mentioned equation allows the transmitted signal to be updated as the attacked version of the signal is still determined based on the time-dependent term $x_j(t)$. Clearly, the non-detection of such consensus-manipulating attacks can have negative repercussions on the system. However, as shown in Fig. 7, a Blockchain network fortified with the proposed set of detection metrics in Table II can immediately recognize the presence of attack elements in the compromised nodes and hence, effectively negate their actions (through signal reconstruction).

To explain the working mechanism of the proposed self-healing strategy in Fig. 6, we have considered an adversarial situation in the same system, where the attacker has access to the current of agent 1. Fig. 10 shows the proposed self-healing Blockchain-based attack detection and mitigation procedure under this scenario. Once DM_2^1 detects the presence of attack elements in an agent I, the mitigation mechanism is immedi-

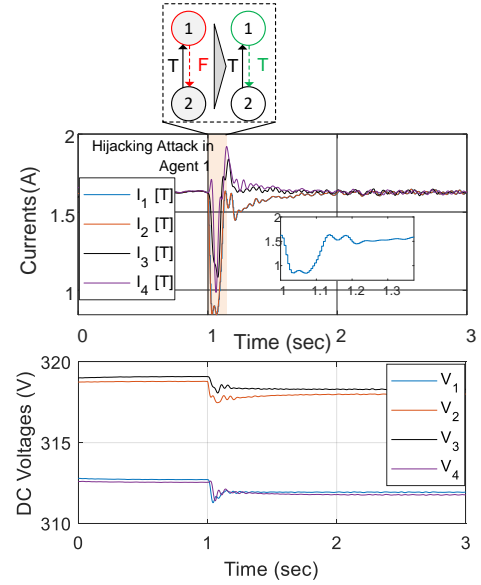


Fig. 10. Performance of the self-healing recovery scheme in DLT-based microgrids when the current of agent I is compromised – in 0.15 sec, the reconstructed signal from agent I is re-transmitted back to its neighbors by retaining the system stability.

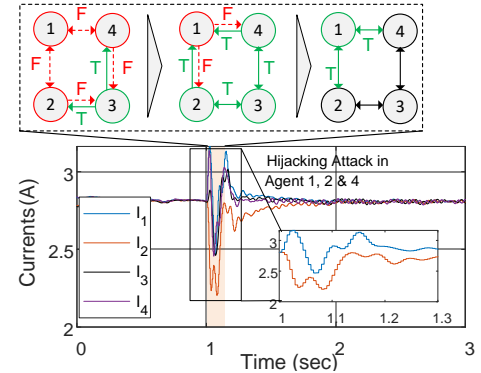


Fig. 11. Performance of the self-healing recovery scheme under cyber attacks on $N-1$ converters – the system is able to heal only from a single trustworthy agent 3.

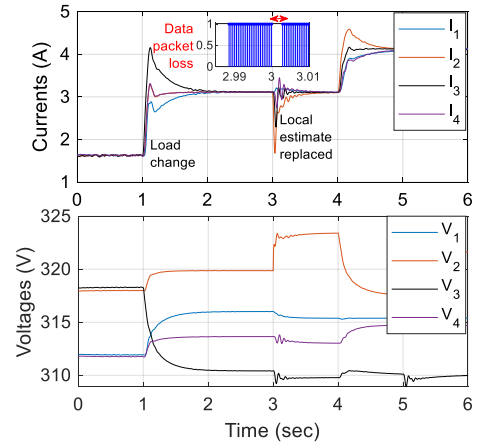


Fig. 12. Performance of the self-healing mechanism during DoS attack when the data packets are lost due to injection of random noise at $t = 3$ sec – the local reconstructed estimate [34] ensures steady-state convergence.

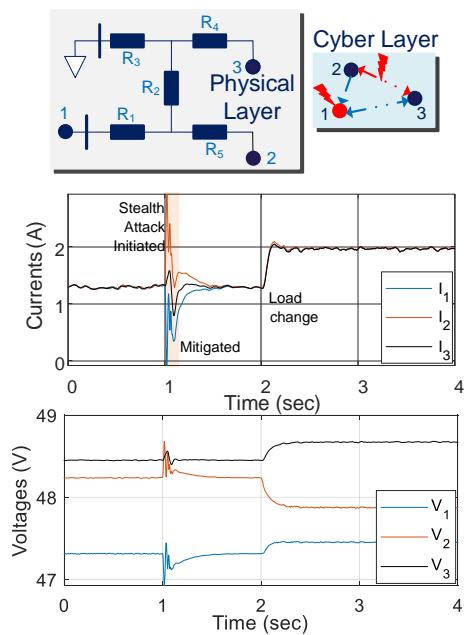


Fig. 13. Performance of the self-healing mechanism being independent of the physical parameters of microgrid, where the line resistances and number of converters are different from Fig. 2 – the system resiliency is still intact under cyber attacks.

ately triggered, which traces a trustworthy current signal from agent 2, as shown in Fig. 10. After acquiring the trustworthy current signal from agent 2, the signal reconstruction is performed to replace the attacked $I_1(t)$ with a trustworthy event-driven signal $I_1(t_k)$. As shown in Fig. 10, after the highlighted event-driven signal is replaced, its communication to neighbors is resumed after the validation process from DLT in 0.15 sec. In this way, the considered system operates normally even under a hijacking attack on one of the agents without causing any power interruption.

To evaluate the $N - 1$ resiliency scale of the proposed self-healing strategy, we have also considered the additional adversarial situations in Fig. 11, where the attacker has access to 3 nodes out of 4 agents. In this scenario, we anticipate that the only trustworthy agent III will self-heal the system by broadcasting its trustworthy information in a step-wise manner. When currents of agents 1, 2, and 4 are simultaneously attacked at $t = 1$ sec in Fig. 11, it can be clearly seen that the system operates normally despite heterogeneous transients from each converter during attacks. The signal authentication is done in a stepwise manner, which has been highlighted in Fig. 11, where the event-driven mitigation is firstly carried out in agents 2 & 4 and then later followed by agent 1 towards the end. Hence, the resiliency scale of $N - 1$ for the proposed strategy is clearly established in a system of N converters.

As outlined in Section IV(D), the self-healing mechanism can also be extended to DoS attacks, wherein a local reconstructed estimate designed using physics-governed equations can be replaced by the missing signal for a DoS attack. This can be seen in Fig. 12, where a signal interruption can be seen across the link between agent III and IV in the form of 15% data packet loss. However, the downsampled estimate

[34] obtained from the local error dynamics of the primary controllers of converter III and IV is used to compensate for the delay and achieve steady-state convergence. As a result, it is not dependent on the blockchain-enabled information transmission, since the divergent secondary controller error is substituted locally. It is worth notifying that the self-healing mechanism allows operation under dynamic disturbances, such as load changes (as shown in Fig. 12), and line outages as well, which signifies the robustness of this approach.

In the final scenario, we consider the performance of the proposed self-healing strategy in another network (shown in Fig. 13) with different system parameters to establish that the strategy is easily scalable to any physical network topology with heterogeneous dynamics. This network topology is developed in the MATLAB R2020a environment and has only three converters (each rated 5 kW). Moreover, it functions at different operation conditions as compared to the system utilized for the preceding case study. The system and control parameters for this system can be found in Table IV.

From Fig. 13, it can be clearly established that the performance of the proposed self-healing strategy remains unaltered with respect to any physical network topology or systems exhibiting different dynamics. This can be attributed to the robust physics-informed detection structure in Table II, that are independent of structural and temporal dependencies. Based on that, it can be seen that the proposed detection and mitigation strategy augmented into DLT provides resiliency immediately against stealth attacks injected into agent 2 at $t = 1$ sec. Hence, the security boundaries of DLT is significantly enhanced due to the augmentation of the physics-informed detection metrics and self-healing mitigation strategy for networked microgrids.

VI. EXPERIMENTAL RESULTS

The proposed self-healing strategy has been validated in an experimental prototype of DC microgrid shown in Fig. 14 operating at a global voltage reference of 48 V with $N = 2$ DC/DC buck converters. It should be noted that the Spitzenberger power amplifier tied to the Imperix 2 level AC/DC converters have been used as the DC source for both buck converters, equally rated around 7.5 kW. A single-line diagram of the experimental setup can be seen in Fig. 15. To emulate the computational & communication delay equipped with blockchain, a programmable delay blockset available in the BoomBox (BB) is appended before the communication channel. Variable delays and signal interruptions were programmed to emulate real-time cyber-physical operation and robustness of the proposed self-healing mechanism. The system and control parameters can be found in Appendix.

In Fig. 16, the performance of the proposed self-healing mechanism is tested under various conditions. In Fig. 16(a), a FDIA attack of magnitude 5 A on I_2 is carried out. However, due to the proposed self-healing scheme, the reconstructed signal obtained using I_1 is immediately substituted to ensure resilience against the cyber attack. This scenario also validates the $N - 1$ resiliency scale attribute of the proposed scheme, which has also been simulated in the case study in Fig. 10. Furthermore in Fig. 16(b) and (c), the impact of DoS attacks

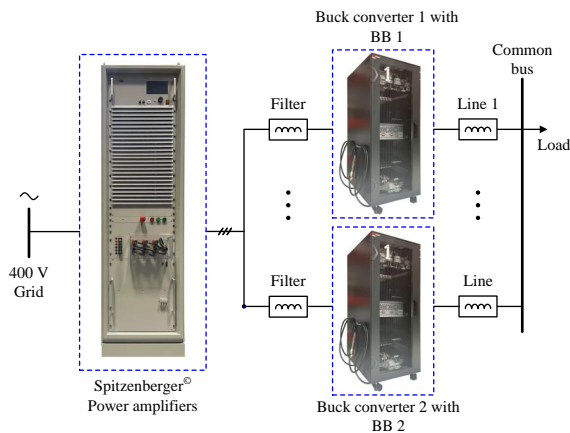


Fig. 14. Experimental setup of a DC microgrid with 2 buck converters controlled by Imperix BoomBox supplying power to the load at common bus. A delay has been programmed before the communication channel to emulate the variable computational time by the blockchain segment for each agent.

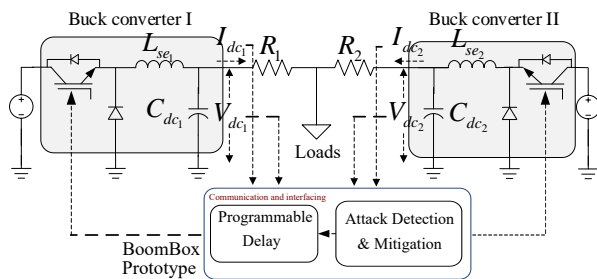


Fig. 15. Single-line diagram of the experimental setup shown in Fig. 14.

and communication & computational delay is studied. It can be seen in Fig. 16(a) that despite the signal interruption, the current sharing and voltage regulation errors are well-regulated despite the dynamic transients due to the initial mismatch in the reconstruction process. Similarly in Fig. 16(c) for a maximum communication delay of 425 ms, the microgrid was initially unstable since the cyber network can only guarantee stability up to a maximum delay of 345 ms. However as soon as the locally downsampled estimate is substituted, the error is regulated under steady-state and dynamics instances. Hence, the performance across the experimental case studies affirm the durability of the proposed self-healing approach under different operating conditions in microgrids.

VII. CONCLUSION

This paper presents a strategy to fortify DC microgrids against potential cyber-attacks through a Blockchain-based approach. The proposed strategy uses a consensus-based verification technique to determine the authenticity of blocks where the majority of the nodes must agree upon the validity of their hash indices for them to be accepted by the recipient node. However, this verification technique may be vulnerable to hijacking attacks, wherein an attacker uses its system-level access to mine malicious, new blocks and fool the recipients into believing their authenticity. Moreover, this access can also be used to fake the consent of the nodes for rejecting authentic blocks or accepting fake blocks.

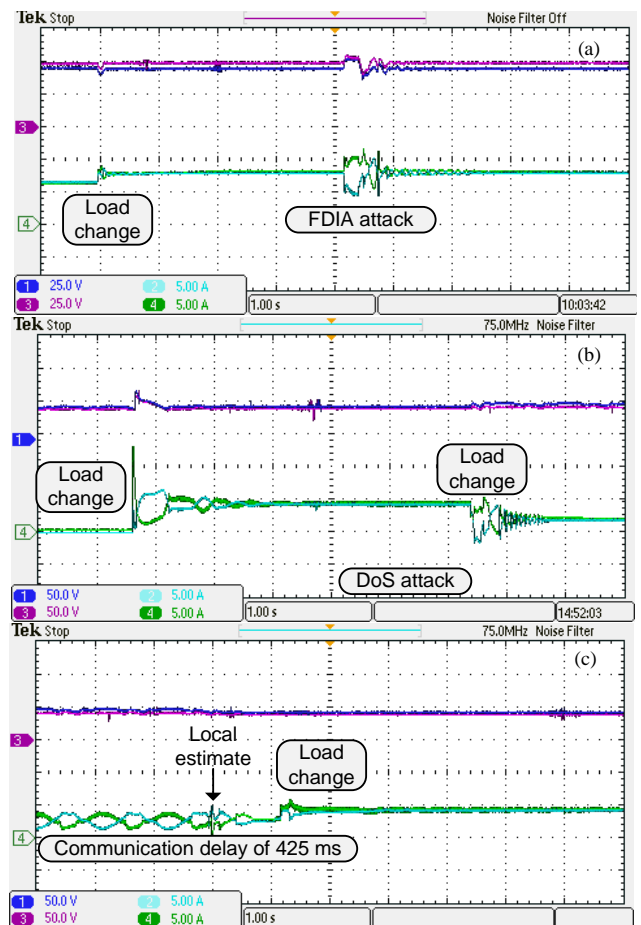


Fig. 16. Performance of the self-healing recovery scheme in DLT-based microgrids under: (a) FDIA attacks, (b) DoS attack, (c) communication delay of 425 ms, which is compensated locally using the downsampled estimate [34].

To remove this limitation, this paper combines the general features of the Blockchain with unique physics-informed attack detection metrics to detect these attacks and trigger mitigation in their presence. This detection strategy is in the form of a series of rules (threshold criteria) which, when violated, lead to the alteration of a detection metric, signifying attack detection. Detection of any false block in the network leads to its immediate rejection by the recipient. It triggers the activation of a self-healing strategy, where the lost signal/data-point is reconstructed by obtaining previous values of the same signal and current values of neighboring measurements (i.e., sensor inputs from other nodes) from the ledger. This leads to the preservation of system stability even under adverse scenarios, provided that at least one node in the network is trustworthy). In addition to this, we also provide a strategy for model-free control that is integrated with the proposed self-healing strategy for defense against random time delays and potential DoS attacks. This ensures that any computational delay created due to the Blockchain-based setup is also mitigated in a robust manner. Clearly, a major limitation of the mitigation method proposed in this paper would be its inability to reconstruct a trustworthy version of the signal if all nodes are attacked simultaneously during FDI attacks. Hence,

we plan to extend this aspect as a future scope of work by overcoming this limitation and providing full resiliency.

APPENDIX

The considered experimental prototype in Fig. 14 & 15 consists of two DC/DC buck converters rated equally for 7.5 kW. It should be noted that the controller gains are consistent for each converter.

Plant: $R_1 = 0.9 \Omega$, $R_2 = 1.2 \Omega$

Converter: $L_{se_i} = 3 \text{ mH}$, $C_{dc_i} = 100 \mu\text{F}$

Controller: $V_{\text{ref}} = 48 \text{ V}$, $K_P^{H_1} = 1.92$, $K_I^{H_1} = 15$, $K_P^{H_2} = 4.5$, $K_I^{H_2} = 0.08$, $h = 1.5$, $c = 1.4$, $\Upsilon_1 = 0.025$, $\Upsilon_2 = 0.035$

REFERENCES

- [1] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.
- [2] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5326–5340, 2021.
- [3] M. Deer, "Centralized vs. decentralized digital networks: Key differences," June 2022, (Accessed on 12/28/2022). [Online]. Available: <https://cointelegraph.com/explained/centralized-vs-decentralized-digital-networks-key-differences>
- [4] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2020.
- [5] "Top trends in the gartner hype cycle for emerging technologies, 2017 - smarter with gartner," <https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/>, (Accessed on 02/03/2021).
- [6] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino, and G. Zizzo, "A technical approach to the energy blockchain in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4792–4803, 2018.
- [7] L. D. Nguyen, I. Leyva-Mayorga, A. N. Lewis, and P. Popovski, "Modeling and analysis of data trading on blockchain-based market in iot networks," *IEEE Internet of Things Journal*, pp. 1–1, 2021.
- [8] Y. Wu, Y. Wu, H. Cimen, J. C. Vasquez, and J. M. Guerrero, "P2p energy trading: Blockchain-enabled p2p energy society with multi-scale flexibility services," *Energy Reports*, vol. 8, pp. 3614–3628, 2022.
- [9] A. Laszka, S. Eisele, A. Dubey, G. Karsai, and K. Kvaternik, "Transax: A blockchain-based decentralized forward-trading energy exchanged for transactive microgrids," in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*. IEEE, 2018, pp. 918–927.
- [10] I. A. Umoren, S. S. A. Jaffary, M. Z. Shakir, K. Katzis, and H. Ahmadi, "Blockchain-based energy trading in electric-vehicle-enabled microgrids," *IEEE Consumer Electronics Magazine*, vol. 9, no. 6, pp. 66–71, 2020.
- [11] "Powerledger energy projects," <https://www.powerledger.io/>, (Accessed on 12/17/2022).
- [12] "Grid singularity," <https://gridsingularity.com/>, (Accessed on 12/17/2022).
- [13] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids: an overview of current projects and concepts," in *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2017, pp. 6153–6158.
- [14] T. Gaybullaev, H.-Y. Kwon, T. Kim, and M.-K. Lee, "Efficient and privacy-preserving energy trading on blockchain using dual binary encoding for inner product encryption," *Sensors*, vol. 21, no. 6, p. 2024, 2021.
- [15] V. Aggarwal *et al.*, "Review of security aspects of 51 percent attack on blockchain," in *International Conference on Machine Learning and Big Data Analytics*. Springer, 2021, pp. 236–243.
- [16] S. Rath, I. Zografopoulos, P. P. Vergara, V. C. Nikolaidis, and C. Konstantinou, "Behind closed doors: Process-level rootkit attacks in cyber-physical microgrid systems," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*, 2022, pp. 1–5.
- [17] W. Yao, Y. Wang, Y. Xu, C. Deng, and Q. Wu, "Distributed weight-average-prediction control and stability analysis for an islanded microgrid with communication time delay," *IEEE Transactions on Power Systems*, vol. 37, no. 1, pp. 330–342, 2021.
- [18] R. Mahmud and G.-S. Seo, "Blockchain-enabled cyber-secure microgrid control using consensus algorithm," in *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*. IEEE, 2021, pp. 1–7.
- [19] B. Soret, L. D. Nguyen, J. Seeger, A. Bröring, C. B. Issaid, S. Samarakoon, A. El Gabli, V. Kulkarni, M. Bennis, and P. Popovski, "Learning, computing, and trustworthiness in intelligent iot environments: Performance-energy tradeoffs," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 629–644, 2021.
- [20] D. L. Nguyen, "Blockchain for internet of things: Data markets, learning, and sustainability," 2022.
- [21] N. T. Courtois, M. Grajek, and R. Naik, "Optimizing sha256 in bitcoin mining," in *International Conference on Cryptography and Security Systems*. Springer, 2014, pp. 131–144.
- [22] D.-L. Nguyen, I. Leyva-Mayorga, and P. Popovski, "Witness-based approach for scaling distributed ledgers to massive iot scenarios," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. IEEE, 2020, pp. 1–6.
- [23] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *IJ Network Security*, vol. 19, no. 5, pp. 653–659, 2017.
- [24] R. Deng, P. Zhuang, and H. Liang, "Ccpa: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017.
- [25] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.
- [26] Y. Chen, Y. Tan, and B. Zhang, "Exploiting vulnerabilities of load forecasting through adversarial attacks," in *Proceedings of the Tenth ACM International Conference on Future Energy Systems*, 2019, pp. 1–11.
- [27] C. Barreto and A. A. Cárdenas, "Impact of the market infrastructure on the security of smart grids," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4342–4351, 2018.
- [28] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against iot demand attacks," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 1115–1132.
- [29] M. R. Mengis and A. Tajer, "Data injection attacks on electricity markets by limited adversaries: Worst-case robustness," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5710–5720, 2017.
- [30] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative dc microgrids - a discordant element approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2019.
- [31] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.
- [32] S. Sahoo, T. Dragičević, and F. Blaabjerg, "An event-driven resilient control strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 35, no. 12, pp. 13 714–13 724, 2020.
- [33] —, "Resilient operation of heterogeneous sources in cooperative dc microgrids," *IEEE Transactions on Power Electronics*, vol. 35, no. 12, pp. 12 601–12 605, 2020.
- [34] S. Sahoo and F. Blaabjerg, "A model-free predictive controller for networked microgrids with random communication delays," in *2021 IEEE Applied Power Electronics Conference and Exposition (APEC)*, 2021, pp. 2667–2672.
- [35] R. Carli, A. Chiuso, L. Schenato, and S. Zampieri, "A pi consensus controller for networked clocks synchronization," *IFAC Proceedings Volumes*, vol. 41, no. 2, pp. 10 289–10 294, 2008.
- [36] S. Sahoo, J. C.-H. Peng, S. Mishra, and T. Dragičević, "Distributed screening of hijacking attacks in dc microgrids," *IEEE Transactions on Power Electronics*, vol. 35, no. 7, pp. 7574–7582, 2019.