A novel distributed privacy-preserving control and data collection method for IoT-centric microgrids

Received: 22 September 2022 | Revised: 22 January 2023 | Accepted: 15 February 2023

IET Generation, Transmission & Distribution

DOI: 10.1049/gtd2.12803

ORIGINAL RESEARCH

A novel distributed privacy-preserving control and data collection method for IoT-centric microgrids

Seyed Amir Alavi[1] | Mehrnaz Javadipour[1] | Ardavan Rahimian[2] | Kamyar Mehran[1]

[1]School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK

[2]School of Engineering, Ulster University, Belfast, UK

Correspondence
Ardavan Rahimian, School of Engineering, Ulster University, Belfast BT15 1AP, UK.
Email: a.rahimian@ulster.ac.uk

Abstract

The privacy of electricity consumers has become one of the most critical subjects in designing smart meters and their proliferation. In this work, a multilayer architecture has been proposed for anonymous data collection from smart meters, which provides: (1) The anonymity of information for third-party data consumers; (2) Secure communication to utility provider network for billing purposes; (3) Online control of data sharing for end-users; (4) Low communication costs based on available Internet of things (IoT) communication protocols. The core elements of this architecture are, first, the digital twin equivalent of the cyber-physical system and, second, the Tangle distributed ledger network with IOTA cryptocurrency. In this architecture, digital twin models are updated in real-time by information received from trusted nodes of the Tangle distributed network anonymously. A small-scale laboratory prototype based on this architecture has been developed using the dSPACE SCALEXIO real-time simulator and open-source software tools to prove the feasibility of the proposed solution. The numerical results confirm that after a few seconds of anomaly detection, the microgrid was fully stabilized around its operating point with less than 5% deviation during the transition time.

1 | INTRODUCTION

With the proliferation of smart meters in residential buildings and recent developments of advanced metering infrastructures (AMIs) based on the Internet of things (IoT), concerns about privacy and security of end-user information have been considerably increased [1, 2]. Moreover, traditional energy and power systems are transitioning toward smart grids, enabling them to integrate renewable energy sources optimally (RESs) [3]. Adding RESs with intermittent generations to electricity networks makes operation complex for a new type of service for increasing flexibility of networks; demand-side response (DSR) is one of them [4]. Growing concerns about the privacy and security of end-user information are the primary sources of distrust of smart meters, leading to a slower transition toward smart grid objectives. Regional and national regulations have been put in place, such as general data protection regulation (GDPR) by European Union (EU), to preserve the privacy of end-user information; however, these regulations are broad and do not entail the architectural details and limitations. As the volume of the data from smart meters is substantial, it also mandates the use of cloud processing algorithms for the required aggregation tasks, such as real-time demand response [5].

A distributed microgrid control system requires well-specified communication patterns to provide scalable operation for numerous controllers and dynamic control system design [6, 7]. Publish-subscribe and request-response are the optimum data-sharing patterns for microgrid controllers, according to [8–10]. Additionally, network security is necessary when using distributed control systems over communication networks. The usual strategy for networked control system security is to physically or digitally segregate control duties from the rest of the network [11]. This strategy performs effectively if the network is private, has few access points, and is adequately supervised. In [12], an optimal network constraint-based expansion planning model combined with an optimal integration framework of intermittent renewable energy resources is proposed using fictitious load theory to improve the topological flexibility in modern distribution networks. A multi-objective strategy for reaching the optimal capabilities of distributed generators

(DGs) is proposed in [13] to alleviate congestion throughout the transmission network using hybrid swarm optimization. In [14], authors have developed an innovative solution for the day-ahead sizing approach of energy storage systems of electric vehicles parking lots and DGs in smart distribution systems minimising demand response pertinent costs. From the network point of view, the authors in [15], introduced a new intelligent integration between an IoT platform and deep learning neural networks (DNN) algorithm for the online monitoring of computer numerical control (CNC) machines.

However, because of their scattered nature, microgrids can adopt a networked control system using networking technologies like the IoT. The security of the distributed controllers in these public networks is a significant concern, especially in light of the development of quantum computers capable of breaking many encryption algorithms. A proactive strategy is required to ensure intrinsic security in the control tasks, which can offer greater degrees of attack detection and mitigation.

Ground-breaking works recently presented the idea of the transactional microgrid by, among others, [11, 16, 17]. According to the core principle of transactional microgrids, energy transmission between consumers, producers, and prosumers (i.e. people who both use and create energy) is modelled in open market transactions [18]. This notion promotes using cryptocurrencies in energy markets, which are managed by a distributed ledger and are completely safe and transparent [19, 20]. A ledger records an ordered set of transactions, including financial and energy transactions, according to [16].

In a decentralised peer-to-peer (P2P) network of computers scattered across many places, a distributed ledger is a collection of information protocols for transparently and securely accessing, verifying, updating, and storing data. Furthermore, it makes special billing software and dynamic energy pricing possible. There have been several transactional microgrid models put forth thus far, such as those in the works cited in citations [19] and [21]; however, their applications were primarily restricted to trades in the energy markets cited in citation [1], and the benefits of real-time control systems for security preservation were not investigated.

In this paper, a multi-layer architecture has been proposed for anonymous data collection from smart meters and distributed controllers, which provides: (1) The anonymity of information for third-party data consumers; (2) Secure communication to utility provider network for billing purposes; (3) Online control of data sharing for end-users; (4) Low communication costs based on the available IoT communication protocols. Furthermore, the proposed data collection method enables microgrid distributed controllers to collect and share data secured by distributed historical ledgers of data and security regulators within controller/meters.

The following is a breakdown of the paper's structure. Section 2 introduces the proposed privacy-preserving method for DC microgrids. The event-based Kalman filter for microgrid state estimation and intelligent meter data aggregation is presented in Section 3. The details of the proposed signal reconstruction method for IoT-based microgrids are provided in Section 3.1. The tangle distributed ledger and the anomaly detection mechanism and isolation scheme are discussed in Section 4. The experimental results and analysis are discussed in Section 5, and the paper is concluded in Section 6.

2 | DISTRIBUTED TRANSACTIONAL ARCHITECTURE FOR PRIVACY PRESERVING

This section provides a summary of the distributed transactional control architecture that has been suggested for cyber-secure DC microgrids, which has the following three primary goals (see Figure 1):

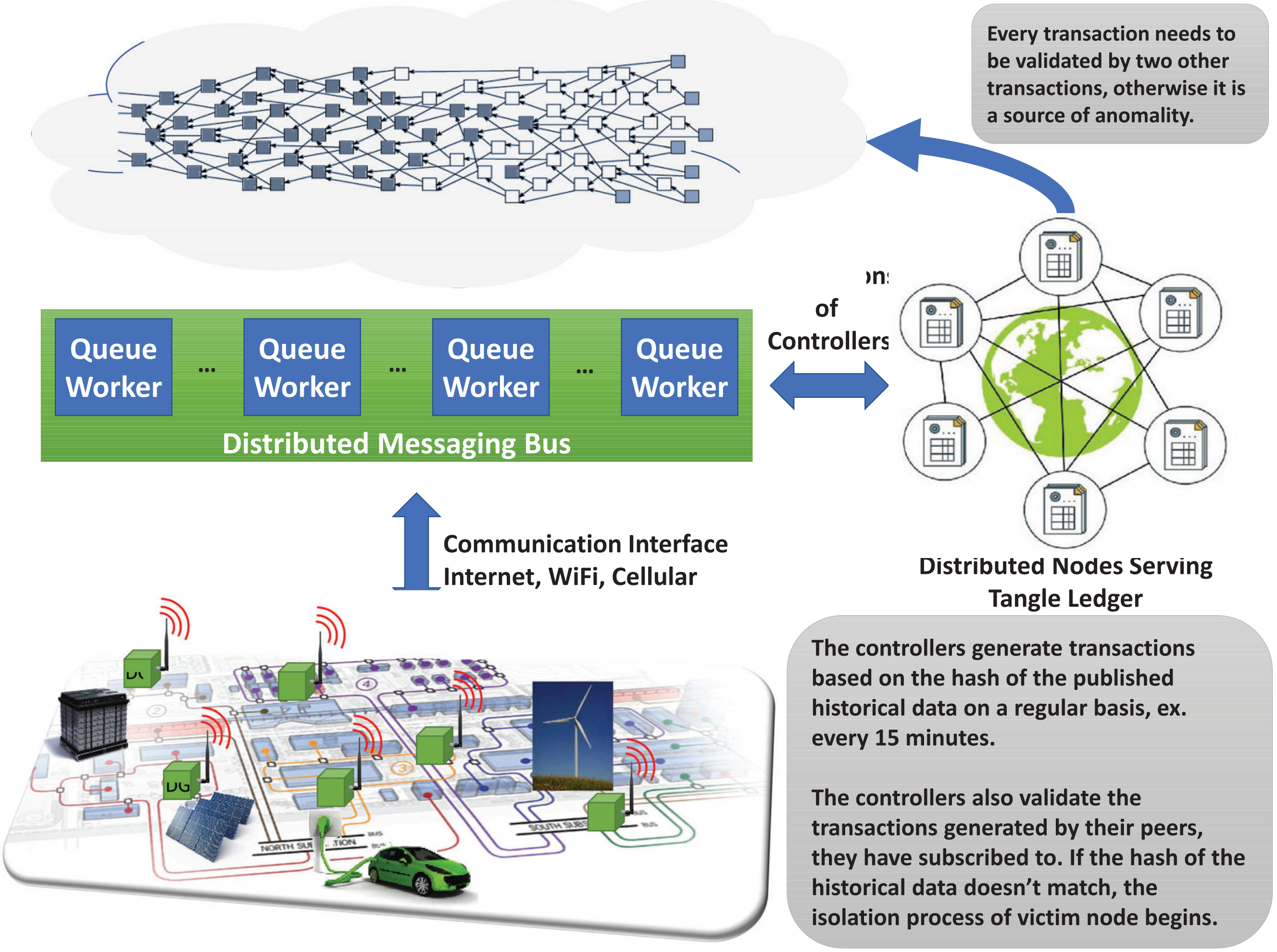
- **Proportional power-sharing:** According to their capability for power delivery, the DGs and ESSs must share load power.
- **Voltage stabilization:** Bus voltage must not deviate from the nominal microgrid voltage by more than a certain percentage.
- **State of charge (SoC) balancing of ESSs:** The (dis)charging of ESSs must be regulated to create a balanced SoC across all the battery storage systems for the microgrid to run for a more extended amount of time, particularly in the event of supply shortages.

DGs, ESSs, and loads comprise a DC microgrid's main elements. The interface joins the DGs and ESSs to a common bus through a DC-DC converter operating in the current control mode (CCM). Each battery storage system has a local controller interacting with other controllers over the microgrid communication network. A publish-subscribe communication architecture is used for data sharing between controllers, and a distributed control approach is implemented. In a publish-subscribe architecture, each controller subscribes to the shared variables important to other controllers and publishes any changes to its subscribers.

The most popular protocol for machine-to-machine (M2M) communication is the publish-subscribe communication pattern-based Message Queue Telemetry Transport (MQTT) protocol. Data can be encoded in any format, including compact binary object representation (CBOR) or Javascript object notation (JSON), with shared variables between controllers organised under several subjects (CBOR).

The data provided by the distributed controllers is verified using a transaction validation mechanism connected with the Tangle distributed ledger. Transactions of the historical data exchanged between the controllers are routinely created by the distributed controllers publishing data streams across the communication network.

The transactions that controllers make will be kept in the distributed ledger, which may be either private or public and is composed of several distributed synchronised servers. It is assumed that transactions are created often and that the time between transactions influences how soon fraudulent activity could be discovered. Shortening the time between transactions may reduce the chance of a malicious attack. Still, it may increase computational expenses depending on the processing



Every transaction needs to be validated by two other transactions, otherwise it is a source of anomality.

The controllers generate transactions based on the hash of the published historical data on a regular basis, ex. every 15 minutes.

The controllers also validate the transactions generated by their peers, they have subscribed to. If the hash of the historical data doesn't match, the isolation process of victim node begins.

FIGURE 1 The distributed transactional framework for cyber secure DC microgrid control systems proposed in this work.

capacity of the controlling nodes and the communication infrastructure used.

The proposed architecture uses a distributed average consensus approach to allow controller nodes to work together to meet DC microgrid goals. In this protocol, only a small number of nearby controllers interact with one another in the communication graph. As a result, controllers do not all subscribe to the standard variables of other controllers. The Tangle distributed ledger also allows for fee-free transactions that include data and funds. However, this architecture primarily utilises the data transmission function.

Because of security restrictions, historical data exchanged by controllers cannot be included in a transaction's raw representation. For validation reasons, it is thus necessary to compress and uniquely represent previous data from related transaction intervals using a unique hashing algorithm. In this paper, MD5 message-digest hashing method is recommended, which produces 128-bit hash values of historical data or time series of standard variables. This data will be further encrypted and signed by the controllers' certificate before being published to a distributed ledger, rendering transactions impervious to alteration and tampering (i.e. details of transactions can not be changed at any future time).

Transactions must be verified by at least two other transactions in the Tangle distributed ledger. As a result, data shared by every controller should have at least two additional controllers subscribed to it. Each controller's security regulator independently calculates the hash of the subscribed (historical) data. If it cannot validate hash code, it either already has control of a controller node or a hostile attacker has broadcast false information in the communication network. Following intrusion detection, the victim controller node is temporarily isolated or removed from the system (with the related DG or ESSs under its control) until the problem is fixed.

In the event of a malicious operation and the loss of control over the energy supply node, this security ensures that the DC microgrid will continue to operate without interruption. Section 4 security provides details on the isolation strategy. The suggested transactional control architecture's primary goal is to make distributed agent-based control systems more secure. The challenging security requirements of distributed multi-agent control systems have always drawn criticism and prevented their implementation in real-world deployments. By breaking up transmitted data into several transactions that can be checked for malicious activity, the transactional control system initially proposed in this study can increase the security of distributed multi-agent-based control systems. A detailed description of distributed control tasks and controller communication is provided in the next section.

3 | EVENT-TRIGGERED STATE ESTIMATOR DESIGN BASED ON INTERMITTENT KALMAN FILTER

The general model of the microgrid and its constituent meters and controllers can be provided as the following multiple-input multiple-output (MIMO) system:

$$\dot{x} = Ax(t) + w(t),$$
$$y(t) = Cx(t) + v(t), \tag{1}$$

where $y \in \mathrm{R}^{\mathrm{p}}$ is the microgrid output and $x \in \mathrm{R}^{\mathrm{n}}$ is the microgrid internal state. $w(t)$ and $v(t)$ are the system and sensors disturbances, respectively, with the following boundary conditions:

$$\mathrm{E}\left\{w(t)\ w(s)'\right\} = Q\,\delta(t-s), \tag{2}$$

$$\mathrm{E}\left\{v(t)\ v(s)'\right\} = R\,\delta(t-s), \tag{3}$$

$$\mathrm{E}\left\{w_i(t)v_j(s)'\right\} = 0,\quad 1 \le i \le n,\quad 1 \le j \le p. \tag{4}$$

Q and R are the system and sensor noise covariances, respectively.

In the previous work of the authors in [22], it was shown that an optimal observer could be synthesized for this MIMO system with two different correlated components:

1) Intermittent Kalman filter with aperiodic sampling.
2) Signal reconstruction unit with send on delta (SoD) sampling.

Assuming that the metering devices send data asynchronously to the control centre and the distributed controllers-based SoD sampling method if the last received i-th sensor value is y_i at time $t_{last,i}$. There is no event from i-th meter for $t > t_{last,i}$, then $y_i(t)$ is bounded as:

$$y_i\left(t_{last,i}\right) - \delta_i \le y_i(t) \le y_i\left(t_{last,i}\right) + \delta_i. \tag{5}$$

The following estimation algorithm could be then followed to restore the state of the system from SoD samples of the meters in a microgrid:

1) **Step 1**

$$\hat{x}^-(0), P_0^-$$

$$y_{last} = C\hat{x}^-(0). \tag{6}$$

2) **Step 2**

$$\overline{R}_k = R, \tag{7}$$

if i-th event are received

$$\hat{y}_{last,i} = y_i(kT) \tag{8}$$

else

$$\overline{R}_k(i,i) = \overline{R}_k(i,i) + \frac{(2\times\delta)_i^2}{12}, \tag{9}$$

end if

$$K_k = P_k^- C'\left(CP_k^- C' + \overline{R}_k\right)^{-1}$$
$$\hat{x}(kT) = \hat{x}^-(kT) + K_k\left(\hat{y}_{last} - C\hat{x}^-(kT)\right)$$
$$P_k = (I - K_k C)P_k^-, \tag{10}$$

3) **Step 3**

$$\hat{x}^-\left((k+1)T\right) = \exp(AT)\hat{x}(kT)$$
$$P_{k+1}^- = \exp(AT)P_k\exp\left(A'T\right) + Q_d, \tag{11}$$

where Q_d is the maximum global microgrid disturbance covariance, and y_{last} is (12):

$$y_{last} = [y_{last,1}, y_{last,2}, \ldots, y_{last,p}]'. \tag{12}$$

However, the introduced intermittent Kalman filter suffers from low estimation accuracy as the maximum global microgrid disturbance covariance is unstable and varies long-range during microgrid operation. This could worsen when RES are integrated into a microgrid with low inertia. Therefore, as discussed in the next section, a signal reconstruction method is employed in [22] to compensate for the Kalman filter estimation error.

3.1 | Kalman filter error compensation

This section provides theoretical aspects of error compensation for the introduced intermittent Kalman filter.

Samples received by the SoD sampler of meters can be used to reconstruct the original signal using curve fitting optimization. This paper uses projection onto convex sets (POCS) to achieve this. In a POCS optimization problem, boundaries should be formed as follows [23].

In SoD sampling, the sample time instants $t_n \in \mathbb{Z}, n \in \mathbb{Z}$ are:

$$t_n = \min\{t > t_{n-1}, x(t) - x(t_{n-1}) > \delta\}. \tag{13}$$

The set of samples is $X_e = \{x(t_0), x(t_1), x(t_2), \dots, x(t_n)\}$. The following convex region is then chosen to find the solution (13):

$$\theta^-(t) \leq x(t) < \theta^+(t), \tag{14}$$

where $\theta^-(t)$ and $\theta^+(t)$ are:

$$\begin{aligned} \theta^-(t) &= \{r \in \mathbb{R}, r = x(k) - \delta, k \in t_n\}, \\ \theta^+(t) &= \{r \in \mathbb{R}, r = x(k) + \delta, k \in t_n\}. \end{aligned} \tag{15}$$

The sign of the signal slope at event instants (t_n) is computed using this definition:

$$S(t_n) = \begin{cases} x(t_n) - x(t_{n-1}), & x(t_n) \neq x(t_{n-1}) \\ S(t_{n-1}), & x(t_n) = x(t_{n-1}) \end{cases} . \tag{16}$$

Set membership represents the samples and implicit boundary information. As a result, the solution to the reconstructed signal $x(t)$ will be convex. In [22], convex sets are defined.

Inspired by the work in [23], a recursive approach is used in this paper to find the optimal solution in the produced convex sets. The projection of the signal g onto a continuous convex set C results in another signal $\hat{x}(t)$, which is nearest to signal g:

$$\hat{x} = P_{Cg} = \arg\min_{y \in C} ||g - y||, \tag{17}$$

where the projection P_{Cg} is closer to any $y \in C$ than g:

$$||P_{Cg} - x|| < ||g - y||, \tag{18}$$

$$\begin{aligned} P_{\mathbb{B}g}(t) &= \hat{x}(t) * \frac{\Omega}{\pi}\mathrm{sinc}(\Omega t) \\ &= \int_{-\infty}^{\infty} \hat{x}(\tau)\frac{\Omega}{\pi}\mathrm{sinc}(\Omega(t-\tau))d\tau, \end{aligned} \tag{19}$$

having defined $sinc(y) = \frac{sin(y)}{y}$. ($*$ is the convolution)

The projection operator onto convex set $\mathbb{I}$ for clipping the signal to the boundary defined by θ is:

$$P_{\mathbb{I}g}(t) = \begin{cases} \theta^+(t), & \hat{x}(t) > \theta^+(t) \\ \hat{x}(t), & \theta^-(t) \leq \hat{x}(t) < \theta^+(t) \\ \theta^-(t), & \hat{x}(t) < \theta^-(t) \end{cases} . \tag{20}$$

Finally, by applying this operator for both projections, the desired accuracy of signal reconstruction will be achieved:

$$\hat{x}_{m+1} = P_{\mathbb{B}g}P_{\mathbb{I}g}\hat{x}_m, \quad m \in \mathbb{Z}. \tag{21}$$

An approximate of the 10 loops for the recursive optimizer was required to achieve an acceptable result in this paper.

3.2 | Mean-square error comparator update rule

The following estimator update rule is proposed to compensate for the error of the Kalman filter. It compares the reconstructed sample at a specific time and corrects the input of the intermittent Kalman filter accordingly.

$$y_i\left(t_{last,i}\right) = \begin{cases} y_i(kT), \ ||y_{i_{predict}} - y_{i_{construct}} < \delta|| \\ y_{i_{construct}}(kT), ||y_{i_{predict}} - y_{i_{construct}} \geq \delta|| \end{cases} , \tag{22}$$

where $y_{i_{predict}}$ and $y_{i_{construct}}$ are the output of the signal reconstructor and the event-based Kalman filter, respectively.

4 | TANGLE DISTRIBUTED LEDGER FOR CONTROLLER TRANSACTION VALIDATION IN REAL-TIME

Tangle is a network data structure that allows for a variety of safe transactions to take place. A distributed ledger, like a blockchain, entails a set of independent operators completing various data-transfer activities and reaching an ownership agreement. There is no reliance on centralised authority, and transactions are saved without using a time-consuming, computationally demanding consensus procedure or blocks. Each transaction is its block that two prior transactions must approve before it can be added to the ledger. Tangle used DAG in a transaction acknowledged by two prior transactions and added to the ledger using proof-of-work (PoW).

The unique tangle design makes it suitable for IoT networks due to fast validation support, scalability, and feeless transactions. The main challenge, however, is choosing the two older transactions for validation. No rule is imposed by tangle on how to choose these two transactions so that the validation process can be fine-tuned according to the required application. Therefore, this paper illustrates the proposed malicious activity detection and isolation scheme in Figure 2.

4.1 | Implementation of Tangle DAG in IOTA cryptocurrency

The IOTA cryptocurrency, whose architecture is IOTA Tangle and uses a PoW system for authenticating transactions on a distributed ledger, is currently the sole mainstream implementation of the Tangle transaction model. Tangle's PoW mechanism is comparable to bitcoin's, except it consumes less energy and takes less time than other PoW systems.

Because of its interconnectivity, Tangle's architecture does not necessitate complete ledger verification. Instead, all parties verify transactions simultaneously to reduce the energy and time required to execute transactions. Tangle's verification process also claims to prevent double-spending by ensuring no duplicate transactions.

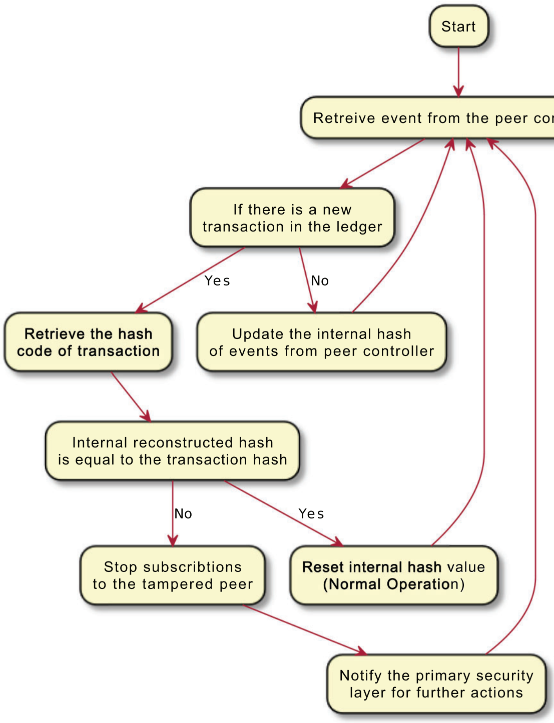

Start
Retreive event from the peer controller
If there is a new transaction in the ledger
Yes
No
Retrieve the hash code of transaction
Update the internal hash of events from peer controller
Internal reconstructed hash is equal to the transaction hash
No
Yes
Stop subscribtions to the tampered peer
Reset internal hash value (Normal Operation)
Notify the primary security layer for further actions

FIGURE 2 Flowchart for transaction validation and protection for distributed controller security regulators.

However, the system could not guard against a large-scale, coordinated attack. To counteract this assault, IOTA developed the “Coordicide” server function, which is excellent for IoT networks because of its rapid validation support, scalability, and fee-free transactions. The problematic aspect is determining which of the two previous transactions should be verified. Because tangle does not impose any constraints on choosing between these two transactions, the validation procedure may be tailored to the application’s needs. As a result, the suggested malicious activity identification and isolation system are presented in Figure 2.

The server software has been written in Node-RED to evaluate the functioning of the IOTA Tangle in the real-time control loop. Node-RED is a graphical programming tool for integrating physical devices, APIs, and web services. It contains a browser-based editor that easily connects flows with a palette of nodes, and it can be published to the runtime with a single click. “node-red-contrib-iota” is the name of the produced application, and it is freely available online under an open-source licence. [24].

5 | EXPERIMENTAL RESULTS

A real-time model of a 380 V DC microgrid is simulated in MATLAB/Simulink to show the effectiveness of the proposed strategy based on our previous work in [25]. The communication topology changes during the operation of the DC microgrid either due to DG getting online/offline or due to the isolation scheme after malicious activity detection. In this experiment, three abnormal messages are published to the bus three times. After detecting malicious activity, controllers have formed a new communication graph by adding/removing DGs to stabilize the control system further. The experimental setup is shown in Figure 4.

TABLE 1 Microgrid case study with controller parameters.

R_{dc}	36 mΩ	Voltage	380 V	$p_i^{\bar{v}p}$	5
L_{dc}	7 μH	p_i^{vi}	10	$p_i^{\bar{v}i}$	100
r	0.2533	w_i^c	100 rad/s	$p_i^{\bar{v}ii}$	0.1
p_i^{vp}	10	p_i^{ep}	5	p_i^{ei}	500

5.1 | DC microgrid configuration

The DC microgrid structure used in the deployed case study is shown in Figure 3. Each bus in the microgrid has one storage unit. The microgrid’s nominal operating voltage is 380 V*pm*5%, as most industrial microgrids, particularly data centres, employ this nominal DC voltage [26]. All buses have 30 kWh (78.947 Ah) batteries installed as microgrid ESSs. The experiment assumes constant power loads. As a result, an internal controller ensures that steady electricity from the microgrid is absorbed. Buses 1 to 3 have constant power loads of 150 W. In comparison, buses 4 and 5 have constant power loads of 50 W, resulting in total power usage of 550 W. Storage systems have an initial energy level of 50% of their capacity. Table 1 lists other parameters utilised in the experimental study, such as controller gains. The associated ESS that buffers generated energy abstracts DG dynamics. With this assumption, the distributed controller is independent of the size and dynamics of deployed DGs on buses. The DGs in the experimental system have a nominal rating of 100 W and contribute 500 W to the microgrid.

5.2 | Microgrid operation analysis

The experiment lasted 80 seconds in two scenarios to demonstrate the entire system’s dynamic responsiveness in a short time frame. In Scenario A’s first scenario, the load on all buses increases from 0 to 100 per cent in 20-s increments. Between distributed controllers, the typical communication delay is 100 ms. In the second case, Scenario B, time-varying loads are imposed on buses, with an average communication latency of 200 ms between controllers. Due to the discovery of malicious threats, the communication graph alters every 20 s from the graph according to Figure 3. Communication delay between agents is a random Gaussian process. As shown in Figure 3, the proposed transactional control system was able to detect malicious activities and remove the associated controller and ESS of the attacked node from the control system. This circumstance necessitates modifying the communication topology, as seen in Figure 3. Bus voltages are stabilised with less than

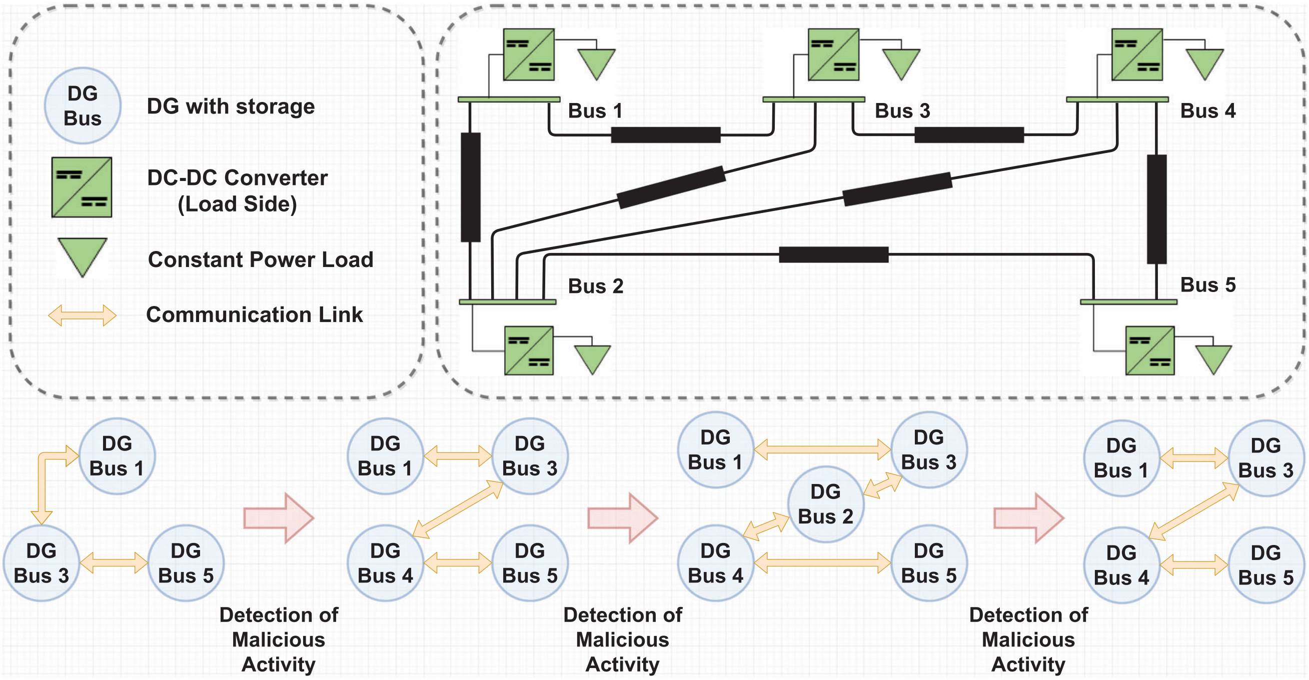


FIGURE 3 The IEEE 5 bus configuration and the corresponding experiment flow.

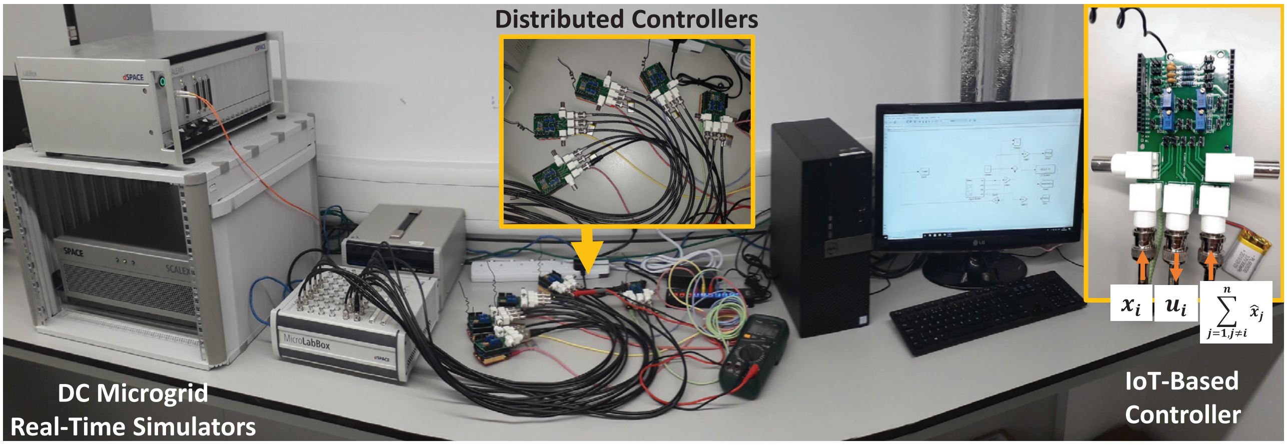


FIGURE 4 Laboratory experimental setup using dSPACE SCALEXIO real-time simulator.

a two per cent variation in the voltages as shown in Figure 6, and consensus controllers further converge in each phase, along with the average consensus value shown in Figure 5. The voltage has been stabilised around the microgrid's nominal 380 V and the destabilising effect of adding or withdrawing DGs has been lessened. In each phase, a balanced per-unit energy level is also attained, as seen in Figure 7, and Figure 8 power.

When a DG is turned off, the microgrid's nominal voltage resets the consensus voltage. The associated controller works with other controllers to get a consensus on the average voltage value once DG is connected to the microgrid. Figure 9 displays the injected power of ESSs on each bus, measured in Watts, and used to supply power to the DC microgrid. The results show that when distributed controllers with event-based delayed communication are used, the consensus is established.

6 | CONCLUSION

This study proposed a novel distributed transactional privacy-preserving control system architecture for smart DC microgrids that embed cybersecurity regulators inside each distributed controller to provide embedded security in control system operation. Furthermore, the suggested security regulators are distributive, eliminating the single point of failure scenarios. To analyze and confirm the performance of the proposed control architecture, a data-centre DC microgrid is tested against

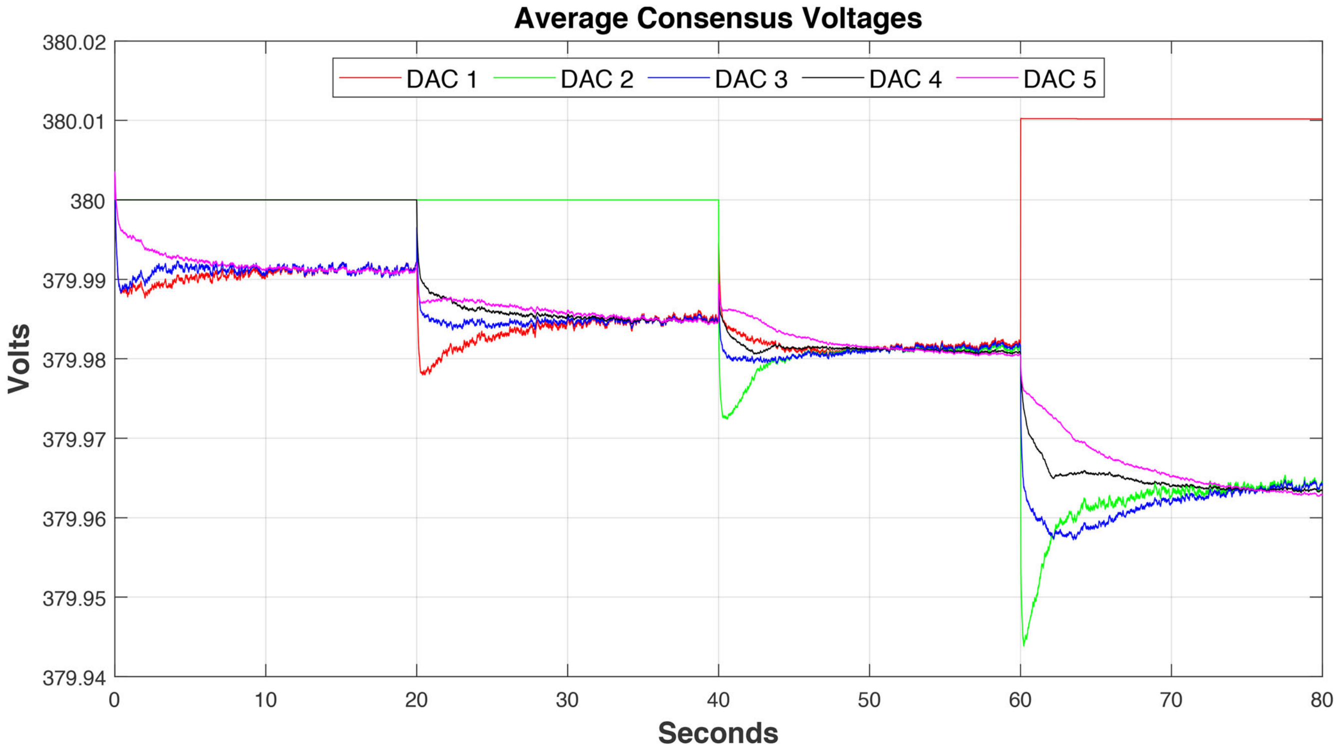


FIGURE 5 The DG controllers' consensus voltage profile during the experiment.

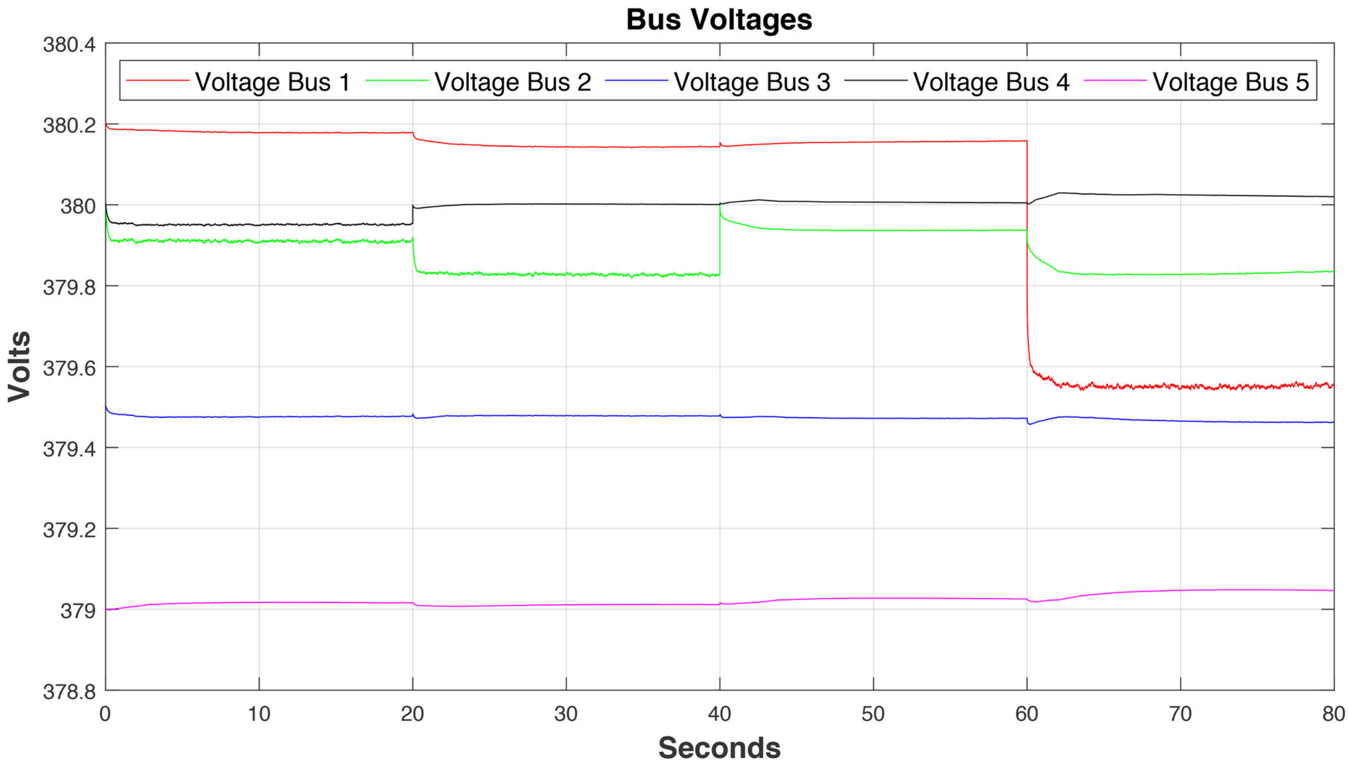


FIGURE 6 The voltage profiles of the buses during the experiment.

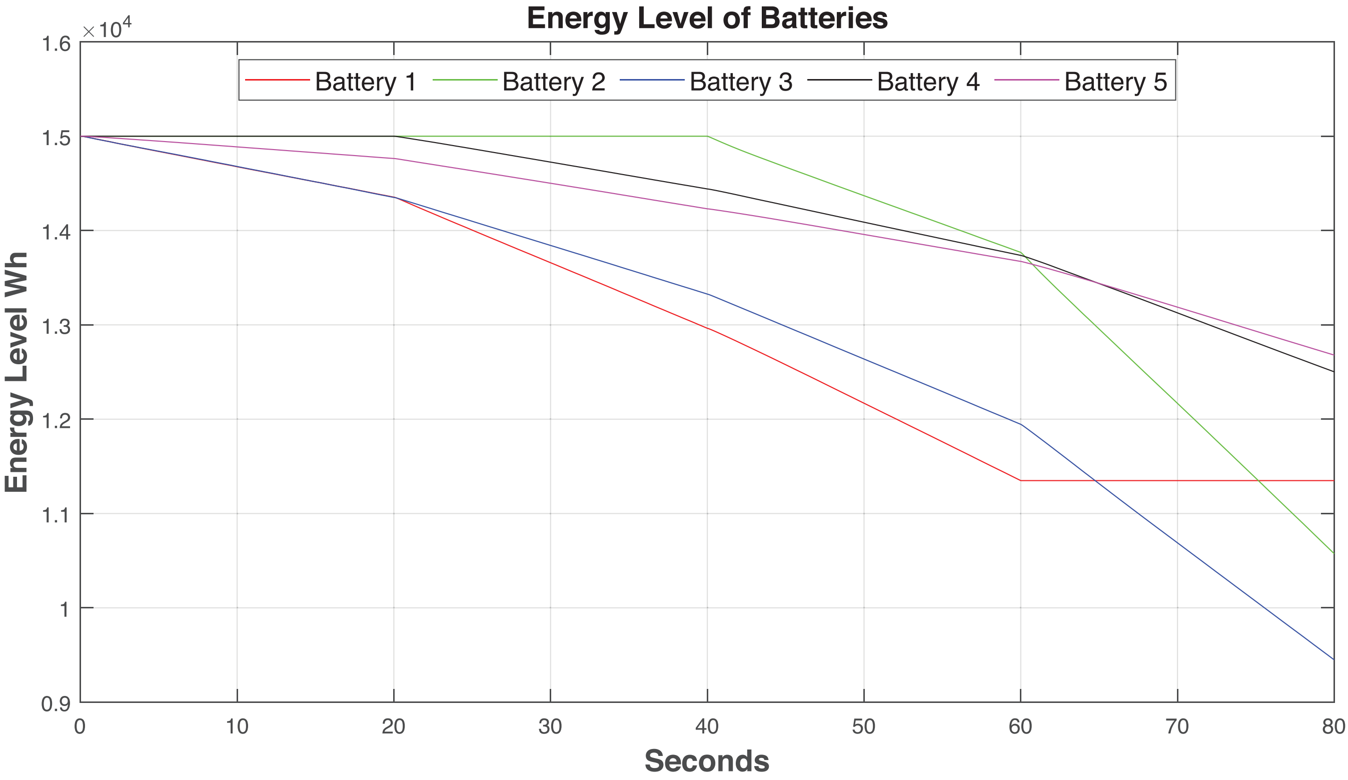


FIGURE 7 The stored energy level profile during the experiment. All DGs feature battery storage to compensate for DG supply deficits in the microgrid. When a DG is disconnected, its related storage ceases charging/discharging; nevertheless, once a DG is connected to the microgrid, the DG controller collaboratively uses storage for demand response.

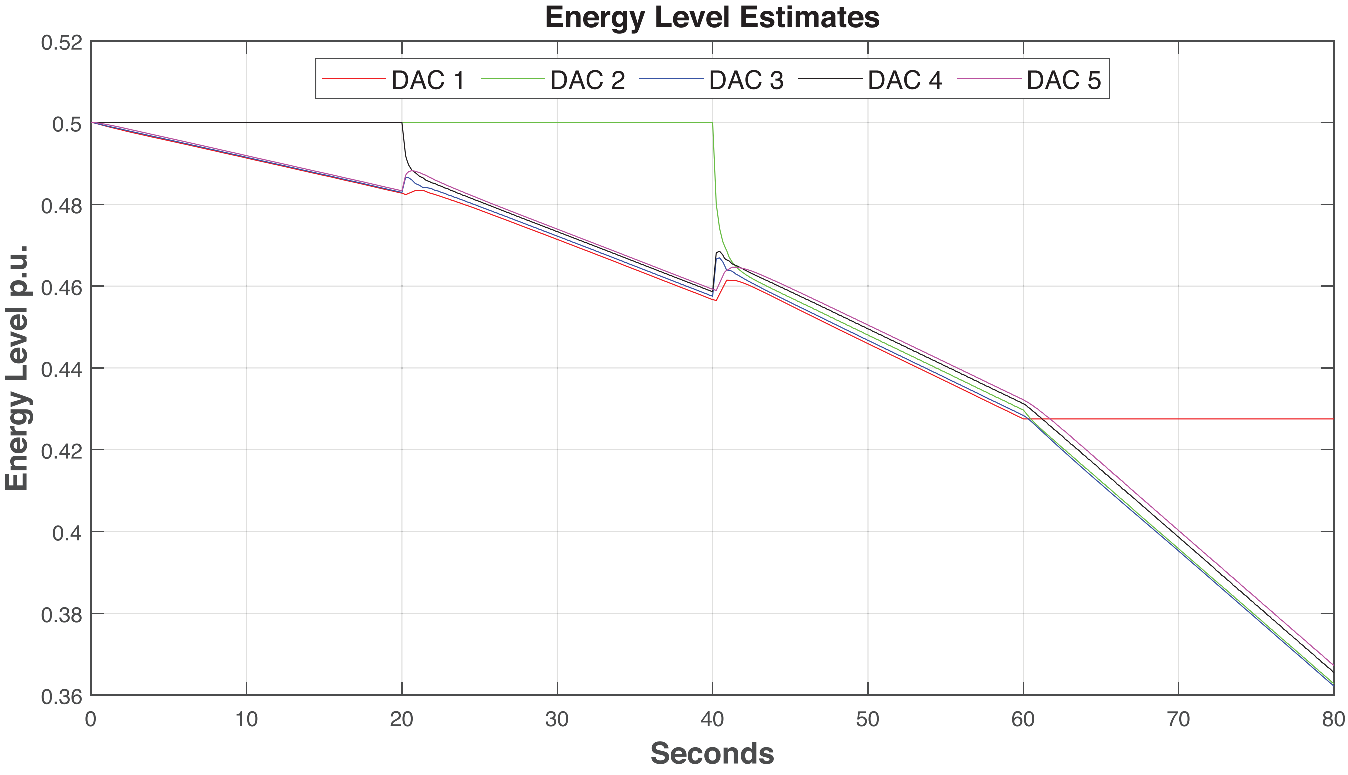


FIGURE 8 During the experiment, the energy level per unit consensus profile was analysed. For easier comparison, the figures are given per unit, which is proportionate to the capacity of energy storage devices.

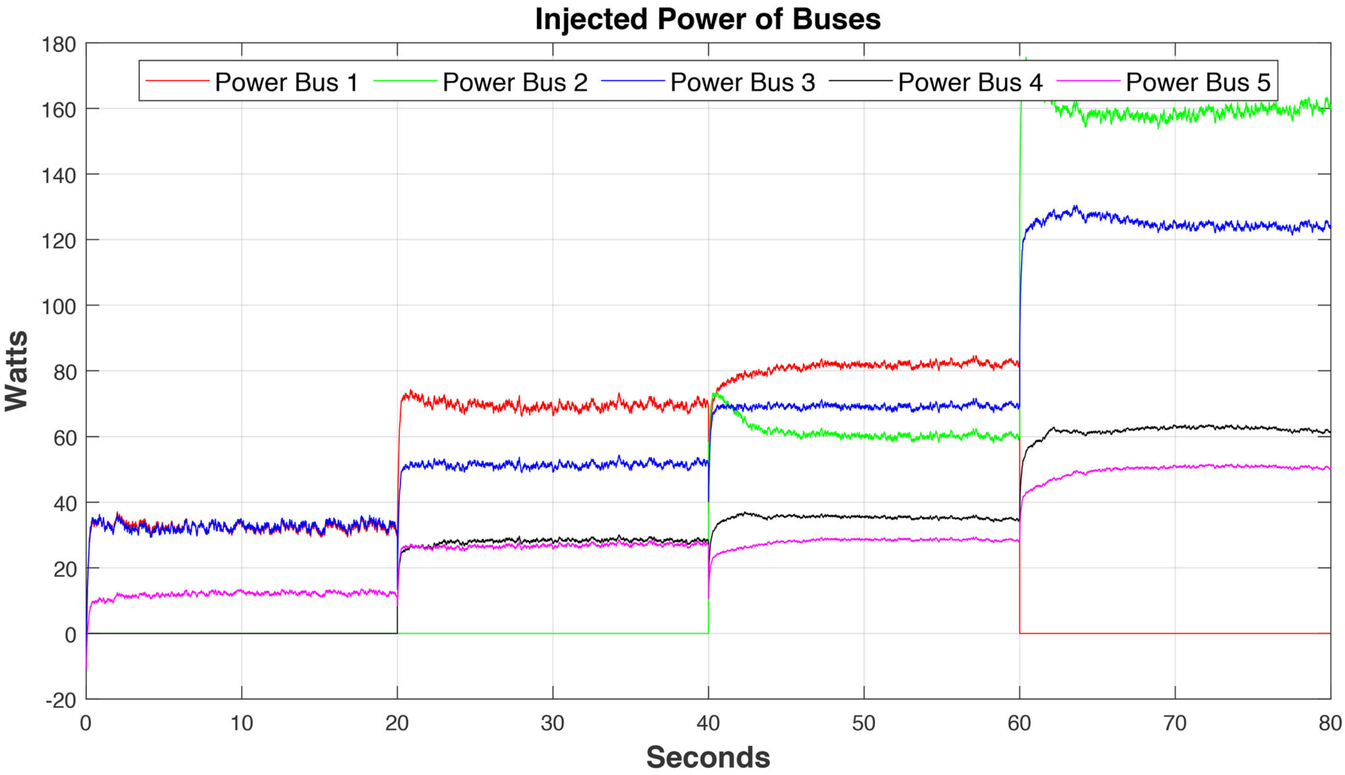


FIGURE 9 When a DG is unplugged, it delivers zero energy supply; however, after the DG is connected to the microgrid, the DG controller collaboratively regulates power based on the average consensus voltage level and per-unit energy level of its associated storage.

several malicious activities in a real-time experimental microgrid setup. The results confirmed that the microgrid control system demonstrated resiliency in the event of malicious actions by fast detection of anomalies and adaptation of the communication topology, correspondingly. The numerical results confirm that after a few seconds of anomaly detection, the microgrid was fully stabilized around its operating point with less than 5% deviation during the transition time.

For future work, different distributed ledgers than IOTA can be used as nearly every year, a new cryptocurrency based on blockchain or other distributed ledger technologies are introduced into the market. Their applicability to the smart grid and cyber security of networked control systems should be assessed to leverage their potential benefits in malicious activity detection. Furthermore, as DC microgrids are getting more attention in academia and industry, the scalability of these systems has always been a challenge, which can be resolved by using distributed ledgers.

AUTHOR CONTRIBUTIONS

Seyed Amir Alavi: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, software, validation, visualization, writing - original draft, writing - review and editing. Mehrnaz Javadipour: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, software, validation, visualization, writing - review and editing. Ardavan Rahimian: Conceptualization, funding acquisition, investigation, methodology, resources, supervision, validation, writing - review and editing. Kamyar Mehran: Funding acquisition, investigation, project administration, resources, supervision, validation, writing - review and editing.

CONFLICT OF INTEREST

No conflict of interest has been declared by the authors.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Seyed Amir Alavi https://orcid.org/0000-0003-2534-8866
Mehrnaz Javadipour https://orcid.org/0000-0001-8590-476X
Ardavan Rahimian https://orcid.org/0000-0001-9643-3019

REFERENCES

1. Daneshvar, M., Mohammadi Ivatloo, B., Abapour, M., Asadi, S., Khanjani, R.: Distributionally robust chance-constrained transactive energy frame-

work for coupled electrical and gas microgrids. IEEE Trans. Ind. Electron. 68(1), 347–357 (2021)
2. Ge, Y., Ye, H., Loparo, K.A.: Agent-based privacy preserving transactive control for managing peak power consumption. IEEE Trans. Smart Grid 11(6), 4883–4890 (2020)
3. Jayalakshmi, V., Sakthivel, K., Sherine, S.: DC microgrid for wind and solar power integration. Int. J. Eng. Adv. Technol. 8(6 Special Issue 2), 24–27 (2019)
4. Liu, Z., Wang, L., Ma, L.: A transactive energy framework for coordinated energy management of networked microgrids with distributionally robust optimization. IEEE Trans. Power Syst. 35(1), 395–404 (2020)
5. Onyeka Okoye, M., Yang, J., Cui, J., Lei, Z., Yuan, J., Wang, H., et al.: A blockchain-enhanced transaction model for microgrid energy trading. IEEE Access 8, 143777–143786 (2020)
6. Sahoo, S., Mishra, S.: A distributed finite-time secondary average voltage regulation and current sharing controller for DC microgrids. IEEE Trans. Smart Grid 10(1), 282–292 (2019)
7. Pau, M., Patti, E., Barbierato, L., Estebsari, A., Pons, E., Ponci, F., et al.: Design and accuracy analysis of multilevel state estimation based on smart metering infrastructure. IEEE Trans. Instrum. Meas. 68(11), 4300–4312 (2019)
8. Amir Alavi, S., Rahimian, A., Mehran, K., Alaleddin Mehr Ardestani, J.: An IoT-based data collection platform for situational awareness-centric microgrids. In: Canadian Conference on Electrical and Computer Engineering, vol. 2018-May, pp. 1–4. IEEE, Piscataway (2018)
9. Alavi, S.A., Javadipour, M., Mehran, K.: Microgrid optimal state estimation over IoT wireless sensor networks with event-based measurements. In: IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society, pp. 4145–4150. IEEE, Piscataway (2019). Available from: https://ieeexplore.ieee.org/document/8927727/
10. Zhou, J., Zhang, H., Sun, Q., Ma, D., Huang, B.: Event-based distributed active power sharing control for interconnected AC and DC microgrids. IEEE Trans. Smart Grid 9(6), 6815–6828 (2018). Available from: http://ieeexplore.ieee.org/document/7981382/
11. Harmon, E., Ozgur, U., Cintuglu, M.H., De Azevedo, R., Akkaya, K., Mohammed, O.A.: The internet of microgrids: A cloud-based framework for wide area networked microgrids. IEEE Trans. Ind. Inf. 14(3), 1262–1274 (2018)
12. Zhou, S., Han, Y., Yang, P., Mahmoud, K., Lehtonen, M., Darwish, M.M.F., et al.: An optimal network constraint-based joint expansion planning model for modern distribution networks with multi-types intermittent rers. Renew. Energy 194, 137–151 (2022). Available from: https://www.sciencedirect.com/science/article/pii/S0960148122007091
13. Prashant, Sarwar, M., Siddiqui, A.S., Ghoneim, S.S.M., Mahmoud, K., Darwish, M.M.F.: Effective transmission congestion management via optimal dg capacity using hybrid swarm optimization for contemporary power system operations. IEEE Access 10, 71091–71106 (2022)
14. Abo Elyousr, F.K., Sharaf, A.M., Darwish, M.M.F., Lehtonen, M., Mahmoud, K.: Optimal scheduling of dg and ev parking lots simultaneously with demand response based on self-adjusted pso and k-means clustering. Energy Sci. Eng. 10(10), 4025–4043 (2022). Available from: https://onlinelibrary.wiley.com/doi/abs/10.1002/ese3.1264
15. Tran, M.Q., Elsisi, M., Liu, M.K., Vu, V.Q., Mahmoud, K., Darwish, M.M.F., et al.: Reliable deep learning and iot-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification. IEEE Access 10, 23186–23197 (2022)
16. Zia, M.F., Benbouzid, M., Elbouchikhi, E., Muyeen, S.M., Techato, K., Guerrero, J.M.: Microgrid transactive energy: Review, architectures, distributed ledger technologies, and market analysis. Institute of Electrical and Electronics Engineers Inc., Piscataway (2020)
17. Nunna, H.S.V.S.K., Srinivasan, D.: Multiagent-Based Transactive Energy Framework for Distribution Systems with Smart Microgrids. IEEE Trans. Ind. Inf. 13(5), 2241–2250 (2017)
18. Zhao, Z., Guo, J., Luo, X., Xue, J., Lai, C.S., Xu, Z., et al.: Energy transaction for multi-microgrids and internal microgrid based on blockchain. IEEE Access 8, 144362–144372 (2020)
19. Liang, L., Hou, Y., Hill, D.J.: An interconnected microgrids-based transactive energy system with multiple electric springs. IEEE Trans. Smart Grid 11(1), 184–193 (2020)
20. Faqiry, M.N., Das, S.: Double auction with hidden user information: Application to energy transaction in microgrid. IEEE Trans. Syst. Man Cybern.: Syst. 49(11), 2326–2339 (2019)
21. Daneshvar, M., Mohammadi-Ivatloo, B., Zare, K., Asadi, S.: Two-stage robust stochastic model scheduling for transactive energy based renewable microgrids. IEEE Trans. Ind. Inf. 16(11), 6857–6867 (2020)
22. Alavi, S.A., Mehran, K., Hao, Y.: Optimal observer synthesis for microgrids with adaptive send-on-delta sampling over IoT communication networks. IEEE Trans. Ind. Electron. 68(11), 11318–11327 (2021). Available from: https://ieeexplore.ieee.org/document/9248609/
23. Rzepka, D., Miskowicz, M., Koscielnik, D., Thao, N.T.: Reconstruction of signals from level-crossing samples using implicit information. IEEE Access 6, 35001–35011 (2018). Available from: https://ieeexplore.ieee.org/document/8361846/
24. Alavi, S.A.: node-red-contrib-iota, version:1.0.0 (2020). https://github.com/qmul-rpcs-lab/node-red-contrib-iota
25. Alavi, S.A., Rahimian, A., Mehran, K., Vahidinasab, V.: Multilayer event-based distributed control system for dc microgrids with non-uniform delays and directional communication. IET Gener. Transm. Distrib. 16(2), 267–281 (2021). Available from: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/gtd2.12284
26. Becker, D.J., Sonnenberg, B.J.: DC microgrids in buildings and data centers. In: INTELEC, International Telecommunications Energy Conference (Proceedings), pp. 1–7. IEEE, Piscataway (2011). Available from: http://ieeexplore.ieee.org/document/6099725/

How to cite this article: Alavi, S.A., Javadipour, M., Rahimian, A., Mehran, K.: A novel distributed privacy-preserving control and data collection method for IoT-centric microgrids. IET Gener. Transm. Distrib. 1–11 (2023). https://doi.org/10.1049/gtd2.12803