DERauth: A Battery-based Authentication Scheme for Distributed Energy Resources

Ioannis Zografopoulos, Charalambos Konstantinou
Department of Electrical and Computer Engineering, FAMU-FSU College of Engineering
Center for Advanced Power Systems, Florida State University
Email:{izografopoulos, ckonstantinou}@fsu.edu

***Abstract*—Over the past decades, power systems have experienced drastic transformations in order to address the growth in energy demand, reduce carbon emissions, and enhance power quality and energy efficiency. This shift to the smart grid concept involves, among others, the utilization of distributed energy resources (DERs) such as rooftop solar panels and storage systems, contributing towards grid decentralization while improving control over power generation. In order to seamlessly integrate DERs into power systems, embedded devices are used to support the communication and control functions of DERs. As a result, vulnerabilities of such components can be ported to the industrial environment. Insecure control networks and protocols further exacerbate the problem. Towards reducing the attack surface, we present an authentication scheme for DERs, *DERauth*, which leverages the inherent entropy of the DER battery energy storage system (BESS) as a root-of-trust. The DER authentication is achieved using a challenge-reply mechanism that relies on the corresponding DER's BESS state-of-charge (SoC) and voltage measurements. A dynamically updating process ensures that the BESS state is up-to-date. We evaluate our proof-of-concept in a prototype development that uses lithium-ion (li-ion) batteries for the BESS. The robustness of our design is assessed against modeling attacks performed by neural networks.**

***Index Terms*—Distributed energy resources, authentication, battery energy storage systems, power grid.**

I. Introduction

According to North American Electric Reliability Corporation (NERC), a distributed energy resource (DER) is any resource on the distribution power grid that generates electricity and is not otherwise included in the bulk electric system [1]. DERs include microgrids, energy storage, behind-the-meter generation, etc. The increasing amounts of DERs – their generation capacity is expected to be 40GWs by 2030 [2] – contribute towards the transformation of the energy infrastructure offering flexible control over power generation while minimizing operating costs. Specifically, DERs with energy storage (e.g., fuel cells, batteries, or flywheels) extend grid reliability while efficiently addressing the balance between real-time energy supply and demand. Battery energy storage systems (BESS) contribute significantly to this balancing process. Among different options, lithium-ion (li-ion) batteries have become the dominant form for BESS installations due to their high energy density, decreasing costs, and performance characteristics [3].

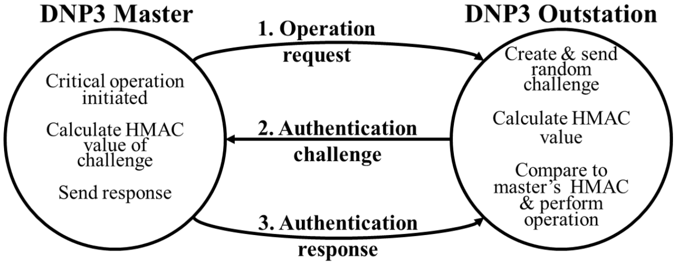

DNP3 Master
DNP3 Outstation
1. Operation request
2. Authentication challenge
3. Authentication response
Critical operation initiated
Calculate HMAC value of challenge
Send response
Create & send random challenge
Calculate HMAC value
Compare to master's HMAC & perform operation

Fig. 1. Secure CRSeq authentication of DNP3-SA, a communications protocol used between components in process automation and industrial systems.

In order to effectively monitor and control the operation of DERs, DER plants involve both local communications between the plant management system and DER units as well as between the plant and operators or aggregators who "manage the DER plant as a virtual source of energy and ancillary services" [4]. The interconnection and interoperability of DERs are enabled by protocols such as Modbus, DNP3, and IEEE 2030.5. However, such interfaces do not typically include any normative and overarching cybersecurity requirements. For example, Modbus and DNP3 have several identified vulnerabilities [5]. The implementation of these protocols is often enabled by legacy embedded systems developed without security in mind. This is evident by the incidents against the Ukrainian grid targeting embedded devices supporting industrial communications [6], [7].

Towards addressing the aforementioned security issues, several software and hardware approaches have been developed [8]. Most software-based monitoring techniques add instrumented code into the original application [9]. Their computing overhead, however, is too large to be deployed in practice, especially in real-time applications [10], [11]. In addition, software-based protocols can be exploited due to implementation vulnerabilities, enabling network attacks or even allow adversaries to disable the protocol communication media [12].

Methods that utilize hardware as a root-of-trust can provide a firm foundation from which to build security and trust [13]. Hardware-assisted technologies include trusted platform modules (e.g., Intel TXT), trusted execution environments (e.g., ARM TrustZone), virtual isolation (e.g., Intel VT), cryptographic acceleration (e.g., Intel AES-NI), random number generation (RNG) (e.g., SRAM physical unclonable functions – PUFs), etc. For instance, PUFs leverage the physical properties of hardware devices to extract randomness ensur-

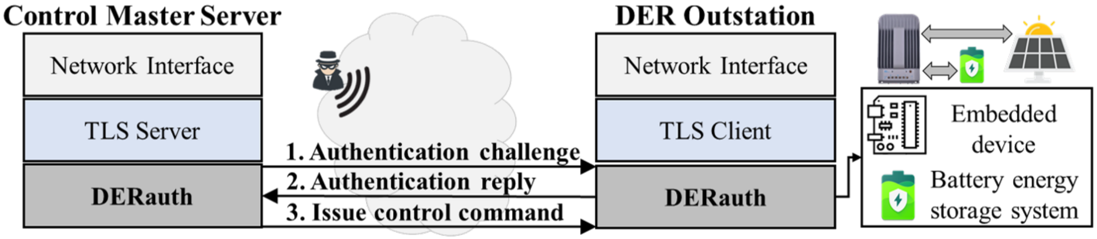


Fig. 2. Overview of the communication configuration with DERauth between DER system operators and DER units.

ing unclonability, prediction infeasibility, and tamper-evident properties.

In this paper, we present *DERauth*, a lightweight hardware-based authentication scheme which can be implemented by deployed embedded devices such as programmable logic controllers and gateways (located at DERs and aggregators) and serve as an add-on feature in existing protocols. DERauth provides a secure method for plant and fleet operators, utilities, retail energy providers, and aggregators to authenticate individual DER systems at various facilities by utilizing the unique hardware characteristics of DERs to serve as a root-of-trust. Authentication support features of existing communication protocols used in power grid substations typically rely on challenge-reply sequences (CRSeqs) [14]. Such schemes assist in verifying that all received commands within the power grid are genuinely sent by authorized remote embedded devices. An example of the CRSeq authentication as part of the secure authentication extension of the distributed network protocol (DNP3-SA, IEEE 1815-2012 std.) is shown in Fig. 1.

The functionality of DERauth is based on the concept of CRSeq authentication making it applicable to a wide range of industrial protocols. Instead of relying on software generated values (e.g., message authentication codes – MACs), DERauth leverages the physical characteristics of DER assets. Fig. 2 presents an overview of the approach within the typical communication configuration between operators and DER plants. DERauth utilizes the properties of li-ion BESS to extract randomness using the BESS real-time state consisting of state-of-charge (SoC) and voltage measurements. Specifically, we *(i)* introduce a BESS-based self-authentication scheme for DERs, *(ii)* utilize a dynamically updating process to improve reliability and account for BESS aging and cycle-to-cycle variations, and *(iii)* address modeling attacks by incorporating BESS data into DERauth's replies.

The rest of the paper is organized as follows. Section II presents the background and related work. Section III describes our methodology while Section IV presents the experimental results. Section V concludes the paper.

II. Background And Related Work

Most industrial protocols were initially developed without any security features, i.e., they do not support mechanisms to ensure data integrity and confidentiality. They rely on an *a priori trusted* relationship between master and slave communication devices. To overcome these pitfalls, security measures involve software assisted wrapper functions. However, such methods have been shown to be susceptible to a variety of attacks since it is easy to decode the algorithm and extract secret keys, especially if stored in the non-volatile memory of the device [14], [15].

The proliferation of hardware-assisted security solutions assumes that hardware can inherently be trusted as the lower lever of abstraction, and thus contribute in reducing the attack surface of embedded devices within industrial environments [16]–[18]. Among them, PUFs are lightweight security structures relying on a challenge-response mechanism where for each challenge provided as input the PUF reacts in a unique and unpredictable (but *repeatable*) way. PUFs can be classified based on their fabrication method as silicon (e.g., SRAM and Arbiter PUFs) and non-silicon PUFs (e.g., MEMS and piezo-sensor PUFs) [19]. Silicon PUFs, however, need to be designed during the integrated circuit (IC) fabrication process [20], [21]. On the other hand, non-silicon PUFs require instrumentation and quantization schemes [22], [23]. Existing solutions cannot be integrated in industrial environments with already deployed embedded devices and established communication protocols since redesigning or suspending system operation can be intolerable [24]. DERauth relies on existing infrastructure to provide hardware-based authentication support for industrial protocols.

Since many protocols that have been used for remote operation of industrial assets did not originally support any security properties, and as industrial environments are less likely to be supported by a dedicated infrastructure, such protocols started to incorporate add-on security features. An example is the hash-based MAC (HMAC) authentication of DNP3-SA (Fig. 1). A DNP3 master device sends an operation request to the outstation device which, upon receiving a critical request, sends an authentication challenge message to the master. The master device calculates the HMAC for the challenge and sends it back to the outstation that computes the HMAC value for the challenge message and compares it with the received one. If the values match, the DNP3 outstation executes the operation request. Despite the security mechanisms of DNP3-SA, the protocol has still significant drawbacks such as: *(i)* the utilization of HMAC-SHA-1 as its MAC algorithm that has been proven to be cryptographically weak, and *(ii)* the dependence on pseudo-RNGs (PRNGs) for its session keys in absence of a high-entropy source [14], [25].

III. DERauth Design

DERauth aims to address the security issues of industrial protocols by leveraging the physical properties of DERs while minimizing redesign efforts. We follow a similar approach to DNP3-SA, in which the execution of an operation request requires authentication of the outstation DER embedded device using a CRSeq. To achieve that, we leverage the inherent physical randomness from the BESS using SoC and voltage measurements as the sensed physical quantities to construct *non-repeatable* replies. Thus, for instance, if DERauth is used with DNP3-SA it would alleviate the issue of relying on PRNGs to build session keys for HMAC. In order to address modeling attacks [26], [27], we compare the BESS measurements of distinct batteries with their previous cycle measurements (i.e., *self-authentication*) rather than performing cell-to-cell comparisons. We also incorporate the BESS real-time measurements in our replies to increase entropy. The latter ensures that same challenges always result in *different* replies, hence mitigating eavesdropping and packet replay attacks. Furthermore, instead of using HMACs to validate the integrity of exchanged data, DERauth includes a transformation function that cannot only support similar HMAC functionality but also assists in mitigating modeling attacks.

A. Threat Model

The objective of DERauth is to ensure that a *control master server*, either at the DER plant management system or the utility, is able to authenticate a *DER outstation unit* in the presence of an attacker eavesdropping the communication channel. The embedded outstation device is placed at a secure location and can acquire real-time BESS measurements. In addition, the master device as part of a secure energy control facility is operated only by authorized users who enforce security mechanisms to mitigate risks related to operational disruptions. We consider the Dolev-Yao threat model where any communication channel between two parties is considered insecure after the initial handshake (*enrollment*) [28]. The Dolev-Yao adversary is capable to perform man-in-the-middle attacks and inject, eavesdrop, modify, and block messages on the communication network in order to get authenticated. Furthermore, DERauth can handle adversaries knowing protocol-specific information. We also consider modeling attacks in which the adversary acquires CRSeqs (e.g., by eavesdropping) aiming to reconstruct the challenge-reply mechanism of DERauth and initiate a communication request as a trusted DER unit.

B. Li-ion Battery Cells

Our design uses li-ion cells as an emerging energy storage solution in BESS. However, the approach is modular in terms of supporting other battery types at the BESS without modifications to the architecture of DERauth. With respect to battery characterization and performance evaluation technologies, electrochemical impedance spectroscopy (EIS) is widely used to monitor changes in batteries under different usage or storage conditions. EIS uses small-amplitude AC signals to measure resistive and capacitive properties over a wide frequency range [29]. Despite the popularity of EIS for the evaluation and thus unique identification of battery cells, EIS requires the cell to be disconnected from any load and be at steady equilibrium state. Additionally, measuring an EIS spectrum takes time (often up to many hours) and requires specialized equipment. Hence, it can become prohibitively expensive if applied to multiple cells.

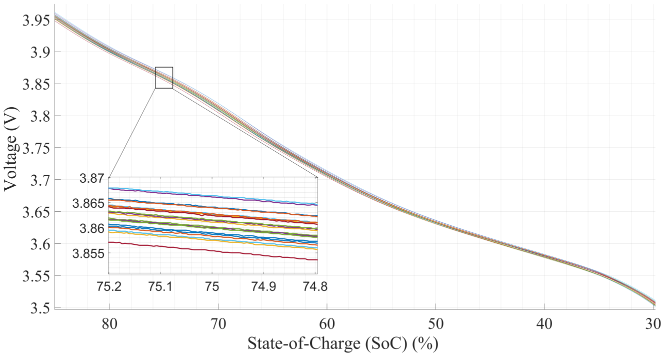


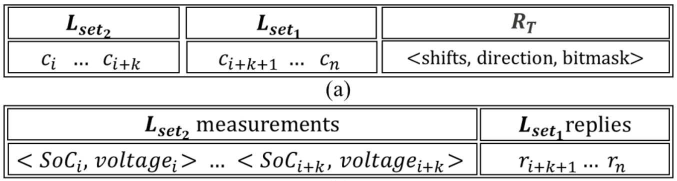
Fig. 3. Voltage and SoC variation for 20 different li-ion cells during their *first* discharge cycle.

In our design, considering the impracticality of EIS in real-time applications, we perform BESS profiling using the *model* of li-ion cells which is based on the cell's real-time voltage and SoC. The voltage describes the difference in electrical potential between the poles of a battery. It provides the cell's electromotive force that changes with the SoC according to each particular variant of the li-ion chemistry. The SoC is the cell's residual charge and therefore the expected operating time. It is a percent ratio of the current battery capacity (measured in mAh) and the rated maximum cell capacity [30].

The behavior profile of li-ion cells regarding voltage and SoC can significantly differ as a result of the intrinsic variability caused by the manufacturing process [31]. Identical li-ion cells manufactured at the same facility and following the same process provide different voltage measurements at the same SoC during their lifetime. The internal resistance, capacitance, and electrochemical effects that cannot be fully controlled during fabrication contribute to these deviations [32]. Fig. 3 demonstrates the voltage and SoC discrepancies between 20 identical li-ion cells during their *first* discharge cycle. As the number of cycles increases, the voltage and SoC variation between different cells of the same BESS, i.e., at the same aging, will further increase. In our design, the multiple li-ion cells constituting the BESS of the DER are leveraged towards entropy generation, i.e., the voltage and SoC of each battery cell are utilized towards the development of DERauth.

C. System Modules

In this section, we discuss the operating modules of DERauth. The control master server and the DER's embedded outstation device share a *cell-reply table*. The content of the table is ephemeral and gets updated asynchronously at



L_{set_2}	L_{set_1}	R_T
c_i ... c_{i+k}	c_{i+k+1} ... c_n	<shifts, direction, bitmask>

(a)

L_{set_2} measurements	L_{set_1}replies
$< SoC_i, voltage_i >$ ... $< SoC_{i+k}, voltage_{i+k} >$	r_{i+k+1} ... r_n

(b)

Fig. 4. Layout of (a) challenge and (b) temporary reply r_{temp}.

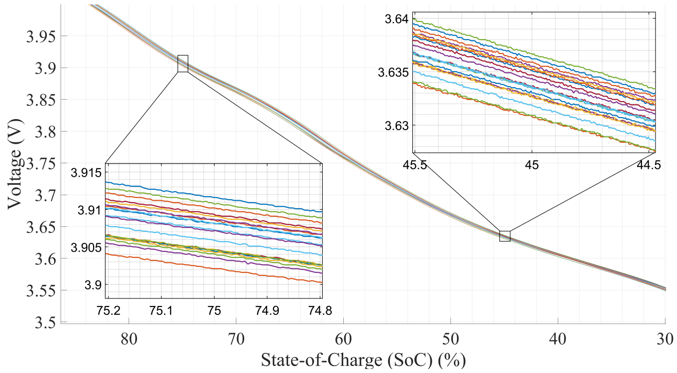


Fig. 5. Cycle-to-cycle discharge variations for the same cell.

both ends without requiring secure storage. In the event of compromise, the stored data will become obsolete the moment that the communication round terminates. The cell-reply table is defined as $C_{rt} = N \times < c_i, r_i >$. N is the number of BESS cells, and c_i and r_i are the selected BESS cell and its reply, respectively. The length of the cell replies, r_i, depends on the system integrator's constraints and number of supported BESS cells. If cell c_i is authenticated, then the reply consists of r_i. C_{rt} is initialized at the first authentication request with pseudo-random r_i values and gets modified at both ends after every authentication request.

At the control server, a *challenge builder module* generates challenges in the form of $< L_{set_1}, L_{set_2}, R_T >$ as shown in Fig. 4(a). L_{set_1} is a set of BESS cells selected to be authenticated and L_{set_2} is a set of cells selected to represent the current BESS state, B_s, i.e., the real-time SoC and voltage measurements. L_{set_1} is not necessarily equal to L_{set_2}, and the cells contained in the two sets are arbitrarily defined by the control server with every challenge request. The challenge also includes the reply transformation bits, R_T. These bits indicate to the DER's outstation device how the DERauth reply, r_{auth}, should be modified before being sent to the master. In our design, R_T values include shift operations and their direction as well as bitmask data. The flexibility of DERauth allows to modify the reply transformation scheme to favor security requirements and effectively increase the replies randomness. We refer to these reversible operations as the *transformation function* T of R_T. It allows to generate different CRSeqs for the same pair of L_{set_1} and L_{set_2} which increases the possible challenge-reply space preventing packet replay or modeling attacks.

Algorithm 1: DERauth enrollment and authentication

```
exchange $C_{rt}$
while session.valid do
    challenge.send($L_{set_1}, L_{set_2}, R_T$)
    if challenge.received then
        if compare(measure($L_{set_1}$), DUCM) then
            replies = get.reply($L_{set_1}, C_{rt}$)
            $B_s$ = measure($L_{set_2}$)
            $r_{auth}$ = transform($B_s$, replies, $R_T$)
            update($C_{rt}, B_s$), send($r_{auth}$)
        else abort.authentication()
    end
    if reply.received then
        [$B_s$, replies] = extract($r_{auth}$)
        if verify(replies, $C_{rt}$) then
            update($C_{rt}, B_s$), issue.controlCommand()
        else abort.authentication()
    end
end
```

At the DER outstation, there exist three main modules to support the authentication functionality of DERauth. *(i)* A *battery fuel gauge* module which records the real-time SoC and voltage measurements for the requested BESS cells. *(ii)* A *dynamically updating characteristic cell-model (DUCM)*: every BESS cell has its own unique DUCM, a dynamic database with transient SoC measurements and their corresponding voltages for each cell. The relationship between SoC and voltage values is not deterministic as presented in Fig. 5. The DUCM adjusts cycle-to-cycle and aging variations. The BESS measuring process is constantly running on the outstation unit updating the DUCM with the latest measurements. *(iii)* A *reply builder* module that generates the authentication reply message r_{auth}. As part of this module, a temporary reply r_{temp} is constructed and it consists of two parts: (a) the B_s provided by L_{set_2} and used to modify the C_{rt} in both the outstation and master, and (b) the replies r_i of cells c_i from L_{set_1}. Finally, r_{auth} is transformed $[r_{auth} \equiv T(r_{temp})]$ using the transformation function T which can be functionally modified according to application-specific security requirements (Section III-E).

D. System Flow

The design details and the process flow of DERauth are presented in Algorithm 1. The overall design process includes two phases: the *enrollment phase* and the *authentication phase*.

1) Enrollment phase: In this stage, the master server and the DER's embedded outstation device establish a secure communication link to exchange the cell-reply table, C_{rt}. The two parties as in a typical power grid environment communicate from geographically dispersed locations utilizing TCP/IP connections. Protocols such as IEEE 2030.5, Modbus and DNP3 facilitate the majority of these TCP/IP links while the security of the exchanged data is ensured by Transport Layer Security (TLS) (Fig. 2). Based on the established communication link, and following the guidelines of the already-in-place DER protocol, the outstation device shares the C_{rt} with the server.

2) Authentication phase: The master control server sends an authentication challenge, formed by the challenge builder module, to the DER embedded device. Once the challenge is received, the selection of L_{set_1} and L_{set_2} occurs in accordance to the challenge layout of Fig. 4(a). With the cell selection completed, the outstation device takes SoC and voltage measurements of L_{set_1} and L_{set_2} using the battery fuel gauge module. In order to authenticate L_{set_1}, each cell's real-time SoC and voltage are compared to the stored values in its respective DUCM (*self-authentication*). Next, DERauth updates C_{rt} based on a predefined operation $p_{[r_i,B_s]}$ between every reply r_i and BESS state B_s to avoid storing invariable C_{rt} data at both ends. r_{auth} is then generated by the reply builder module and sent from the DER device to the master server. The server extracts the replies r_i of L_{set_1} and the current battery state B_s. To achieve that, first the reverse transformation of function T is performed according to the reverse shift and bitmask operations within R_T. Then, each cell's r_i is verified using the master server's C_{rt}. The C_{rt} at the control server is also updated based on the $p_{[r_i,B_s]}$ operation. The selection of operations within $p_{[r_i,B_s]}$ and R_T can be adapted based on the time-critical latency requirements of the industrial process and protocol.

E. Security Discussion

In order to address man-in-the-middle (e.g., eavesdropping, packet replay, etc.) and modeling attacks, we incorporate within the challenge-reply mechanism of DERauth the current BESS state measurements, B_s, and the transformation function, T. The BESS state allows to: *(i)* generate different replies for the same challenges, and *(ii)* update the C_{rt} after every communication round. The inclusion of B_s within DERauth protects against replay and rollback attempts for authentication using old versions of r_{auth}. The transformation function, T, serves as a data integrity check; any received reply – at the master server side – has to conform to T defined when the challenge was issued. Any modified reply will be disregarded as counterfeit since after reversing T the data will have an incorrect format.

According to the design of DERauth, all of the three following conditions are necessary for an attacker to compromise DERauth's operation: *(i)* exact knowledge of the challenge and reply layout as well as their content representation, *(ii)* the transformation function T being used, and *(iii)* the most current version of the C_{rt}. The first requirement is necessary in order to be informed which cells are measured for the B_s and which are authenticated against their DUCM. The second condition is required in order to properly structure the reply and not get rejected (as modified) from the master server. Overall, the transformation function can be changed every time an enrollment phase is initiated; its update frequency can be specified by the DERauth integrator based on the security and flexibility constraints of the monitored DER asset. The third requirement is needed in order to provide the correct reply values r_i for the indicated L_{set_1} cells, else the authentication will fail. Knowledge of the current version of C_{rt} requires physical access to the master server or the outstation device. Also, since C_{rt} gets updated after every communication round, any previous knowledge becomes ineffective.

IV. Experimental Results

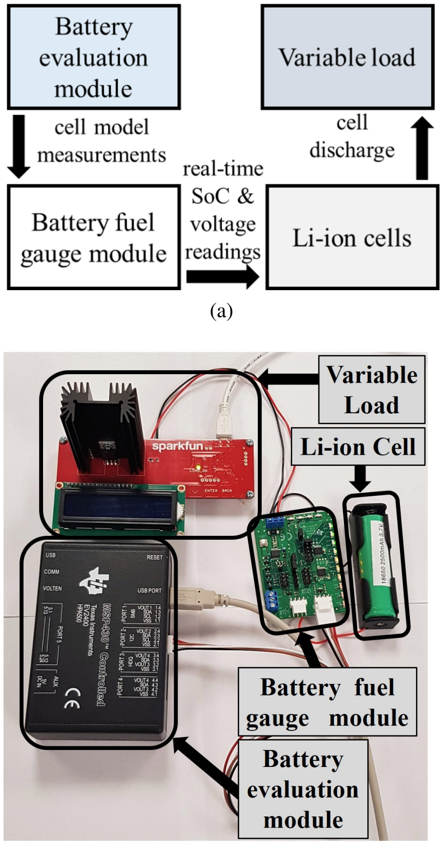
A. Design Parameters

For the implementation of DERauth we opted for 64-bit CRSeqs. The c_i and r_i of C_{rt} are selected to be 8-bit long, and N was set to 100 by extrapolating the measurements of multiple BESS cells. Based on the size of c_i, we use in the challenges: four cells for L_{set_1} and two cells for L_{set_2} (Fig. 4(a)). The remaining 16 bits in the challenge layout are reserved for the reply transformation, R_T. The first five bits of R_T define the number of positions that each reply will be shifted (cyclically), the following three indicate the direction of the shift, and the remaining eight bits are an XOR bitmask applied to the shifted reply. We adopt bitwise logical operations and shifts for the transformation function T as well as the $p_{[r_iB_s]}$ operation used for the C_{rt} updating process, ensuring that DERauth meets the stringent timing requirements of industrial protocols such as DNP3-SA. Regarding the replies r_{temp}, their first half is the B_s of L_{set_2} and the second half includes the 8-bit r_i of L_{set_1}, as shown in Fig. 4(b).

B. Implementation Setup

In order to evaluate DERauth, we have developed a proof-of-concept implementation in which li-ion battery cells (Samsung 25R 18650) are used as the BESS of DER. For the cell discharge characterization, which provides the cell SoC and voltage, we assume a constant load of 500 mA. This is sufficient since DUCM constantly monitors the BESS cells and can account for varying load conditions. For the extraction of DUCM measurements, we use the battery evaluation module TI EV2400 with the battery fuel gauge TI BQ34Z100EVM. The setup provides the SoC and voltage measurements of cells with a maximum error of $\pm 1\%$. To attain the highest possible accuracy from the battery fuel gauge, each battery cell is subjected to a "learning cycle". The cycle involves a full discharge for the fuel gauge module to accurately calculate each cell's impedance. The setup is presented in Fig. 6.

As presented in Section III, during the authentication phase the outstation device compares the measured SoC and voltage for L_{set_1} cells with their corresponding DUCM. The DUCM consists of the discharge measurements between voltage levels of $\Delta V = 4 – 3.45\ V$ as the nominal operating range per li-ion cell [33]. Exceeding those limits could severely impact the cell's condition and performance (e.g., low capacity, poor cycle life, high self-discharge, etc.). For example, a prolonged low voltage may cause dissolution of metals (e.g., copper) while a high voltage can cause battery degradation. SoC and voltage measurements are acquired at 10 mAh intervals for every cell. Obtaining and storing these values more frequently (e.g., 1 mAh) has also been examined. However, this offers marginal accuracy improvements while the memory footprint


Battery evaluation module
Variable load
cell model measurements
cell discharge
real-time SoC & voltage readings
Battery fuel gauge module
Li-ion cells
Variable Load
Li-ion Cell
Battery fuel gauge module
Battery evaluation module

(a)

(b)

Fig. 6. (a) Schematic diagram and (b) experimental measurement setup.

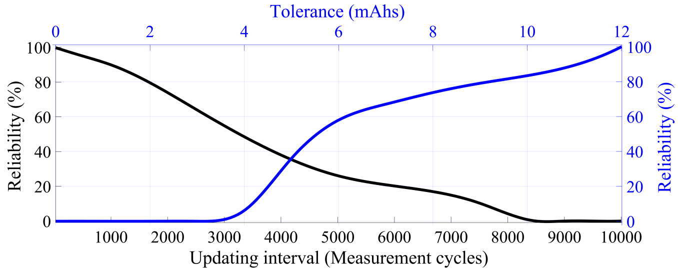


Fig. 7. Reliability Vs. updating interval (black) and tolerance threshold (blue).

increases almost tenfold. In the scenario of additional memory constraints, the measurement voltage interval ΔV could be further decreased, assuming the BESS is operating in the ΔV range, without altering the operating principles of DERauth or impacting the authentication reliability.

C. Evaluation Analysis

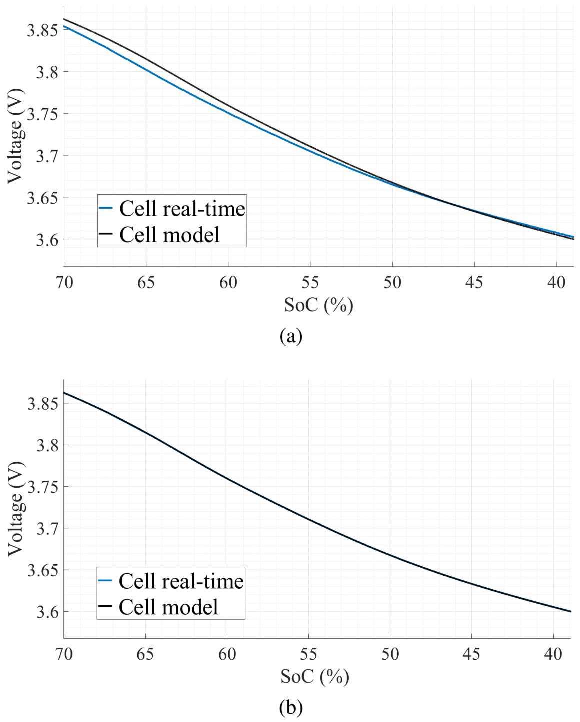
In this part, we present the evaluation of our implementation. We describe the procedure to ensure that cell SoC and voltage measurements are sufficient for authenticating each li-ion battery cell. We also discuss DUCM accuracy and present the experimental results that illustrate the impact of the DUCM updating frequency. In addition, we assess the resiliency of the DERauth's CRSeqs against machine learning attacks. We test the CRSeqs with three different multilayer perceptron neural networks (MLP-NN).

1) Battery model evaluation: In order to examine the battery model and the reliability of DERauth, we measure $S_{auth}/A_{auth} \times 100\%$, where S_{auth} is the number of successful authentications and A_{auth} is the total number of attempted authentications for the same cell. In order to construct the battery model, we discharged cells for 20 cycles. Fig. 5 shows that, even for the same cell, discharge curves vary from cycle-to-cycle depending on inherent battery features (e.g., electrochemical properties, resistance, capacitance, process variations, etc.), or exogenous causes such as the the cell's operating temperature, the type of load connected to the cell, aging effects, state of health, etc. A *static* battery model (e.g., Randle's circuit) could not address the time varying characteristics of the cells [34]. DUCM is constantly polling the SoC and voltage of every cell and contributes to an updated cell model.

Towards addressing the cycle-to-cycle discharge variation, we define a tolerance threshold (τ) representing the difference between real-time state of L_{set_1} and DUCM. The blue curve of Fig. 7 shows how the selection of τ affects the reliability of the cell authentication *before the deployment of DUCM*. A higher threshold could result in efficiently self-authenticating the cells under test due to the smaller disparity between the cells' real-time measurements and their corresponding model when compared against τ. As the threshold increases, although we can reliably self-authenticate any requested cell, we can also have many false positives, i.e., cells at similar SoC and voltage values (*cell model*), which could get authenticated if the discrepancy between their model and the real-time measurements is less than τ. This could allow adversaries to acquire cell replies, r_i. DUCM minimizes τ to $1\ mAh$ while authenticating the defined cells with reliability of 90%, eliminating the false-positives issue. DUCM achieves that by updating the model of each cell – to account for the offset between previous cycles and aging over the cell's lifetime – keeping it always below the tight threshold τ.

Fig. 5 presents the difference in discharge graphs between 20 discharge cycles. Without DUCM, the cell model would be identical to the first discharge cycle (cycle 1), thus real-time and cell model values would significantly differ over time. This is presented in Fig. 8(a). DUCM can eliminate the cycle-to-cycle discrepancy as illustrated in Fig. 8(b). The DUCM accurately tracks the transient discharge behavior of every cell and addresses the cycle-to-cycle variations. We further examine DUCM reliability with $10k$ measurements taken every $2\ secs$ (measurement cycle). Fig. 7 illustrates how the updating interval of DUCM affects authentication reliability. For example, if the cell model is updated every $1,000$ measurements (10 times in $10k$ measurements) the authentication reliability is 89.92%.

2) System Evaluation: Physical system variations can be utilized for lightweight authentication protocols used by resource-constrained platforms. However, the challenge-reply mapping could be predicted if a number of CRSeqs is avail-



(a)

(b)

Fig. 8. Cell real-time Vs. cell model discharge behavior. (a) without the dynamically updating characteristic cell-model (DUCM), and (b) with DUCM.

TABLE I
MLP Neural Network Performance with 100k CRSeqs.

Network Architecture	Batch size	Validation accuracy	Prediction accuracy
$64-320-128-64-64$	32	81.50%	81.46%
$64-320-128-64$	32	81.90%	80.93%
$64-64-64-64$	64	71.47%	71.26%

able. For instance, prediction accuracy that exceeds 90% with a small number (in the range of a few thousands) of CRSeqs has been reported [27]. In order to evaluate DERauth against such modeling attacks resulting from machine learning, we provide a set of CRSeqs to a MLP configuration [35]. Increasing the number of MLP layers creates well-defined relationships between inputs and outputs improving the learning efficacy of the algorithm. In our case, three different network architectures are utilized. Their best prediction results are achieved with a dataset of $100k$ CRSeqs. The $100k$ CRSeqs are generated in Python as part of the challenge-reply protocol implementation. As for the entropy of CRSeqs, we utilize real-time battery voltages and SoC values collected by our experimental setup. Different sizes of hidden layers are used in order to enhance the learning rate of the machine learning modeling attacks. A grid search is also performed to fine-tune the hyperparameters of the MLPs. In Table I, we provide results for the three MLP-NN architectures with different batch sizes for the training stage of the MLP-NN.

We train the configurations of the MLP-NN algorithms using different dataset sizes ranging from $1k$ to $100k$ CRSeqs and a 20% validation split. The 64-bit CRSeqs emulate the behavior of DERauth in a real-world scenario. The machine learning attack model is tested on generated sets using the same procedure. Our results indicate that increased number of available CRSeqs ($> 10k$) has minor improvements in prediction accuracy. This emphasizes the robustness of our proof-of-concept. Ideally, the accuracy should be 50% (complete randomness). In our experiments, the MLP never exceeds accuracy levels of $\approx 82\%$ despite increasing the size of the CRSeq training set. This level could be further decreased using longer CRSeqs (e.g., 128-bit) able to incorporate higher BESS entropy (more cell replies r_i and B_s measurements). The results showing the prediction accuracy for the three different configurations of MLP networks are depicted in Fig. 9.

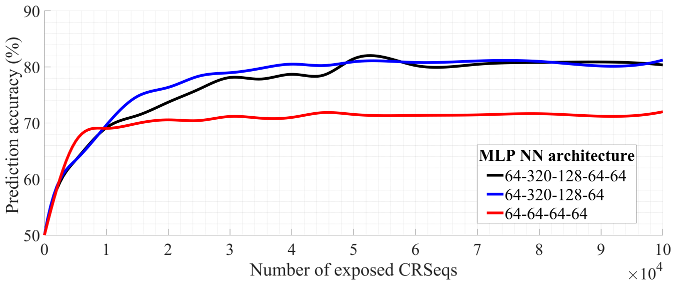


Fig. 9. Prediction accuracy Vs. known CRSeqs datasets.

V. Conclusion and Future work

This paper presents DERauth, a proof-of-concept hardware authentication framework for DERs in power grids using li-ion battery cells. This prototype version shows the potential of leveraging existing hardware to authenticate BESS-based DER systems. Thus, DERauth can serve as an add-on feature in existing industrial DER protocols. We have developed a dynamic process to update the BESS state and evaluate our model using MLP-NN. Building an ecosystem for a scalable and modular design will be included in our future work. Our research will incorporate a formal security analysis, fuzzy extractor error correction techniques, hardware-in-the-loop experiments, investigation of longer CRSeqs to explore trade-offs between security, performance and storage overhead, and variable loads to simulate cells discharge behavior. Furthermore, we will develop the required application program interface (API) which will enable the integration of our authentication framework into existing communication protocol standards (e.g., DNP3, IEEE 2030.5, etc.) used for issuing commands between aggregators and DER devices.

Acknowledgement

Partial support of this research was provided by the Woodrow W. Everett, Jr. SCEEE Development Fund in cooperation with the Southeastern Association of Electrical Engineering Department Heads.

References

[1] North American Electric Reliability Corporation, "Distributed energy resources: Connection modeling and reliability considerations," 2017.

[2] U.S. DOE, Office of Energy Analysis, "Annual energy outlook 2019 with projections to 2050," 2019.

[3] P. J. Hall and E. J. Bain, "Energy-storage technologies and electricity generation," *Energy policy*, vol. 36, no. 12, pp. 4352–4355, 2008.

[4] F. Katiraei, "DER communication," CANMET Energy Technology Centre - Varennes (Canada), Tech. Rep., 2019.

[5] S. East, J. Butts, M. Papa, and S. Shenoi, "A taxonomy of attacks on the dnp3 protocol," in *Critical Infrastructure Protection III*. Springer, 2009, pp. 67–81.

[6] SANS, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[7] C. Konstantinou and M. Maniatakos, "Security analysis of smart grid," *Commun. Control. Secur. Chall. Smart Grid*, vol. 2, p. 451, 2017.

[8] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016.

[9] N. Burow, S. A. Carr, J. Nash, P. Larsen, M. Franz, S. Brunthaler, and M. Payer, "Control-flow integrity: Precision, security, and performance," *ACM Computing Surveys*, vol. 50, no. 1, pp. 1–33, 2017.

[10] K. Basu, R. Elnaggar, K. Chakrabarty, and R. Karri, "Preempt: Preempting malware by examining embedded processor traces," in *56th Design Automation Conference (DAC)*. ACM/IEEE, 2019.

[11] H. Liu, H. Ning, Y. Zhang, and M. Guizani, "Battery status-aware authentication scheme for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 99 – 110, 2013.

[12] A. Faruk, "Testing and exploring vulnerabilities of the applications implementing dnp3 protocol," Master's thesis, Institutt telematikk, 2008.

[13] L. Batina, P. Jauernig, N. Mentens, A.-R. Sadeghi, and E. Stapf, "In hardware we trust : Gains and pains of hardware-assisted security," in *56th Design Automation Conference (DAC)*, 2019.

[14] C. Cremers, M. Dehnel-Wild, and K. Milner, "Secure authentication in the grid: A formal analysis of DNP3 SAv5." *Journal of Computer Security*, vol. 27, no. 2, pp. 203 – 232, 2019.

[15] A. Shamsoshoara, A. R. Korenda, F. Afghah, and S. Zeadally, "A survey on hardware-based security mechanisms for internet of things," *arXiv:1907.12525*, 2019.

[16] S. Bhunia and M. Tehranipoor, "Chapter 12 - hardware security primitives," in *Hardware Security*, 2019, pp. 311 – 345.

[17] X. Wang, C. Konstantinou, M. Maniatakos, R. Karri, S. Lee, P. Robison, P. Stergiou, and S. Kim, "Malicious firmware detection with hardware performance counters," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 160–173, 2016.

[18] C. Konstantinou, E. Chielle, and M. Maniatakos, "Phylax: Snapshot-based profiling of real-time embedded devices via jtag interface," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2018, pp. 869–872.

[19] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know About PUFs," *IEEE Potentials*, vol. 36, no. 6, pp. 38–46, 2017.

[20] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2009.

[21] S. Tajik, E. Dietz, S. Frohmann, J.-P. Seifert, D. Nedospasov, C. Helfmeier, C. Boit, and H. Dittrich, "Physical Characterization of Arbiter PUFs," [Online]: https://eprint.iacr.org/2014/802.pdf .

[22] O. Willers, C. Huth, J. Guajardo, and H. Seidel, "Mems gyroscopes as physical unclonable functions," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 591–602.

[23] C. Labrado and H. Thapliyal, "Design of a Piezoelectric-Based Physically Unclonable Function for IoT Security," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2770–2777, 2018.

[24] S. Falas, C. Konstantinou, and M. K. Michael, "A hardware-based framework for secure firmware updates on embedded systems," in *2019 IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2019, pp. 198–203.

[25] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, A. Bianco, and C. Baisse, "Announcing the first SHA1 collision," [Online]. Available: https://security. googleblog.com/2017/02/announcing-first-sha1-collision.html, 2017.

[26] J. Ye, Q. Guo, Y. Hu, H. Li, and X. Li, "Modeling attacks on strong physical unclonable functions strengthened by random number and weak PUF," in *IEEE 36th VLSI Test Symposium (VTS)*, 2018, pp. 1–6.

[27] J. Delvaux, "Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF–FSMs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2043–2058, 2019.

[28] H. Nicanfar and V. C. Leung, "Multilayer consensus ecc-based password authenticated key-exchange (mcepak) protocol for smart grid system," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 253–264, 2013.

[29] S. Zhang, K. Xu, and T. Jow, "Electrochemical impedance study on the low temperature of li-ion batteries," *Electrochimica Acta*, vol. 49, no. 7, pp. 1057 – 1061, 2004.

[30] "A guide to understanding battery specifications," [Online]. Available: http://web.mit.edu/evt/summary_battery_specifications.pdf, 2008.

[31] L. Patnaik and S. Williamson, "A Five-Parameter Analytical Curvefit Model for Open-Circuit Voltage Variation with State-of-Charge of a Rechargeable Battery." *IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES)*, pp. 1 – 4, 2018.

[32] V. Laue, O. Schmidt, X. Xie, F. Röder, R. Schenkendorf, and U. Krewer, "Model-based uncertainty quantification for the product properties of li-ion batteries," *Energy Technology*, vol. 8, no. 2, 2020.

[33] F. Leng, C. M. Tan, and M. Pecht, "Effect of temperature on the aging rate of li ion battery operating above room temperature," *Scientific reports*, vol. 5, p. 12967, 2015.

[34] M. Galád, S. Pavol, M. Cacciato, and G. Nobile, "Analysis of state of charge estimation methods for smart grid with VRLA batteries." *Electrical Engineering*, vol. 99, no. 4, pp. 1233 – 1244, 2017.

[35] P. Gaurang, A. Ganatra, Y. Kosta, and D. Panchal, "Behaviour analysis of multilayer perceptrons with multiple hidden neurons and hidden layers," *International Journal of Computer Theory and Engineering*, vol. 3, no. 2, pp. 332–337, 2011.