Journal of
Cyber Security

Tech Science Press

https://doi.org/10.32604/jcs.2026.079617

ARTICLE

Mitigating Fragmentation Attacks in DNP3-Based Microgrids through Permissioned Blockchain Validation

Benedict Djouboussi[1,*] **and Elie Fute Tagne**[1,2]

[1]Department of Computer Engineering, Faculty of Engineering and Technology (FET), University of Buea, Buea, Cameroon
[2]Department of Mathematics and Computer Science, Faculty of Science (FS), University of Dschang, Dschang, Cameroon

*Corresponding Author: Benedict Djouboussi. Email: benedict.djouboussi@gmail.com

Received: 24 January 2026; Accepted: 16 March 2026; Published: 15 April 2026

ABSTRACT: The Distributed Network Protocol 3 (DNP3) is widely deployed in SCADA-based microgrids; however, it was not originally designed to meet the cybersecurity requirements of modern decentralized energy infrastructures. Although DNP3 Secure Authentication (DNP3-SA) introduces HMAC-based session-level protection, it does not ensure fragment-level integrity, leaving the protocol vulnerable to fragmentation disruption, replay attacks, and sequence manipulation. Such vulnerabilities can cause desynchronization between master and outstation devices, compromising the operational reliability of distributed energy resources. This paper proposes DNP3Chain, a blockchain-enabled framework that provides real-time fragment-level validation and enforces end-to-end message integrity in DNP3 communications. An OpenDNP3-based experimental testbed was implemented to simulate fragmentation attacks by manipulating the FIR/FIN flags and transport sequence numbers, thereby preventing correct fragment reassembly at the master station. In the proposed architecture, each DNP3 fragment is associated with a unique HMAC fingerprint stored as an immutable transaction on a private permissioned blockchain (Ethereum/Ganache). A Web3-based verification service performs real-time integrity checks by comparing received fragments against blockchain records. An experimental evaluation shows that classical DNP3 lacks real-time validation capabilities, whereas DNP3-SA provides only session-level protection. In contrast, DNP3Chain detects missing and replayed fragments, restores sequence integrity, and ensures ordered message delivery. By leveraging decentralization, immutability, and distributed consensus, the framework eliminates single points of failure and significantly enhances the resilience and cybersecurity of hierarchical SCADA communications in microgrid environments.

KEYWORDS: DNP3 secure authentication (DNP3-SA); microgrids; SCADA systems; blockchain; fragment interruption attacks; HMAC integrity verification; distributed ledger technology (DLT); distributed energy resources (DERs)

1 Introduction

Microgrids provide a reliable energy supply and can manage electricity flows when connected to the main grid, in stand-alone (islanded) mode, or in the transition phase between these two modes. A microgrid can incorporate a variety of interconnected renewable energy sources, such as fuel cells, solar, wind or hydro power. However, this technological diversity poses several challenges for communication among the various components [1]. The SCADA (Supervisory Control and Data Acquisition) system is used to monitor and control industrial processes in critical infrastructure, such as microgrids. It is therefore essential to detect and reduce potential faults in this system. SCADA systems use a variety of communication protocols, including Modbus, IEC series protocols, Fieldbus, Profibus, Omnibus, DNP3, and Conitel [2]. Each of these

protocols was originally designed to meet the needs of a particular industrial sector, although several are now used across different fields or types of industrial processes. The DNP3, widely used in the electricity sector, is an open standard for communications within SCADA networks. The DNP3 is commonly used to exchange data packets between network nodes, particularly in utility distribution systems. According to several studies, more than 75% of utilities in North America have adopted, or are using, DNP3 as their primary communications protocol [3]. The DNP3 protocol enables bidirectional transmission between master and slave devices over different transport media. It is recognised for its reliability and efficiency, even in low-bandwidth or resource-limited environments. To optimise its performance, DNP3 is based on a simplified layered architecture called Enhanced Performance Architecture (EPA), which consists of just three layers: physical, data link and application [4]. Due to its open connectivity, the DNP3 is vulnerable to Internet attacks. Most DNP3 devices are configured and communicate without proper authentication mechanisms or are poorly protected against vulnerabilities in the SCADA network. Cryptography-based security mechanisms have been proposed for DNP3 by the DNP3 User Group, in which symmetric and asymmetric methods are defined and a detailed description of the challenge-response technique is made to address security objectives, such as authentication and integrity, and to protect the transmission against attacks, such as replay, spoofing and modification attacks, at the application layer [5]. In communication mode, the DNP3 runs over TCP/IP to ensure exchanges over the Internet, while using security protocols such as TLS/SSL and IPSec to prevent unauthorised access. However, DNP3 itself lacks a robust authentication mechanism. For this reason, its frames are encapsulated in secure protocols such as TLS/SSL or IPSec. Research has examined vulnerabilities affecting SCADA/DNP3 communications, highlighting the importance of using anomaly- and intrusion-detection techniques. These mechanisms identify various attack types, including flooding attacks, denial-of-service (DoS) attacks, spoofing attempts, data modifications, fraudulent responses, and man-in-the-middle attacks [6]. Considering the vulnerabilities of the DNP3 protocol, DNP3 provides Secure Authentication (DNP3-SA) has emerged as a solution to address them. DNP3-SA is a security extension to the DNP3 protocol, used to authenticate critical commands between master stations and outstations in SCADA/Smart Grid systems and prevent command manipulation, falsification or replay. DNP3 provides Secure Authentication as the mechanism to authenticate unicast messages from a master station to its outstations in supervisory control and data acquisition systems. The authors [7] have proposed a DNP3 SA model based on a unilateral application authentication mechanism using HMACs (Keyed-Hash Message Authentication Code) in two modes: NACR (Non-Aggressive Challenge Response) and AGM (Aggressive Mode). Session keys are derived from statically shared keys (long-term). This model has been formalised using Coloured Petri Nets (CPN) to check its robustness against various attack scenarios. In recent years, additional security measures have been implemented to strengthen the DNP3. The security measures in IEC 62351 can also be applied to DNP3, making it suitable for use alongside modern ICT(Information and Communication Technology) systems [8]. In the DNP3-SA formal model, behavioural analysis using coloured Petri nets revealed a critical weakness in the management of fragmented message sequences, particularly at the Challenge Sequence Number (CSN) level. The authors [9] highlight a critical vulnerability in DNP3's fragment management, particularly at the Challenge Sequence Number (CSN) level. This number, which is incremented in a predictable manner, can be guessed and manipulated by an attacker to cause desynchronisation between the master and the outstation. In the absence of a challenge message authentication mechanism, this flaw allows attacks by sequence interruption or by replay of valid commands, compromising the integrity of the authentication. This structural weakness makes DNP3-SA vulnerable to stealth attacks without alerting the system. Moreover, though the DNP3-SA employs a unilateral authentication through the HMAC mechanism to protect the devices against certain attack vectors, the mechanism does not protect messages that are not considered "critical". The DNP3, widely used in SCADA systems, fragments large messages into packets identified by the FIR (First) and FIN (Final)

indicators. This fragmentation makes the protocol vulnerable to a specific class of attacks, called fragment interruption attacks, which consist in deleting or desynchronizing certain fragments before their reception by the Master. These attacks lead to partial or erroneous reconstruction of messages, compromising the consistency of commands and the monitoring of remote devices. Unlike a Man-in-the-Middle (MITM) attack, which involves actively intercepting and potentially modifying communications between two parties, replay and sequence interruption attacks exploit structural weaknesses in the protocol's authentication and sequencing logic. In replay attacks, a valid authenticated message is captured and resented later without modification, taking advantage of the absence of anti-replay or challenge response mechanisms. Thus, while MITM compromises the communication channel itself, replay and sequence attacks compromise the logical integrity of the protocol without necessarily controlling or altering the communication path. Despite the improvements introduced by DNP3 Secure Authentication (DNP3-SA), no native measure allows real-time detection of the loss of individual fragments or their sequence alteration, since authentication mainly concerns logical blocks or complete sessions. The main motivation in this work is to demonstrate the contribution of blockchain as an innovative security solution to address the vulnerabilities of the DNP3 adapted with the new paradigm of microgrids based on decentralization architectures. Today, blockchain has made a remarkable contribution to microgrids with the rise of the Internet of Things and cyber-attacks [10]. Unlike traditional security architectures in microgrids, blockchain provides a higher level of security through its decentralised architecture. The authors [11] have developed a Deep Learning-based solution to secure the DNP3. The proposed model produced acceptable results, and they also proposed integrating blockchain to improve it.

Following this introduction, we will first highlight related work, focusing on DNP3 protocol vulnerabilities and cyberattacks. We also demonstrate the evolution of this protocol through DNP3 Sec and DNP3 SA. For the experimental part, we leveraged fragment interruption attacks to model a scheme for integrating blockchain technology into microgrids to improve the security of the DNP3 protocol and ensure secure communication between the RTU (Remote Terminal Units) and SCADA, particularly in its master-slave architecture. The final section analyses the results obtained and future improvements. This article is organized as follows:

- Section 2 discusses related work, presenting the operation of the DNP3, its vulnerabilities, the different layers that compose it, and the message exchange mechanisms. It also highlights the security enhancements of this protocol, such as DNP3 Sec and DNP3 SA, and examines attacks that exploit DNP3 vulnerabilities by interrupting fragmented messages at the master station and remote stations.
- Section 3 focuses on the application of blockchain technology in SCADA systems to secure communications between the master station and the remote station via DNP3. This section also highlights the proposed approach to integrate blockchain to enhance the internal security of communications within SCADA systems.
- Section 4 highlights the various results obtained and an interpretation.
- Section 5 is the conclusion of the article, which summarizes the work as well as the contributions and suggestions for future research.

2 Related Works

The Distributed Network Protocol version 3 (DNP3) was originally developed by General Electric and released to the public in 1993. It was designed to meet the communication requirements of Supervisory Control and Data Acquisition (SCADA) systems. The original protocol structure was based on a four-layer model: the physical layer, the data link, the transport, and the application. Initially, the physical layer used serial communication standards such as RS-232, RS-422, or RS-485. As communication technologies have

evolved, the protocol has been ported to the TCP/IP stack, enabling more flexible end-to-end communication that is compatible with modern network infrastructures. In this context, DNP3 can be interpreted as a network protocol structured into three logical layers that operate on top of TCP/IP. However, one of the critical points of DNP3, as with IEC 61850, is the lack of security mechanisms built into its initial design. This vulnerability leaves the protocol susceptible to attacks such as message interception or falsification, compromising either the behavior of the control and protection devices or the confidentiality of the exchanged data. In the sensitive context of intelligent microgrids, this weakness represents a major risk to the reliability and security of infrastructures [12]. Although the DNP3 uses open standards such as TCP and UDP for transmission over the Internet, it has several cybersecurity weaknesses. In particular, SCADA systems based on DNP3 are exposed to risks of interception, interruption and modification of communications, affecting central controllers as well as remote stations and communication networks. The design of the protocol does not natively provide for security mechanisms such as authentication, encryption or access control. As a result, an attacker can exploit these weaknesses to alter the messages transmitted, particularly at the application, pseudo-transport and data link layers, without the DNP3 nodes being able to detect these alterations or check the integrity of the messages received [13]. The DNP3 can be partially associated with the OSI model. Designed as a multi-layer protocol, DNP3 has clear correspondences with certain layers of the OSI model, although it does not cover all layers, particularly the presentation and session layers. Fig. 1 below illustrates the mapping between the OSI model, the TCP/IP model and the DNP3stack, providing an overview of the communication mechanism within microgrids.

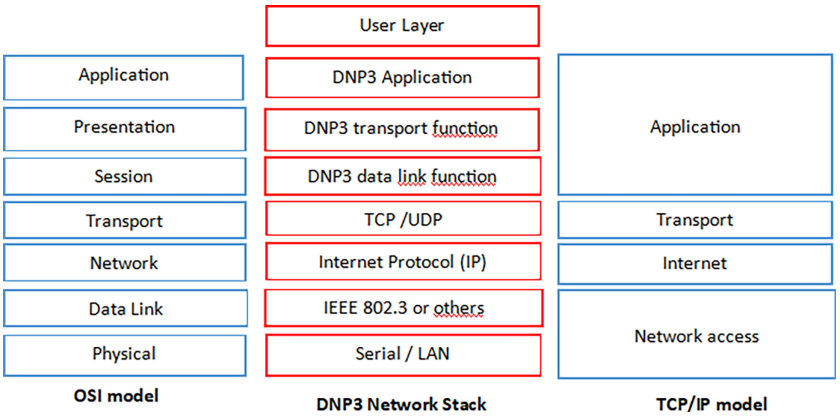

Figure 1: Overview of OSI, TCP/IP DNP3 models.

There are two types of communication: request-response communication and unsolicited communication. Request-response communication is when a remote station responds after a request is sent by the master. Unsolicited communication allows the remote station to send a message without a request from the master in order to report important events more quickly. The transmitted data does not contain detailed information, such as the name of the data, other than its type. Therefore, when establishing communication, the master requests all data from the remote station to perform synchronisation. The DNP3 protocol operates mainly at the application layer and incorporates a data link layer, a transport mechanism, and an application layer itself. The data link layer is responsible for managing station addressing, detecting transmission errors, and coordinating communications within the DNP3 protocol [14]. The transport function is responsible for dividing messages into segments of up to 249 bytes to ensure reliable transmission. It uses a control field comprising a FIR (First) bit, a FIN (Final) bit, and a 6-bit sequence number indicating the position of the segment in the overall message. Like the transport layer, the application layer can also segment messages

based on performance requirements. The header of this layer contains control fields similar to those of the transport layer. In addition, data objects are described in a specific header, which includes information about the object type (e.g., binary or analogue signals), as well as details about the associated address ranges and data types (integers or floats). The Application Layer stands on top of the EPA and OSI models. It interfaces with the DNP3 user's software and with the lower layers. The Application Layer mainly performs standardised functions, data formats, and procedures for exchanging data acquisition values, attributes, and control commands. DNP3 user software makes use of the services offered by the DNP3 Application Layer to send and receive messages with peer DNP3 devices [15].

2.1 Security of DNP3 (DNP3 SA and DNP3 Sec)

The DNP3 protocol, in its standard form, lacks built-in security features for Intelligent Electronic Devices (IEDs). Remote authentication is typically limited to a username and password, and this basic measure is available only in versions that support secure authentication. However, many IEDs ship with default, factory-set credentials. As a result, if an attacker, whether internal or external, gains access to the network, they can exploit these default settings using dictionary attacks to compromise the smart grid system [16]. DNP3 SA is the official security extension for the DNP3 application layer. Thanks to this extension, the protocol complies with IEC 62351-5. Based on open technologies, DNP3 SA uses a challenge-response mechanism with HMAC to ensure the authenticity and integrity of communications. It supports both symmetric and asymmetric cryptography for key management. In addition, this solution ensures perfect forward secrecy by allowing multiple users to be authenticated on the same device. It thus strengthens the protection of SCADA systems against attacks involving identity theft, modification, or replay.. DNP3-SA is a unilateral authentication mechanism designed to ensure that DNP3 messages exchanged between interconnected stations are protected against malicious applications. This mechanism can operate in two distinct modes: non-aggressive mode (NACR) and aggressive mode (AGM). To date, DNP3 remains one of the first standardised SCADA protocols to directly integrate cryptographic security mechanisms into its operation. When it comes to DNPSec, it's a security framework for DNP3. It effectively ensures confidentiality, authenticity, and integrity. To encrypt and authenticate its frames, DNPSec changes the original structure of the DNP3 data link layer. In this framework, encryption and authentication are done separately. DNPSec encapsulates the original DNP3 frame with a new header, a new frame sequence number, and authentication data. It uses the session key to encrypt and authenticate the frame. The session key is updated when the session time expires, or the new frame sequence number reaches its limit. DNPSec uses several encryption and authentication algorithms, namely 3-DES (Triple Data Encryption Standard) and HMACSHA-1 (keyed-Hash Message Authentication Code using Secure Hash Algorithm). However, 3-DES and SHA-1 are insecure, slow and outdated algorithms [4]. Several layered security methods, widely recognized for protecting SCADA networks, have been developed. However, these approaches have certain limitations, particularly due to their heavy reliance on the protocols used. Protocols such as SSH, SSL, IPSec, and TLS provide end-to-end security, complementing cryptographic-based encryption systems. In addition, research has been conducted specifically on application-layer security, with a particular focus on data integrity and authentication mechanisms, to counter known attacks such as modification, identity theft, and flooding [17].

2.2 Message Interruption Attack

The Fig. 2 illustrates a message-interruption attack targeting DNP3 communication in a SCADA or microgrid environment. In this scenario, after a TCP session is established between the master station and the outstation, the outstation sends an unsolicited message (DNP3 Unsolicited Message) to spontaneously

inform the master of a critical event. The attack occurs when the attacker intercepts this message, modifies it, or prevents it from reaching its destination, thereby creating a silent break in communication. This form of interruption attack exploits the lack of protection at the fragment or packet level in the DNP3 protocol, including in its secure version DNP3-SA, which does not offer end-to-end integrity checking for fragmented or injected messages at the transport level. The result is partial desynchronization of the system, in which the master station remains blind to events emitted by the outstation [16].

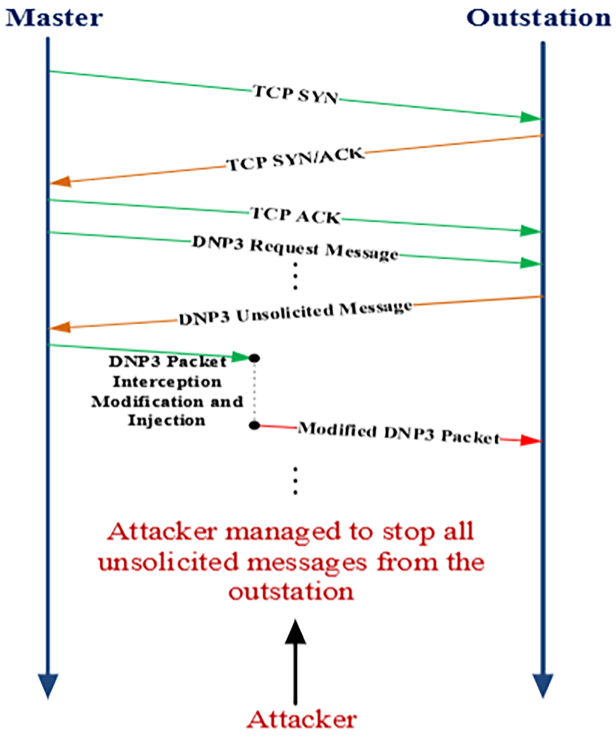

Figure 2: Interruption attack scenario on DNP3.

A DNP3 message can contain more data than a single link-layer frame can carry. For this reason, the transport layer adds sequence numbers and flags to indicate which frame is the start (FIR) or end (FIN) of a packet. This allows an application or IED to collect multiple frames and reassemble them once received. If the packet contains only one frame, both its FIR and FIN flags are set. The fragmented message interruption attack (P1) describes a scenario in which changing the FIN or FIR flags disrupts the assembly of a DNP3 message. We tested the behavior of the SCADA master and the IED when the flags were changed (and the CRC checksums were correctly recalculated). When the FIN flag was disabled, the SCADA system and the IED exhibited different behavior. The IED acknowledged, at the TCP level, several DNP3 messages with the FIN flag disabled, but after receiving several of them, it finally closed the connection with a TCP FIN. Wireshark showed that the packets were unassembled DNP3 packets. In the opposite direction, the master received packets (displayed as unassembled packets) without closing the connection. Similar behavior was observed when the FIR flag was disabled: the IED closed the connection after several messages, and the SCADA system kept the connection active. Although it is possible to disrupt packet assembly, in this scenario an attacker could interrupt communication more easily with TCP-based disruptions, such as sending a TCP RESET or retaining packets. The transport sequence modification attack (P2) notes that an attacker could predict the next transport-layer sequence number and inject additional data. Modifying a transport sequence number is not, in itself, an attack [18].

To mitigate this vulnerability, the integration of a private blockchain is proposed: each message, even if fragmented, would be recorded in a distributed ledger, time-stamped, and verified before validation by the recipient. This approach would not only detect interruptions or abnormal absences of messages but also guarantee the integrity and continuity of critical exchanges in microgrids.

3 Application of Blockchain in Microgrids

3.1 Blockchain and Scada

In microgrid systems that rely on an Internet connection, for example to access energy price data or weather forecasts for remote control purposes, external network connections can present potential vulnerabilities. These connections can serve as entry points for malicious actors who inject false data into the system, disrupting its normal operation [19]. Several key requirements must be met in microgrid communications to ensure the reliable and efficient operation of microgrid systems: Real-time capability and low latency, High reliability and system stability, Flexibility and scalability and Sufficient bandwidth capacity [20]. In the future, adopting a decentralized control architecture potentially supported by blockchain technology can strengthen the resilience of distributed microgrid systems against cyberattacks and minimize the risk associated with single points of failure. By eliminating reliance on a central node or communication pathway, the system can maintain functionality even if individual components are compromised. Furthermore, a decentralized approach enhances the scalability of microgrids, making it easier to integrate new devices without significantly impacting overall system performance [21]. Moreover, blockchain technology in grid management enhances system transparency by enabling the reading and sharing of state estimation data among grid participants. This increased transparency strengthens the reliability and resilience of network management systems [22]. Blockchain is emerging as an innovative solution to address cybersecurity challenges in distributed energy resource (DER) networks. Thanks to its decentralised, transparent, cryptographically secure and tamper-resistant properties, it enables secure peer-to-peer exchanges, access management, identity authentication and data sharing. Smart contracts ensure reliable automation of interactions, while consensus mechanisms reinforce decentralised validation, limiting the risk of failure. In this way, blockchain helps to enhance the security, transparency and reliability of distributed energy systems [23].

3.2 Architecture of the Proposed Solution

After designing the solution using the OpenDNP3 library [24], we built a small-scale test bench that simulates a hierarchical structure consisting of four outstations, a master substation and a master station, as shown in Fig. 3. The architecture follows a typical hierarchical SCADA architecture for DNP3 deployments, with a Central Master Station (CMS), a Sub Master Station (SMS) that manages several outstations (A, B, C), and a direct connection between the CMS and outstation D. We consider an attack that aims to interrupt or fragment authenticated messages between two nodes, rendering the session invalid or out of sync.

The integration of blockchain technology, through an immutable permissioned distributed ledger, mitigates structural vulnerabilities inherent in DNP3 communications while operating under clearly defined security and trust assumptions. In our architecture, each Outstation verifies CSNs and HMACs computed with securely generated symmetric keys that are provisioned during an authenticated initialization phase, stored in protected local keystores, and periodically rotated to limit exposure in case of compromise. HMAC keys are never written to the ledger; only their hash-based validation artifacts are recorded. Validators in the permissioned blockchain are authenticated entities whose write access is restricted through smart contract policies, and the system assumes that a majority of validator nodes cannot be simultaneously compromised. Each microgrid component is modeled as a blockchain node within a consortium framework (e.g., Hyperledger Fabric) [23], ensuring distributed consistency, non-repudiation between peer entities, and

resilience to temporary outages. In the specific case of interruption or fragmentation attacks exploiting the absence of integrity checks on DNP3 fragment fields (FIR, FIN, SEQ), recording per-fragment hashes on the ledger guarantees chronological order, completeness, and authenticity of exchanges. Because the ledger is append-only and tamper-evident, interruptions, packet loss, replay attempts, or desynchronization are automatically detectable and cannot be silently altered post-event. This design is particularly relevant in hierarchical microgrid architectures where centralized control servers represent single points of failure. By distributing trust across authenticated validator nodes and enforcing controlled key management and access policies, the blockchain layer enhances redundancy, strengthens forensic traceability, and improves resilience against both external attackers and insider threats targeting centralized infrastructure [25].

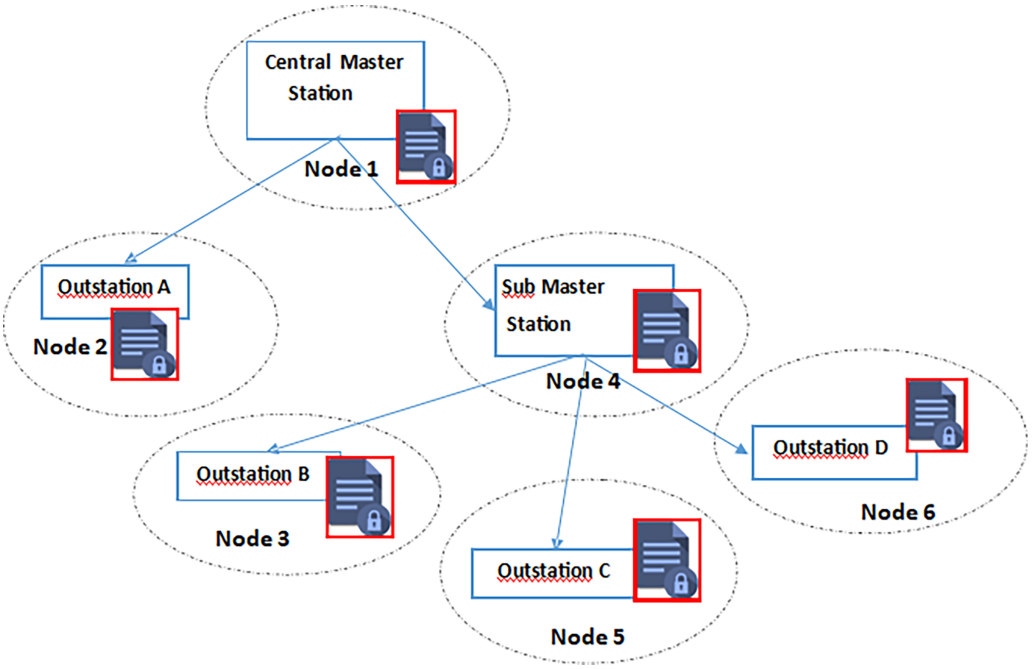

Figure 3: Topology of the blockchain solution.

Fig. 4 illustrates a secure communication model between a master station and an outstation, integrating blockchain technology to enhance the reliability of the DNP3-SA protocol against fragmentation attacks. The authenticated message is segmented (Fragment 1, Fragment 2, until fragment n.), and each fragment is encapsulated in a blockchain transaction. The blockchain acts as a distributed filter, validating the order, completeness and cryptographic consistency (via HMAC) before the fragments are delivered to the outstation. This validation ensures that only legitimate, unmodified and complete fragments are accepted, thus preventing injection attacks, incomplete fragmentation or desynchronisation. Following the authors [14], who recommend that critical fields (FIR, FIN, SEQ, addresses, and function codes) must be cryptographically protected through a mechanism that covers both the payload and the header, the HMAC computation is not limited to the fragment payload, it explicitly covers both the payload and critical header fields, including FIR, FIN, sequence number (SEQ), source and destination addresses, and function codes. This design choice ensures that the authentication mechanism protects not only data integrity but also the structural integrity of the fragmentation and reassembly process. By incorporating these header fields into the HMAC input, any attempt to manipulate fragment ordering, inject gaps, alter control flags, or modify addressing information results in an HMAC mismatch and immediate validation failure. This prevents attackers from exploiting DNP3's native lack of integrity checks on fragmentation-related fields to tamper

with reassembly logic without altering payload content. This model enhances the operational reliability of interconnected microgrids.

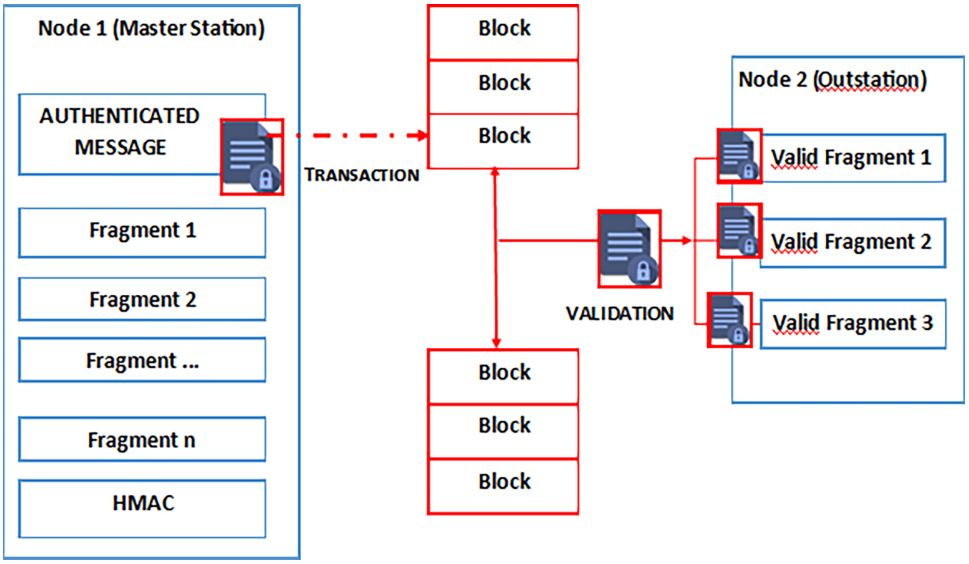

Figure 4: Principle of message fragment validation with blockchain.

4 Results

The platform used for the experiment consists primarily of the OpenDNP3 library, which emulates the central monitoring station (Master station). A DNP3 Outstation sends fragmented messages from the RTUs to the Master. The Web3 Microservice Python validator (with web3.py) compares the HMACs of received fragments with those stored in the blockchain. Given the centralized architecture of microgrids, we implemented a local Ganache blockchain in the simulated Ethereum environment to record HMAC fingerprints of transmitted fragments and to deploy a smart contract to verify and detect abnormal fragments (replay, loss, corruption) [26,27]. The choice of the Ganache private blockchain was motivated by the authors' research [28]. We carried out local deployments on virtual machines, and Docker Compose orchestrated all the containers used in this work. To better present the results, data was collected every second for 30 units, representing the simulation timeline. Between the Master and the Outstation, the DNP3 fragments are numbered from 1 to 30. Fig. 5, which shows the fragments with HMAC validation, clearly shows gaps (fragments 5, 11 and 20 missing) as well as a replayed fragment (incorrect sequence of fragment 14 in position 15). These altered transitions are typical of interruption or replay attacks, which are invisible without a security mechanism.

Each fragment is verified via an HMAC recorded in an Ethereum smart contract, thus guaranteeing its integrity, uniqueness and chronological order. Fig. 6 shows the complete and validated sequence of DNP3 fragments, thanks to a validation mechanism based on our local blockchain. We can clearly see that no fragments are missing or duplicated, and the sequence is strictly ascending, demonstrating the power of blockchain to prevent replay and fragmentation attacks in a critical context.

Fragment interruption attacks, which involve deleting or desynchronising certain packets, thereby compromising the accurate reconstruction of messages at the master station. Although the DNP3 Secure Authentication (DNP3-SA) extension improves session security through the introduction of HMAC, it does not provide fragment-by-fragment validation, leaving the protocol vulnerable to silent loss or rejection of critical fragments. The blockchain integration approach we have proposed implements a dynamic real-time

fragment validation mechanism. Fig. 6 clearly shows that for each fragment received; the master verifies the uniqueness and continuity of the sequence to detect replay and losses.

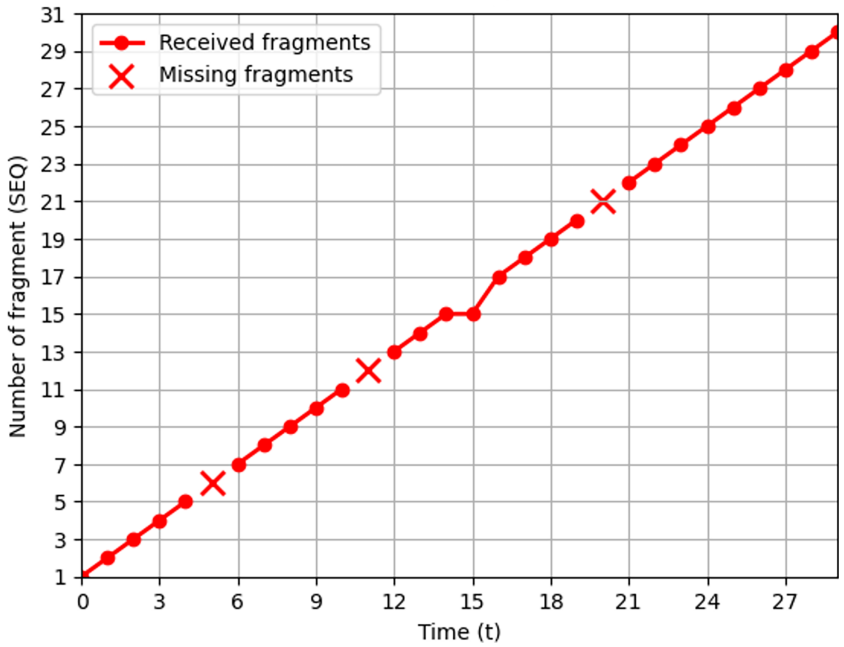

Figure 5: Before fragment validation with HMAC missing.

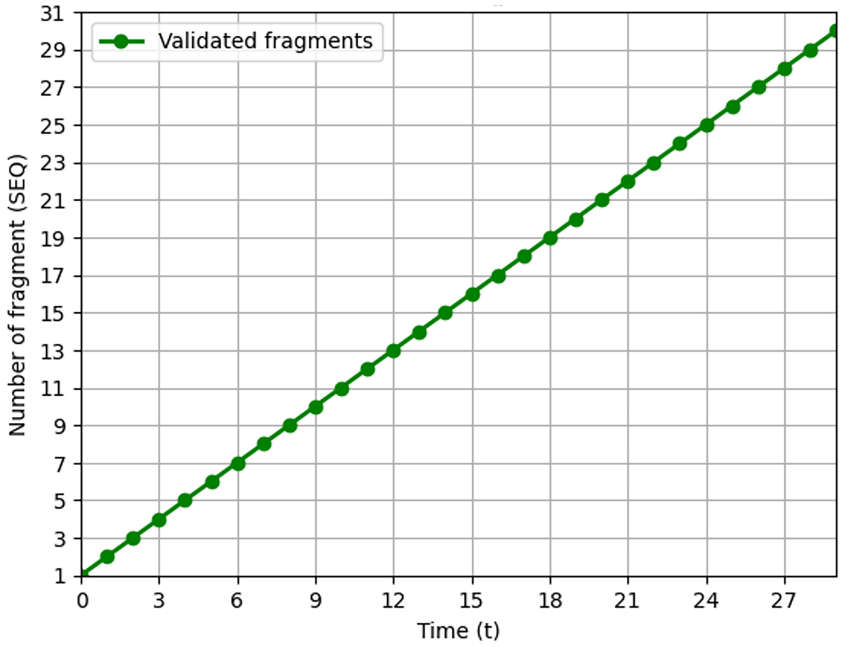

Figure 6: After validation via blockchain.

Figs. 7 and 8 jointly demonstrate both the effectiveness of the detection mechanism and the controlled overhead introduced by the blockchain layer. Fig. 7 highlights fine-grained, deterministic anomaly detection at the fragment level identifying missing fragments and replay attacks through sequential DNP3 flow analysis

based on formal rules (SEQ desynchronization, duplication, timeout), with no false positives observed in simulation. Each point represents the state of a transmitted fragment, distinguishing valid fragments (0), missing fragments (1), and replay attacks (2). The localized occurrence of non-zero values demonstrate the system's ability to precisely identify both the timing and the nature of the anomaly. This fragment-level granularity confirms that detection does not rely solely on a global authentication failure, but rather on a consistent sequential analysis of the DNP3 flow. Meanwhile, Fig. 8 shows that blockchain-based validation introduces an average latency of approximately 25 ms, remaining stable over time without progressive drift. This delay is compatible with the operational requirements of SCADA systems and secondary microgrids. Overall, the results confirm that the proposed model significantly enhances communication resilience and integrity while maintaining a manageable and acceptable performance overhead.

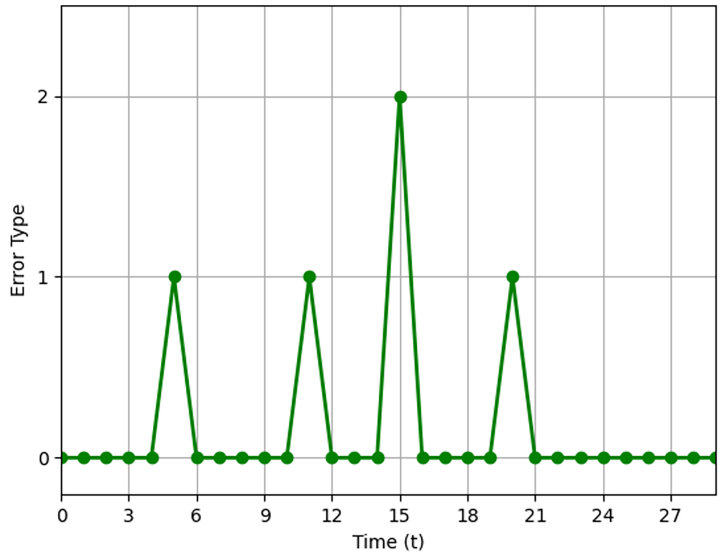

Figure 7: Fragment error detection.

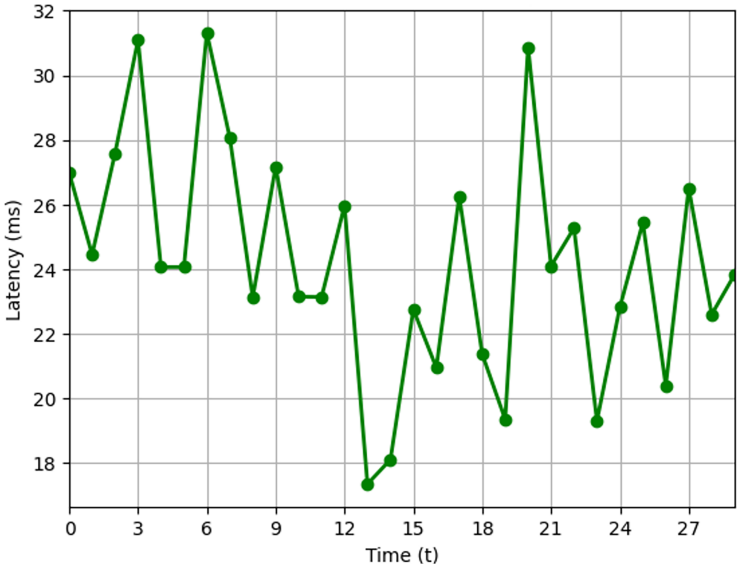

Figure 8: Blockchain-based fragment validation latency analysis.

Although this experiment was conducted in a virtualized environment composed of multiple virtual machines representing the outstations, particular attention was given to key performance parameters namely end-to-end latency, throughput, CPU/memory utilization, and scalability analysis in order to ensure that the DNP3Chain solution remains compliant with microgrid communication standards. The entire environment was hosted on a single physical laptop equipped with an Intel Core i7 processor and 32 GB of RAM. The work of authors [29] guided our evaluation framework, particularly regarding communication delay requirements in microgrids as defined by the European Telecommunications Standards Institute (ETSI) and summarized in Table 1 [28], since non-compliance with these timing constraints may result in dangerous voltage fluctuations and other adverse effects within the microgrid.

Table 1: Communication delay requirements in microgrids.

Microgrid Messages	Delay Requirement
Protection Information	4 ms
Control Information	16–100 ms
Monitoring Information	1 s
Operations and Maintenance Information	1 s
Messages requiring immediate actions at receiving controller devices	3–10 ms; 20–100 ms
Continuous data streams from controller devices	3–10 ms

These delays requirements also depend on the communication medium used between the Master and the Outstation, as well as the physical distance separating these control entities [30]. In real-world deployments, the adoption of blockchain technology may negatively impact these timing constraints depending on the consensus algorithm employed. In our approach, each DNP3 fragment (1–30 per second) is assigned an HMAC that is recorded and verified through a blockchain to detect replay and sequence interruption attacks. From a performance standpoint, the total end-to-end latency can be expressed as $T_{total} = T_{DNP3} + T_{HMAC} + T_{blockchain\_write/read} + T_{validation}$. In a local Ganache deployment, blockchain interaction typically introduces only a few milliseconds per transaction due to the absence of distributed consensus, thereby maintaining overall latency within soft real-time SCADA constraints (<100 ms), although higher than native DNP3 or DNP3-SA. Throughput is limited by the per-fragment blockchain transaction rate; with 30 fragments per second, the system remains within the processing capacity of a local Ethereum instance, which satisfies the 16–100 ms delay window required for control information in microgrids. However, scalability may degrade if fragment rates or RTU counts increase significantly due to transaction serialization and smart contract execution overhead. Furthermore, the work of authors [31] conducted under similarly conditions but with a larger number of nodes (up to 100) demonstrates reasonable latency values that remain within the limits defined by ETSI standards.

The obtained results are relevant and comparable to previous work on replay attacks, which exploit a vulnerability in dynamic authentication. However, the comparisons presented in Table 2, excluding the approaches based on centralized traditional security mechanisms that rely on protecting communication channels, such as IDS and the TLS protocol.

The comparative analysis presented in the table highlights the intrinsic limitations of the classic DNP3 protocol when faced with fragment interruption attacks. The total absence of fine validation mechanisms and protection against replay makes this protocol particularly vulnerable, leading to silent errors in the transmission of data and commands, with a high operational risk in SCADA and microgrid environments. The DNP3 Secure Authentication (DNP3-SA) extension provides a significant improvement in terms of integrity

and replay protection at the session level, but remains insufficient to specifically address fragment loss or desynchronisation within a single session. Our solution offers the unique ability to perform fragment-by-fragment validation, ensuring real-time anomaly detection, immutable traceability and automated response to attacks. This granularity of control, combined with a distributed ledger, significantly reduces the attack surface and enhances the resilience of communications in microgrids. Moreover, CPU and memory overhead increase due to Docker orchestration, Web3 processing, and blockchain state management; however, experimental results demonstrate that the entire framework remains computationally feasible on a single machine, confirming its practical deployability for small-to-medium microgrid environments.

Table 2: Comparison of fragment interruption with DNP3.

Methods of Sending Fragments to the Master by the Outstation	Real Time Detection	Protection against Interruptions and Replays	Validation Fragment by Fragment
Classic DNP3 (IEEE 1815–2012) [32]	No	No	No
DNP3 Secure Authentication (DNP3 SA) [25]	Partial (validation at session level)	Yes (for each session)	No
Securing Networked Microgrids with DNP3 (Soliman 2021) [33]	Partial	Yes (per message)	No
Securing Microgrid Operation through DNP3 (Soliman 2021 IAS) [34]	Partial	Yes (per message)	No
Design and Evaluation of a Cyber-Physical Resilient Power System Testbed (arXiv 2020) [35]	Yes	Partial	No
Networked Microgrid Cybersecurity Architecture Design Guide—A New Jersey TRANSITGRID Use Case (NJT 2023) [36]	Partial	Partial	No
Distributed IDS for SCADA DNP3 (arXiv 2024) [37]	Yes	Partial	No
Cyber-Physical Security for Microgrids via Digital Twin (2025) [38]	Yes	Partial	No
Our solution: DNP3Chain	Yes	Yes (for each fragment)	Yes

Given the above, Table 3 presents a comparative assessment of the security mechanisms provided by the DNP3 protocol, its secure extension DNP3-SA, and the proposed DNP3Chain architecture, which incorporates a blockchain layer. The comparison is conducted using measurable technical criteria, including fragment integrity, replay protection, real-time detection capability, control granularity, and temporal overhead. This analysis aims to quantify the level of resilience offered by each approach within SCADA and

microgrid environments, to identify the structural limitations inherent in conventional solutions, and to demonstrate the scientific contribution of fragment-level distributed validation.

Table 3: Comparative security analysis of DNP3, DNP3-SA, and DNP3Chain in SCADA.

Feature	DNP3	DNP3-SA	DNP3Chain
Fragment Integrity	Not protected	Partial (HMAC per message)	Verified per fragment
Replay Protection	None	Limited (challenge-based)	Blockchain uniqueness check
Missing Fragment Detection	No native detection	Not explicit	Timeout + ledger verification
Real-Time Detection Window	Not defined	Dependent on session validation	$\Delta T_{detect} \approx 20–30$ ms
Detection Trigger	None	HMAC mismatch	SEQ mismatch, missing fragment, duplicate hash
Alarm Mechanism	None	Authentication failure only	Smart-contract event + SCADA alert
Audit Trail	No	Limited	Immutable distributed log
False Positive Rate	High (undetected)	Moderate	Low (hash-based verification)
Detection Granularity	Message level	Message level	Fragment level
Latency Overhead	None	~5–10 ms	~20–30 ms

The comparative table highlights a structured progression of security mechanisms across DNP3, DNP3-SA, and the proposed DNP3Chain architecture. While the native DNP3 protocol does not provide intrinsic mechanisms for detecting interruption, replay, or fragment loss, DNP3-SA introduces challenge–response–based authentication combined with HMAC, thereby enhancing message authenticity without explicitly guaranteeing the detection of missing fragments or fine-grained control at the transport level. In contrast, DNP3Chain extends protection to the fragment level by integrating a blockchain-based ledger that enables verification of the uniqueness, ordering, and integrity of each fragment within a bounded detection window ($\Delta T\_detect \approx 20–30$ ms). This approach transforms anomaly detection from a reactive mechanism (authentication failure) into a proactive and deterministic process based on sequential consistency and distributed cryptographic validation.

5 Conclusion

In this project, we looked at how secure the DNP3, and DNP3-SA are when using a microgrid SCADA environment by looking specifically at how fragmentation of messages can create security holes due to how these messages are managed (handled). Although DNP3-SA does improve the authentication and session integrity of both protocols, it does not prevent validation of each fragmented message from being completed before being sent onwards for processing in other systems such as master stations (MS) and outstations (OS). As a result, DNP3-SA and all DNP3 protocol implementations face the risk of fragments being interrupted, unrecoverable, replayed back into the network or manipulated based on sequence to cause the master station and outstation communication systems to get out of sync.

To bridge this gap, we developed a blockchain-based solution, DNP3Chain, that enables real-time, immutable validation of each DNP3 fragment and assigns each fragment a unique HMAC fingerprint. Smart-contract logic validates each fragment. We validated our concept in a test environment using an OpenDNP3 testbed and a private Ethereum/Ganache blockchain. Based on the results of our experiments, we can see that the proposed solution accurately detects missing fragments, identifies replay-blob injections, and finds sequences of injections not present in the normal DNP3 or DNP3-SA protocols. The introduction of DNP3Chain significantly enhances message integrity and operational resilience in hierarchical architectures for microgrid-type environments.

While the results of this study show promise and can lead to improved operational performance when using DNP3Chain, deploying the blockchain-based solution in a microgrid also presents challenges, including communication network resource consumption and storage overhead costs. Future studies will need to investigate lightweight consensus algorithms for microgrids, develop a scalable deployment framework, and optimize performance in microgrid environments to assess their impact on real-world microgrid operation. Overall, the creation of DNP3Chain demonstrates how blockchain technology can strengthen the overall cybersecurity and reliability of next-generation distributed systems for storing and delivering energy. Under sustained-attack conditions, DNP3Chain ensures controlled degradation rather than service disruption by rejecting malicious fragments, triggering bounded retry and session reset mechanisms, and applying rate limiting to prevent self-inflicted denial-of-service. Persistent anomalies result in structured security events that are tamper-evidently recorded, and communication can be redirected to backup nodes in redundant deployments. To enhance operational resilience, operator notification is recommended through SCADA alarms, SIEM (Security Information and Event Management) integration, or supervisory dashboards, enabling real-time alerting, rapid incident response, and comprehensive forensic visibility without compromising system availability.

Acknowledgement: The authors acknowledge the administrative support of their university, whose provision of institutional resources and logistical assistance significantly contributed to the successful completion of this work.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Benedict Djouboussi: conceptualization, data collection and processing, formal analysis, methodology, resources, writing—original draft, writing—review & editing. Elie Fute Tagne: conceptualization, supervision, methodology, review & editing. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The data used to support the findings of this study are included within this article.

Ethics Approval: Not applicable.

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

References

1. Kumar S, Islam S, Jolfaei A. Microgrid communications—Protocols and standards. In: Variability, scalability and stability of microgrids. London, UK: Institution of Engineering and Technology; 2019. p. 291–326. doi:10.1049/pbpo139e_ch9.
2. Shahzad A, Lee M, Kim H, Woo SM, Xiong N. New security development and trends to secure the SCADA sensors automated transmission during critical sessions. Symmetry. 2015;7(4):1945–80. doi:10.3390/sym7041945.
3. Bel O, Kim J, Hofer WJ, Maharjan M, Hyder B, Purohit S, et al. Co-simulation framework for network attack generation and monitoring. IEEE Access. 2024;12:142227–40. doi:10.1109/access.2024.3468272.
4. Musa S, Shahzad A, Aborujilah A. Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security. In: Proceedings of the 7th International

Conference on Ubiquitous Information Management and Communication. New York, NY, USA: The Association for Computing Machinery (ACM); 2013. p. 1–8. doi:10.1145/2448556.2448588.
5. Shahzad A, Udagepola KP, Lee YK, Park S, Lee M. The sensors connectivity within SCADA automation environment and new trends for security development during multicasting routing transmission. Int J Distrib Sens Netw. 2015;2015(4):738687. doi:10.1155/2015/738687.
6. Amoah R, Camtepe S, Foo E. Formal modelling and analysis of DNP3 secure authentication. J Netw Comput Appl. 2016;59:345–60. doi:10.1016/j.jnca.2015.05.015.
7. Reihs D, Bouda F, Leimgruber F, Machtinger K, Strasser TI, Stefan M, et al. Unlocking customer flexibilities through standardized communication interfaces'. Elektrotech Inftech. 2023;140(5):441–51. doi:10.1007/s00502-023-01153-1.
8. Siniosoglou I, Radoglou-Grammatikis P, Efstathopoulos G, Fouliras P, Sarigiannidis P. A unified deep learning anomaly detection and classification approach for smart grid environments. IEEE Trans Netw Serv Manag. 2021;18(2):1137–51. doi:10.1109/TNSM.2021.3078381.
9. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023;12(6):1333. doi:10.3390/electronics12061333.
10. Allah Bakhsh S, Shahbaz Khan M, Saidani O, Alasbali N, Abbas SQ, Almas Khan M, et al. Enhancing security in DNP3 communication for smart grids: a segmented neural network approach. IEEE Access. 2025;13:110436–56. doi:10.1109/access.2025.3580507.
11. Jamil N, Qassim QS, Bohani FA, Mansor M, Ramachandaramurthy VK. Cybersecurity of microgrid: state-of-the-art review and possible directions of future research. Appl Sci. 2021;11(21):9812. doi:10.3390/app11219812.
12. Shahzad A, Lee M, Xiong N, Jeong G, Lee YK, Choi JY, et al. A secure, intelligent, and smart-sensing approach for industrial system automation and transmission over unsecured wireless networks. Sensors. 2016;16(3):322. doi:10.3390/s16030322.
13. Pliatsios D, Sarigiannidis P, Lagkas T, Sarigiannidis AG. A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Commun Surv Tutor. 2020;22(3):1942–76. doi:10.1109/comst.2020.2987688.
14. Patwardhan M. DNP3: Security and scalability analysis [dissertation]. Sacramento, CA, USA: California State University; 2012.
15. Darwish I, Igbe O, Celebi O, Saadawi T, Soryal J. Smart grid DNP3 vulnerability analysis and experimentation. In: Proceedings of the 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing; 2015 Nov 3–5; New York, NY, USA. p. 141–7. doi:10.1109/cscloud.2015.86.
16. Yin XC, Liu ZG, Nkenyereye L, Ndibanje B. Toward an applied cyber security solution in IoT-based smart grids: an intrusion detection system approach. Sensors. 2019;19(22):4952. doi:10.3390/s19224952.
17. Rodriguez JDP, Boakye-Boateng K, Kaur R, Zhou A, Lu R, Ghorbani AA. SoK: a reality check for DNP3 attacks 15 years later. Smart Cities. 2024;7(6):3983–4001. doi:10.3390/smartcities7060154.
18. Zhang H, Yue D, Dou C, Hancke GP. Resilient optimal defensive strategy of micro-grids system via distributed deep reinforcement learning approach against FDI attack. IEEE Trans Neural Netw Learn Syst. 2024;35(1):598–608. doi:10.1109/TNNLS.2022.3175917.
19. Zhang Z, Turnbull B, Kermanshahi SK, Pota H, Damiani E, Yeun CY, et al. A survey on resilient microgrid system from cybersecurity perspective. Appl Soft Comput. 2025;175(3):113088. doi:10.1016/j.asoc.2025.113088.
20. Muhammad M, Alshra'a AS, German R. Survey of cybersecurity in smart grids protocols and datasets. Procedia Comput Sci. 2024;241(3):365–72. doi:10.1016/j.procs.2024.08.049.
21. Banks C, Kim S, Neposchlan M, Velez N, Duncan KJ, James J. Blockchain for power grids. In: Proceedings of the 2019 SoutheastCon; 2019 Apr 11–14; Huntsville, AL, USA. p. 1–5. doi:10.1109/SoutheastCon42311.2019.9020573.
22. Ibrahim O. Blockchain-enabled cybersecurity frameworks for distributed energy resource (DER) networks; 2025. [cited 2026 Jan 1]. Available from: https://www.researchgate.net/publication/392734294_BLOCKCHAIN-ENABLED_CYBERSECURITY_FRAMEWORKS_FOR_DISTRIBUTED_ENERGY_RESOURCE_DER_NETWORKS.
23. Singh C, Nivangune A, Patwardhan M. Function code based vulnerability analysis of DNP3. In: Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS); 2016 Nov 6–9; Bangalore, India. p. 1–6. doi:10.1109/ANTS.2016.7947865.

24. Amanlou S, Hasan MK, Asma' Mokhtar U, Mahmood Malik K, Islam S, Khan S, et al. Cybersecurity challenges in smart grid systems: current and emerging attacks, opportunities, and recommendations. IEEE Open J Commun Soc. 2025;6(1):1965–97. doi:10.1109/ojcoms.2025.3545153.
25. Tempesta S, Peña MJ. Developing blockchain solutions in the cloud: Design and develop blockchain-powered Web3 apps on AWS, Azure, and GCP. Birmingham, UK: Packt Publishing Ltd.; 2024.
26. Alshudukhi KS, Ali Khemakhem M, Eassa FE, Jambi KM. An interoperable blockchain security frameworks based on microservices and smart contract in IoT environment. Electronics. 2023;12(3):776. doi:10.3390/electronics12030776.
27. Alrashede H, Eassa F, Ali AM, Aljihani H, Albalwy F. Enhancing east-west interface security in heterogeneous SDN via blockchain. PeerJ Comput Sci. 2025;11(12):e2914. doi:10.7717/peerj-cs.2914.
28. Kondoro A, Dhaou I, Tenhunen H, Mvungi N. A low latency secure communication architecture for microgrid control. Energies. 2021;14(19):6262. doi:10.3390/en14196262.
29. Ortega A.Shinoda A.Schweitzer CM, Granelli F, Ortega AV, Bonvecchio F. Performance evaluation of the DNP 3 protocol for smart grid applications over IEEE 802.3/802.11 networks and heterogeneous traffic. [cited 2026 Mar 1]. Available from: https://www.semanticscholar.org/paper/Performance-Evaluation-of-the-DNP-3-Protocol-for-.-Ortega-Shinoda/da4e51560615224c0f066441f2d2fb7e0cfa4025.
30. Marino DL, Wickramasinghe CS, Singh VK, Gentle J, Rieger C, Manic M. The virtualized cyber-physical testbed for machine learning anomaly detection: a wind powered grid case study. IEEE Access. 2021;9:159475–94. doi:10.1109/ACCESS.2021.3127169.
31. Siddavatam IA, Kazi F. Security assessment framework for cyber physical systems: a case-study of DNP3 protocol. In: Proceedings of the 2015 IEEE Bombay Section Symposium (IBSS); 2015 Sep 10–11; Mumbai, India. p. 1–6. doi:10.1109/IBSS.2015.7456631.
32. Zografopoulos I, Konstantinou C. DERauth: A battery-based authentication scheme for distributed energy resources. In: Proceedings of the 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI); 2020 Jul 6–8; Limassol, Cyprus. p. 560–7. doi:10.1109/isvlsi49217.2020.00086.
33. Soliman AS, Saad AA, Mohammed O. Securing networked microgrids with DNP3 protocol. In: Proceedings of the 2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe); 2021 Sep 7–10; Bari, Italy. p. 1–6. doi:10.1109/eeeic/icpseurope51590.2021.9584818.
34. Soliman AS, Saad AA, Mohammed O. Securing networked microgrids operation through DNP3 protocol implementation. In: Proceedings of the 2021 IEEE Industry Applications Society Annual Meeting (IAS); 2021 Oct 10–14; Vancouver, BC, Canada. p. 1–6. doi:10.1109/ias48185.2021.9677139.
35. Sahu A, Wlazlo P, Mao Z, Huang H, Goulart A, Davis K, et al. Design and evaluation of a cyber-physical resilient power system testbed. IET Cyber-Phys Syst Theory Appl. 2021;6(4):208–27. doi:10.1049/cps2.12018.
36. Networked microgrid cybersecurity architecture design guide—A New Jersey TRANSITGRID use case. [cited 2025 Dec 28]. Available from: https://www.researchgate.net/publication/365801573_Networked_Microgrid_Cybersecurity_Architecture_Design_Guide_-_A_New_Jersey_TRANSITGRID.
37. Mohan SN, Ravikumar G, Govindarasu M. Distributed intrusion detection system using semantic-based rules for SCADA in smart grid. In: Proceedings of the 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D); 2020 Oct 12–15; Chicago, IL, USA. p. 1–5. doi:10.1109/td39804.2020.9299960.
38. Canaan B, Makhlouf Y, Ould Abdeslam D. Cyber-physical security for microgrids through Digital Twin technologies: a review and research outlook. Energy Convers Manag X. 2025;28(16):101406. doi:10.1016/j.ecmx.2025.101406.