A Data Rate Monitoring Approach for Cyberattack Detection in Digital Twin Communication

Cláudio H. Albuquerque Rodrigues *, Waldir S. S. Júnior, Wilson Dias de Oliveira, Isomar Silva

Posted Date: 14 October 2025

doi: 10.20944/preprints202510.1127.v1

Keywords: Digital Twins; Data Rate; Cyberattacks; IIoT Security

 doi:10.20944/preprints202510.1127.v1

Article

A Data Rate Monitoring Approach for Cyberattack Detection in Digital Twin Communication

Cláudio Rodrigues [1,2], Waldir S. S. Júnior [2], Wilson Oliveira [3] and Isomar Silva [1,*]

[1] Conecthus Institute - Technology and Biotechnology of Amazonas
[2] Federal University of Amazonas - UFAM
[3] Ulbra Manaus - Universidade Luterana do Brasil
* Correspondence: claudio.rodrigues@conecthus.org.br; Tel.: +55-92-98113-4537

Abstract

The increasing integration of Digital Twins (DTs) in Industry 4.0 environments establishes the physical-virtual communication layer as a critical vector for cyber vulnerabilities. Current literature predominantly focuses on complex security mechanisms, leaving a gap in the exploration of fundamental and computationally cost-effective network metrics. This paper addresses this gap by validating a non-intrusive attack detection method based exclusively on monitoring data rate throughput. A Docker simulation environment was used to emulate Denial of Service (DoS), Man-in-the-Middle (MiTM), and other intrusion attacks. The results demonstrate that each attack produces a distinct and detectable statistical signature. For example, the DoS attack caused a 50-fold increase in packet rate. We conclude that data rate analysis represents a viable and complementary approach to IIoT security, providing a robust, interpretable, and cost-effective first line of defense towards developing more resilient Digital Twins.

Keywords: digital twins; data rate; cyberattacks; IIoT security

1. Introduction

The adoption of Digital Twins (DTs) has become a fundamental pillar of Industry 4.0, transforming the way complex systems are monitored, analyzed, and optimized in real-time [1,2]. By creating a dynamic, high-fidelity virtual representation of a physical asset or process, DTs enable more precise and proactive decision-making, with applications ranging from manufacturing to critical infrastructure management [3,4]. The operation of this technology fundamentally relies on a continuous, bidirectional data stream that synchronizes the state between the physical asset and its digital counterpart.

Despite its operational advantages, this persistent interconnection introduces a novel and critical vector for cyber vulnerabilities. The communication layer, responsible for transporting data from IIoT sensors and PLC commands, becomes a primary attack surface where the integrity, confidentiality and availability of data can be compromised [5,6]. Attacks targeting this channel can corrupt the fidelity of the Digital Twin and may also trigger hazardous actions within the physical system. These effects can lead to severe operational disruptions and safety risks.

Recent literature has investigated various approaches to mitigate these risks, including the use of machine learning and blockchain technologies for anomaly detection and data integrity assurance [7–9]. However, as highlighted in our systematic review presented in Section 2, a notable gap remains: the lack of detection methods focusing on fundamental, low-level, and computationally efficient network metrics. Specifically, the use of data throughput as a primary indicator for detecting a broad spectrum of attacks—from service disruptions to subtle data manipulations—has been comparatively underexplored.

To address this gap, this paper proposes and validates a non-intrusive methodology for detecting cyberattacks in Digital Twin communications based on monitoring and analyzing data rate anomalies.

 doi:10.20944/preprints202510.1127.v1

The primary objective is to demonstrate the feasibility of using this metric as an early warning sign of malicious activities. Accordingly, this study characterizes data rate behavior under normal, fault, and various simulated attack scenarios (e.g., DoS, MiTM), demonstrating identifiable anomaly patterns correlated with security events.

The remainder of this paper is organized as follows. Section 2 presents a critical review of the literature, which underpins the contribution of this work. Section 3 details the methodology used, including the architecture of the simulation environment and the procedures for data collection and analysis. Section 4 presents and discusses the results obtained from the simulation experiments. Finally, Section 5 concludes the paper, summarizing the findings, discussing the implications, and suggesting directions for future research.

2. Background

The transition to cyber-physical production systems enabled by Digital Twins fundamentally depends on the integrity and security of the data stream connecting the physical and virtual domains. To contextualize the contribution of this work, this section provides a critical review of the literature, beginning with the architectures and inherent connectivity challenges of Industrial Digital Twins. Next, it examines the broader landscape of cybersecurity and threat detection within Operational Technology (OT) and IIoT environments, where these Digital Twins are deployed. The focus then narrows to studies specifically addressing intrusion detection in physical-virtual communication—the central topic of this review. The section concludes by identifying research gaps and situating the contribution of the present study within this context.

To conduct this critical review, a systematic search strategy was designed and executed across major scientific databases, such as IEEE Xplore and the ACM Digital Library. The search string employed was: ("digital twin" OR "digital twins") AND ("intrusion detection" OR "attack detection" OR "anomaly detection" OR "threat detection" OR detection) AND ("industrial IoT" OR IIoT OR "industrial control system"). Following the initial retrieval, the results were subjected to a rigorous filtering process, prioritizing publications from 2020 onward and the relevance of the search terms within the title and abstract. This process yielded a final set of 22 articles, representing the state-of-the-art at the intersection of Digital Twins and threat detection. Table 1 consolidates the key characteristics of these studies, providing the foundation for the analysis developed in subsequent subsections.

Table 1. Summary of the Most Relevant Articles in the Systematic Review.

Reference	System Type	Security Focus	Detection	Monitor. Metric	Technique	Attacks	Validation
[9]	IIoT	D, P	AN	DR, SC	FL, DL	DDoS	Simulation
[7]	Industrial	I, R, A	PR	SC, NF	BC	DI, FR	Theoretical
[10]	IIoT	D, I	CA	NF	BC, ML	GA	Simulation
[11]	ICS	D	AN	SC	DT, ML	GA	Simulation
[12]	ICS	D	AN(S)	SC	DT, Sim.	GA	Simulation
[13]	CPS	D	AN	SC	ML, DT	GA	Simulation
[8]	IIoT	D, P, R	CA	NF, SC	FL	IN	Simulation
[14]	CPS	D	AN(C)	NF	DT	GA	Simulation
[15]	IIoT	D, I	AD	NF	Testbed	DA	Testbed
[16]	CPS	D	TD	SC	DRL, IoT, DT	TCPS	Simulation
[17]	ICS	D	AN	SC	DT, DL	GA	Simulation
[18]	CPS	D, R	HY(A)	SC, NF	DT, Hybrid	GA	Simulation
[19]	IIoT	D	AN(B)	SC	DT, ML	GA	Simulation
[20]	IIoT	D	AN	SC	DT, ML	GA	Simulation
[21]	ICS	D	IN(A)	SC	DT, ML	IN	Simulation
[22]	ICS	D	AN(D)	SC	DT, ML	CA	Simulation
[23]	ICS	C, I, D	SA	SC, NF	DT, Data	GT	Simulation
[24]	Industrial	P	AN	SC	HMMs	FA	Dataset
[25]	Industrial	A, I	PD	SC	BC, AI	FR	Simulation

 doi:10.20944/preprints202510.1127.v1

Table 1. *Cont.*

Reference	System Type	Security Focus	Detection	Monitor. Metric	Technique	Attacks	Validation
[26]	ICS	D	FD	SC	DT	CA	Simulation
[27]	IIoT	C, A	TM	SC	DT, BC	MB	Simulation
[28]	Industrial	D	AN(SH)	SC	DT, ML	GT	Simulation

System Type: IIoT (Industrial Internet of Things), ICS (Industrial Control System), CPS (Cyber-Physical System). **Security Focus:** C (Confidentiality), I (Integrity), D (Availability), P (Privacy), R (Resilience), A (Authenticity). **Detection:** AN (Anomaly), PR (Prevention), CA (Collab. Anomaly), AN(S) (Anomaly, Sim.), AN(C) (Anomaly, Collab.), AD (Attack Detection), TD (Threat Detection), HY(A) (Hybrid, Anomaly), AN(B) (Anomaly, Behav.), IN(A) (Intrusion, Anomaly), AN(D) (Anomaly, Defense), SA (Situational Aware.), PD (Prediction), FD (Fault Detection), TM (Trust Management), AN(SH) (Anomaly, Self-heal.). **Monitoring Metric:** DR (Data Rate), SC (System Comp.), NF (Network Flow). **Technique:** ML (Machine Learning), DL (Deep Learning), FL (Federated Learning), BC (Blockchain), DRL (Deep Reinforcement Learning). **Attacks:** DI (Data Injection), FR (Fraud), GA (Generic Attacks), IN (Intrusions), DA (Diverse Attacks), TCPS (Threats in CPS), CA (Cyberattacks), GT (Generic Threats), FA (Faults), MB (Malicious Behavior).

2.1. Digital Twins: Concepts, Architectures, and Connectivity Challenges

A Digital Twin (DT) is a dynamic and high-fidelity virtual representation of a physical asset, process, or system [1]. This digital representation is continuously synchronized through the real-time collection of data from sensors and other sources in the physical environment, enabling it to mirror the behavior and characteristics of its physical counterpart for observation, analysis, and operational optimization [3,19,29,30]. A fundamental pillar of this technology lies in the bidirectional interaction between the physical domain and its digital counterpart: real-world data feeds the virtual model, which, in turn, can generate insights to influence the physical system, establishing a continuous cycle of control and enhancement [3,19]. The implementation of DTs is enabled by the convergence of technologies such as the Internet of Things (IoT), artificial intelligence (AI), and machine learning (ML) [30,31]. Their intrinsically connected nature and the dependence on data exchange underscore the critical importance of communication security [5,6,32].

Building an effective Digital Twin (DT) requires a robust architecture. While various models are proposed in the literature [3,19,33], a fundamental set of core components is shared. Conceptually, a DT architecture can be structured into several key layers. The first layer is the physical entity, representing the real-world system and including the sensors and actuators responsible for data collection and interaction [5,6]. The second layer is the virtual model, the digital representation comprising components ranging from 3D models to AI algorithms used to process data, simulate scenarios, and optimize operations [30,34]. Serving as the bridge between these layers, the data connection layer enables the bidirectional flow of information, where IoT and communication network technologies are crucial [5,6,32]. Finally, the service and application layer utilizes the insights generated by the DT to deliver value through control dashboards, predictive maintenance tools, and decision-support systems [19,33].

The seamless integration of these layers facilitates the successful application of DTs across domains ranging from manufacturing to smart city management [3,4]. It is evident that the data connection layer serves as the central nervous system of the entire architecture. Its integrity and availability are not only critical functional requirements but also constitute the primary potential attack surface. Therefore, understanding the security challenges inherent in this connectivity is a prerequisite for developing more resilient DT systems, a topic explored in the following section.

2.2. Cybersecurity and Threat Detection in IIoT/OT Environments

Securing Operational Technology (OT) and Industrial Internet of Things (IIoT) environments presents a unique set of challenges distinct from those in traditional IT environments [35]. Ensuring the availability and integrity of critical physical processes—often operating in real time—coexists with the proliferation of resource-constrained devices and heterogeneous communication protocols, including legacy systems [5,35]. This complex scenario demands security approaches that transcend

 doi:10.20944/preprints202510.1127.v1

conventional network perimeters, focusing on detecting anomalies and malicious behaviors directly within data traffic and system operations.

The research community has concentrated on developing increasingly sophisticated Intrusion Detection Systems (IDS) for these environments. Many proposed solutions utilize machine learning and deep learning techniques to analyze network traffic and identify deviations from normal behavior [16]. However, the sophistication of these detection mechanisms introduces new vulnerabilities. Studies such as [36] demonstrate that deep learning-based detection systems can be vulnerable to evasion attacks, where adversaries deliberately manipulate input data to deceive the detection model. This highlights that, despite advanced techniques, threat detection in complex distributed systems remains an ongoing challenge.

The introduction of a Digital Twin into an IIoT/OT environment, while providing operational benefits, exacerbates these security challenges. The DT not only inherits the vulnerabilities of the ecosystem in which it is embedded but also creates a new and attractive attack vector: the continuous, high-value data stream that feeds it. Therefore, threat detection cannot be limited to a generic analysis of industrial network traffic; methods capable of scrutinizing the integrity of the specific communication between the physical and virtual domains must be developed, as discussed in the following section.

2.3. Intrusion Detection in the Physical–Virtual Communication of Digital Twins

The fidelity and utility of a Digital Twin are directly proportional to the integrity of the bidirectional communication with its physical counterpart. As highlighted previously, ensuring the confidentiality, integrity, and availability (CIA) of this channel is imperative [5,6]. Any compromise of this data stream—whether through manipulation, interception, or disruption—can invalidate the virtual model and lead to erroneous or hazardous operational decisions in the physical environment [37]. Therefore, this section focuses on studies that directly address threat detection at this communication layer.

The recent literature proposes several strategies to address these challenges. A significant line of research applies machine learning and deep learning techniques for anomaly detection. For example, [7] explore the use of Federated Learning to train intrusion detection models in a distributed manner, thereby preserving data privacy. Others, such as [9], apply a similar approach with a specific focus on detecting Distributed Denial of Service (DDoS) attacks in IIoT networks that support Digital Twins. In parallel, there is growing interest in using blockchain to ensure the integrity and traceability of exchanged data. Studies such as [10] and [8] propose architectures in which data transactions between the physical and virtual domains are immutably recorded, preventing undetected manipulation.

However, a critical analysis of these contributions reveals a notable gap. Although effective against certain types of attacks, many of these approaches introduce significant computational and latency overheads (as in the case of blockchain) or require large volumes of labeled data for training (as with supervised deep learning). More importantly, few studies investigate low-level network metrics, such as throughput, as primary security indicators. The hypothesis that subtle or abrupt variations in the volume and frequency of data packets can signal different classes of attacks—ranging from DoS disruptions to reconnaissance activities or false data injection—remains relatively underexplored. This shortcoming justifies the investigation of a lightweight, computationally inexpensive detection method focused directly on the fundamental behavior of the communication channel.

2.4. Emerging Cyber Threats and Their Impacts

Digital Twin security deals not only with known threats but also with a constantly evolving attack landscape. The growing sophistication of threats such as Advanced Persistent Threats (APT) and AI-powered attacks, designed to be stealthy and long-term, presents a particular challenge. Such attacks may not aim for immediate service disruption but rather for the continuous exfiltration of data or the subtle and gradual manipulation of physical operations by corrupting the data stream that feeds the Digital Twin.

 doi:10.20944/preprints202510.1127.v1

This new generation of threats tests the limits of existing detection mechanisms. Evasion attacks are specifically designed to bypass AI-based systems by subtly manipulating input data to be misclassified as benign traffic [36]. Furthermore, these new attack capabilities exacerbate systemic concerns about data privacy and security in Digital Twins, which can lead to large-scale data manipulation or critical information leakage, as reviewed in [37].

The impact of these emerging threats on the physical-virtual communication flow is, therefore, direct. A sophisticated attack may not generate an obvious traffic spike like a DDoS, but it can alter the frequency, size, or regularity of data packets, subtly deviating from the operational baseline. This reinforces the need for monitoring approaches sensitive to fundamental variations in the communication channel. The data rate analysis proposed in this work offers such a defense-in-depth mechanism, capable of detecting anomalies that more specialized methods focused on signatures or high-level behaviors might overlook.

2.5. Literature Gaps and Proposed Contribution

The literature analysis reveals a vibrant research field with significant advances in defining Digital Twin architectures and applying techniques such as machine learning and blockchain to enhance security in IIoT environments. Despite this progress, our systematic review highlights critical gaps that remain and motivates the present investigation. The main identified gaps are as follows:

- Architectures with reactive security: most architectural models treat security as an adjacent layer rather than as an intrinsic design principle. There is a lack of proposals for architectures conceived from the outset to facilitate intrusion detection within communication flows, while accounting for the performance constraints of IIoT.
- Focus on complex high-level methods: predominant detection strategies rely on computationally intensive methods (e.g., deep learning, federated learning, blockchain) or on system-level behavioral analysis, while neglecting fundamental, low-cost communication channel metrics.
- Lack of throughput-focused detection: specifically, the exploration of data throughput as a primary indicator for detecting a wide range of attacks—from service disruptions to subtle manipulations—remains notably underexplored in the Digital Twin literature.
- Limited validation against emerging threats: there is a pressing need for experimental validation of detection strategies capable of operating in real time and maintaining DT resilience under sophisticated stealthy attacks that target data integrity rather than simply causing denial of service.

In light of these gaps, this article proposes and validates an approach for detecting cyberattacks in the communication of industrial Digital Twins, based on monitoring and analyzing anomalies in data throughput. The investigated method aims to provide a non-intrusive, computationally lightweight, and complementary solution to existing strategies, thereby contributing to the development of more secure and resilient Digital Twin architectures in IIoT environments.

3. Materials and Methods (Methodology)

The experimental environment was developed using Docker containerization technology. This platform was selected for its ability to create isolated, lightweight, and reproducible environments, making it ideal for simulating the complex architecture of a Digital Twin system. The simulation architecture comprised three main container types, each fulfilling a specific role:

- Simulated physical device containers: These containers emulate the behavior of Programmable Logic Controllers (PLC) and Industrial Internet of Things (IIoT) devices.
- Digital twin container: This container hosts the virtual representation of the physical devices and is implemented as a system capable of receiving, processing, and storing data across various protocols.
- Monitoring container (Sniffer): Operating as a dedicated component, this container is responsible for capturing and analyzing network traffic without interfering with the primary data flow.

 doi:10.20944/preprints202510.1127.v1

An overview of the proposed method is illustrated in Figure 1. The monitoring system (Sniffer) non-intrusively observes the communication channel that links the Physical World and its digital representation, the Digital Twin, to detect anomalies that may indicate a cyberattack.

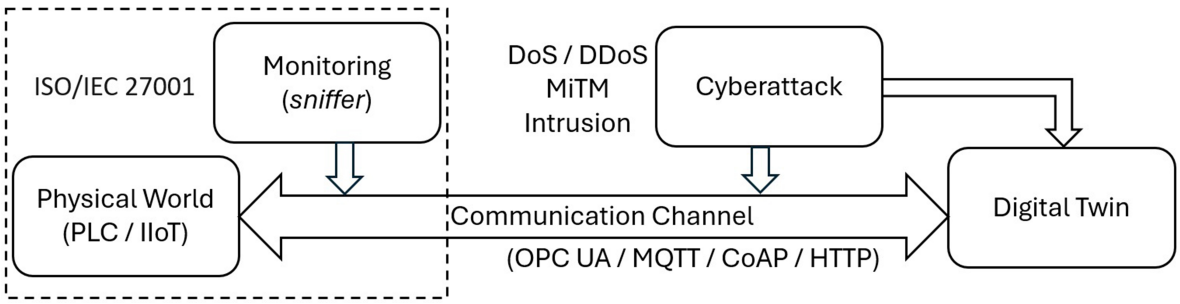

Figure 1. Block diagram of the proposed attack detection approach.

The monitoring system (Sniffer) non-intrusively observes the communication channel linking the Physical World (simulated by PLC and IIoT devices) and its digital representation, the Digital Twin. The sniffer continuously analyzes the data rate (PPS and BPS) to detect anomalies that could indicate a cyberattack, operating within a conceptual security perimeter aligned with guidelines such as ISO/IEC 27001 [38].

The detailed logical architecture of the simulation environment is presented in Figure 2. The diagram illustrates the interaction among the main containerized services, grouped into three functional domains: the Main Flow, Monitoring, and Attack Vectors. The diagram depicts the interaction between the containerized services. The main operational flow (Main Flow) involves the exchange of data and commands via MQTT between the Device and the Digital Twin, through the MQTT Broker. The Monitoring component (Sniffer/IDS) passively observes the traffic. The Attack Vectors indicate the different entry points for the simulated attacks, including direct attacks on the Digital Twin's API and interception of MQTT traffic via a proxy (MiTM Proxy).

The experiments were conducted in a controlled environment. The host operating system used was Ubuntu 24.04.3 LTS. Containerization was managed by Docker Engine version 28.4.0 along with Docker Compose version v2.39.4. All scripts were developed in Python 3.12. The system's functionality depended on a set of core libraries, whose versions are crucial for replicating the results: Paho-MQTT 1.6.1, Requests 2.32.3, Python-OPC-UA 0.98.13, and aiocoap 0.4.3. This documented configuration provides a solid foundation for the experiments performed, allowing other researchers to replicate and extend the proposed scenarios (the complete source code is available as detailed in the Data Availability Section).

3.1. Scenario Simulation

A fundamental step of our methodology consisted of the simulation of different operational scenarios to characterize the impact of anomalous events on the transmission data rate. The objective was to establish a comparative basis to distinguish anomalies caused by operational faults from those resulting from malicious cyberattacks. To this end, the following types of communication faults were simulated:

- Loss of connectivity: Simulation of temporary and permanent interruptions in the communication of specific devices or in the connection with the Digital Twin.
- Network latency: Introduction of variable delays in the network to observe the effect on response time and data transfer rate.
- Transmission errors: Simulation of packet transmission errors to induce retransmissions and observe the consequent changes in the data rate, mimicking potential data corruption.
- Bandwidth limitation: Introduction of network bottlenecks to reduce data transmission capacity and simulate congestion conditions.

 doi:10.20944/preprints202510.1127.v1

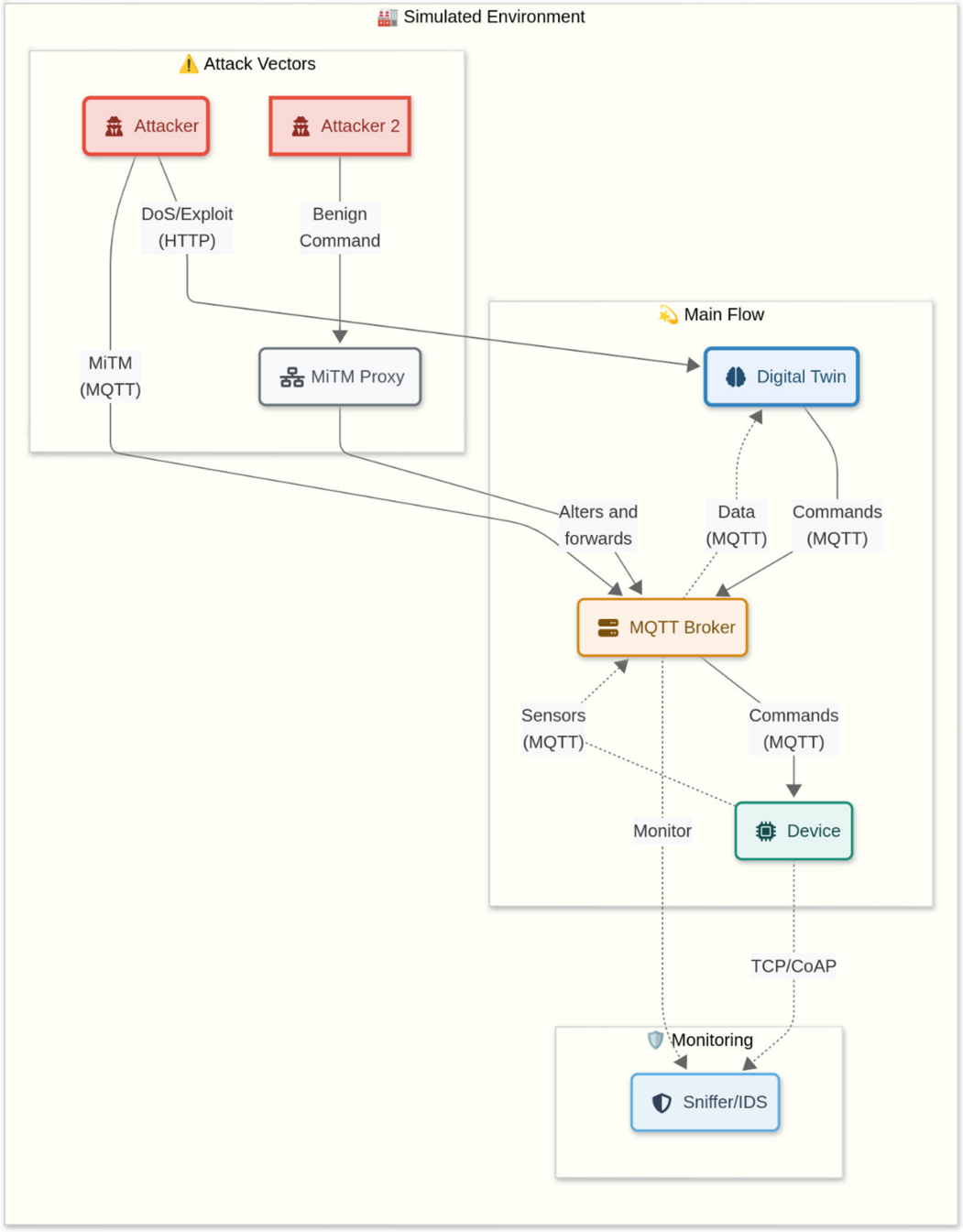

Figure 2. Logical architecture of the simulation environment.

For each type of fault, different implementation methods were studied within the Docker environment, with varying parameters such as duration and intensity, based on a risk analysis and the most common faults observed in industrial and IIoT environments. The analysis of the data collected during these scenarios allowed for the identification of specific patterns used to differentiate faults from cyberattacks in later stages of the research.

To investigate the sensitivity of the data rate in detecting malicious activities, different types of cyberattacks were simulated, targeting the communication between the simulated physical elements and the Digital Twins, as well as the Digital Twin itself. The primary targets were the communication channel and the Digital Twin container, with the objective of compromising the integrity and availability of the exchanged data. The types of simulated attacks include:

 doi:10.20944/preprints202510.1127.v1

- Denial of Service (DoS) and Distributed Denial of Service (DDoS): These attacks aim to make the system unavailable by overloading the communication resources or the Digital Twin itself with an excessive volume of requests or malicious traffic. Different methods and tools were explored within the Docker environment to generate high network traffic towards the targets.
- Man-in-the-Middle (MiTM): This attack aims to intercept the communication between the physical devices and the Digital Twin, with the potential to read or modify data in transit. Various tools and network configurations in the Docker environment were used to simulate an attacker positioning itself at the communication layer to intercept traffic.
- Intrusion and Asset Compromise: This attack targets vulnerabilities to gain unauthorized access to the Digital Twin, sending malicious commands (e.g., shutting down sensors) to the physical asset. This scenario simulates targeted sabotage with the objective of disrupting physical operations through manipulation of digital control.

For each type of attack, parameters such as the intensity and characteristics of malicious activity were varied. This allowed us to observe whether the anomalies in the data rate would be detectable in different scenarios and with different levels of intensity, seeking to identify the detection thresholds and the sensitivity of the proposed method for different types of threats.

3.2. Data Collection and Analysis

The bidirectional communication flow during normal operation is illustrated in the sequence diagram shown in Figure 3. The Simulated Physical Device sends telemetry data to the Digital Twin (step 1), which in turn can issue actuation commands to the device (step 3). The monitor (Sniffer), positioned within the communication channel, passively captures and analyzes all traffic (steps 2 and 4).

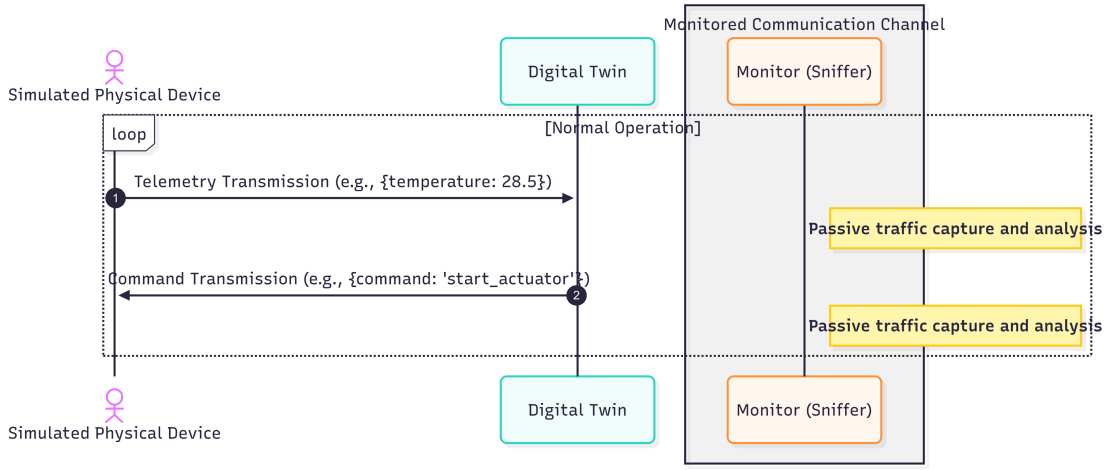

Figure 3. Sequence diagram of communication and monitoring.

Figure 3 illustrates the bidirectional communication flow during normal operation. The Simulated Physical Device sends telemetry data to the Digital Twin (step 1), which, in turn, can send actuation commands back to the device (step 3). The monitor (Sniffer) passively captures and analyzes all traffic (steps 2 and 4) to establish a baseline and detect anomalies.

The analysis of the collected data followed a structured methodological pipeline consisting of three main stages: baseline establishment, anomaly detection, and correlation verification.

Initially, normal communication behavior was characterized by running the simulation environment continuously for 60 minutes without introducing any faults or attacks. During this phase, data rate metrics, packets per second (PPS) and bytes per second (BPS), were recorded in one-second time

 doi:10.20944/preprints202510.1127.v1

windows. The mean (μ) and standard deviation (σ) of these metrics were calculated to establish a statistical baseline of the system's normal behavior.

In the second stage, anomaly detection was implemented based on this baseline. For each new data rate measurement taken during the fault and attack scenarios, an anomaly was flagged whenever the observed value exceeded a defined threshold. As an initial criterion, a threshold of three standard deviations ($\mu \pm 3\sigma$) was adopted, a common method in statistical process control for identifying statistically significant events. In addition to threshold-based detection, the analysis included the calculation of descriptive statistics for each scenario, allowing a formal comparison of the data distributions.

In the second stage, anomaly detection was implemented based on the established baseline. For each new data rate measurement collected during the fault and attack scenarios, an anomaly was flagged whenever the observed value exceeded a defined threshold. As an initial criterion, a threshold of three standard deviations ($\mu \pm 3\sigma$) was adopted, a common approach in statistical process control for identifying statistically significant deviations. Beyond threshold-based detection, the analysis also included the calculation of descriptive statistics for each scenario, facilitating a formal comparison of the data distributions.

The third and final stage consisted of validating the methodology by verifying the correlation between the detected anomalies and the simulated events. This validation was performed by overlaying time series graphs, where the data rate was plotted alongside visual indicators marking the exact start and end periods of each fault or attack. This visual and temporal analysis confirmed whether the detected anomalies coincided with the introduced events, thereby validating the method's ability to accurately identify abnormal activities.

The attack scenarios presented in Section 4 were executed with the following parameters: the Denial-of-Service (DoS) attack (Figure 4) was generated using 50 concurrent threads, resulting in an increased packet rate averaging approximately 800 PPS; the Man-in-the-Middle (MitM) attack (Figure 5) was modeled to simulate the overload caused by a malicious proxy, raising the packet rate to an average of 60 PPS; and the Intrusion attack (Figure 6) consisted of a 5-second burst of activity, with the packet rate reaching peaks of 150 PPS to simulate the sending of sabotage commands.

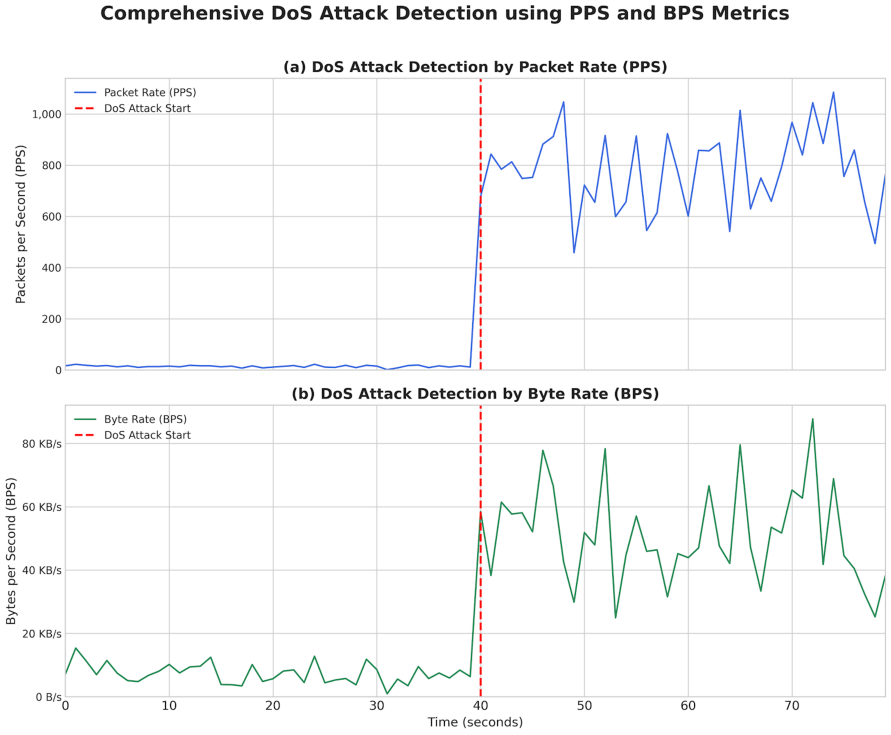

Figure 4. Denial-of-Service (DoS) Attack Detection.

 doi:10.20944/preprints202510.1127.v1

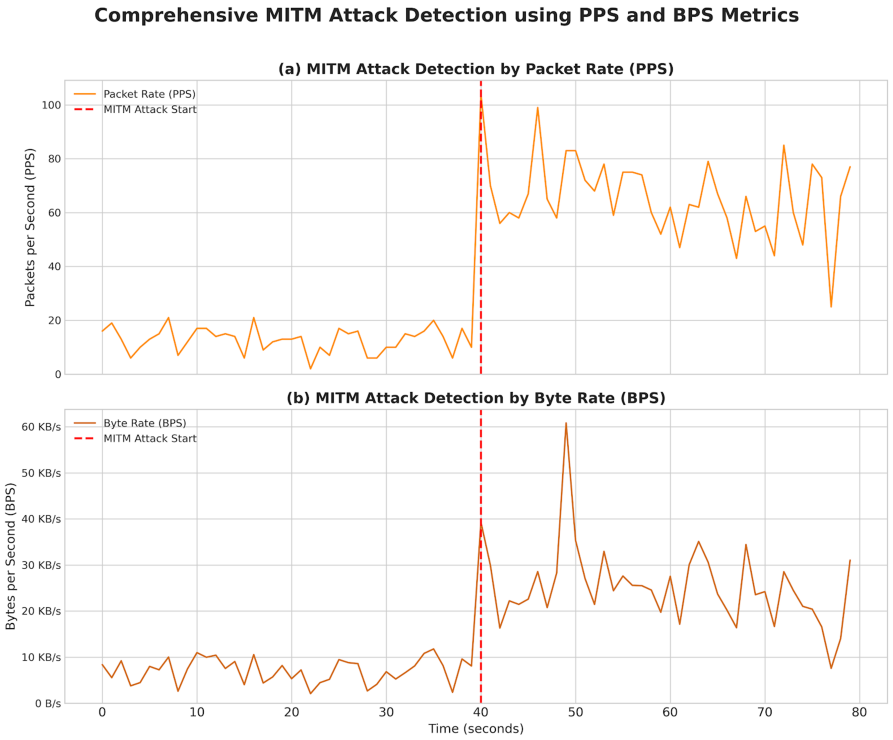

Figure 5. Man-in-the-Middle (MiTM) Attack Detection.

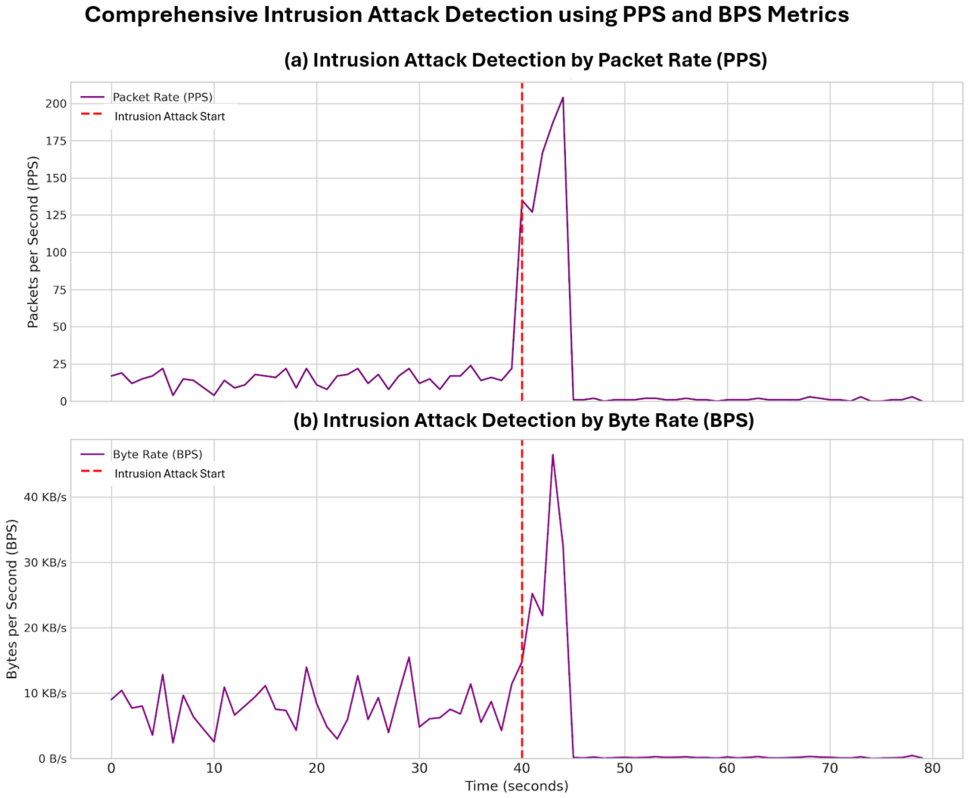

Figure 6. Intrusion Attack Detection.

4. Results and Discussion

This section presents the experimental results obtained and discusses their implications. Subsection 4.1 first details the quantitative outcomes of the simulation, demonstrating the efficacy of the data rate monitoring approach in detecting the three attack scenarios. Subsequently, Subsection 4.2

 doi:10.20944/preprints202510.1127.v1

interprets and discusses the results, contextualizing the contributions of this work within the existing literature, highlighting its advantages, and acknowledging its limitations.

4.1. Results

The proposed data rate monitoring approach was evaluated across three distinct cyberattack scenarios. The results demonstrate a strong correlation between the simulated attacks and the occurrence of statistically significant anomalies in network traffic metrics, thereby validating the method's effectiveness. A detailed statistical analysis is presented in Table 2, while the temporal behavior of the traffic is illustrated in Figures 4, 5, and 6.

Table 2. Comparative Statistical Analysis of Network Traffic.

Attack Type	Period	Mean PPS	Std. Dev. PPS	Mean BPS	Std. Dev. BPS
DoS	Normal	13.75	4.27	7309.92	3082.47
DoS	Attack	779.30	156.03	50904.75	15049.37
MiTM	Normal	12.70	4.59	7085.28	2656.04
MiTM	Attack	65.68	14.97	25445.80	8674.89
Intrusion	Normal	14.95	5.08	7721.48	3213.76
Intrusion	Attack	21.52	55.55	3664.50	10141.59

As presented in Table 2, network traffic under normal operating conditions exhibited a consistent and stable baseline across all experiments, with an average packet rate between 12.70 and 14.95 PPS. This behavior serves as a reliable reference for deviation detection.

In the first scenario, the initiation of the Denial-of-Service (DoS) attack (Figure 4) resulted in the detection of a drastic and immediate anomaly. Table 2 quantifies this event: the average packet rate surged from a baseline of 13.75 PPS to 779.30 PPS, an increase exceeding 50-fold. The plot visually illustrates this traffic flood, where both packets per second (a) and bytes per second (b) escalate to an extreme and sustained level, validating the unequivocal success of the method in identifying volumetric attacks.

The intrusion attack (Figure 6) revealed a distinctive statistical signature. As shown in Table 2, although the mean PPS exhibited a modest increase (from 14.95 to 21.52), the standard deviation surged dramatically from 5.08 to 55.55. This high variance corresponds to the behavior visualized in the plot: a very brief and sharp traffic peak (command injection) followed by an almost complete communication collapse. These results demonstrate that the method can detect anomalies not only based on volume but also on instability and state changes in the communication channel.

The Man-in-the-Middle (MiTM) attack (Figure 5) presented a more subtle yet clearly detectable signature. The average packet rate increased from 12.70 PPS to 65.68 PPS (Table 2). Although less pronounced than the DoS attack, this anomaly demonstrates the system's sensitivity in flagging not only flooding attacks but also traffic manipulations indicative of communication interception.

4.2. Discussion

The presented results provide compelling evidence supporting the viability of data rate analysis as a primary indicator for detecting cyberattacks in Digital Twin communication channels. However, the significance of these findings extends beyond simple anomaly detection and can be interpreted through three critical perspectives: the diagnostic versatility of the method, its operational implications for industrial environments, and its role as a lightweight and robust security mechanism.

The main implication of this study lies in demonstrating that fundamental network metrics, such as packet and byte rates, serve not only as performance indicators but also as rich sources of security information. The method's capability to detect three fundamentally distinct attack classes—a volumetric attack (DoS), an interception attack (MiTM), and a sabotage attack (Intrusion)—attests to its robustness and generalizability. Rather than being a threat-specific solution, this approach functions

 doi:10.20944/preprints202510.1127.v1

analogously to a "nervous system" for the communication channel, exhibiting sensitivity to diverse types of disturbances.

Most notably, each attack generated a unique statistical signature, as detailed in Table 2. The DoS attack was manifested by a substantial increase in mean PPS, while the MiTM reflected a more moderate rise. The Intrusion attack, conversely, was characterized not by an increase in the mean but by a dramatic surge in variance (standard deviation). This finding is crucial: data rate monitoring provides not only a binary alert (normal vs. anomalous) but also serves as a foundation for the preliminary characterization and classification of threats, offering a significant operational advantage for prioritizing incident response.

This point regarding threat characterization highlights a fundamental contrast with many state-of-the-art approaches in the literature. While machine learning and deep learning strategies have demonstrated remarkable proficiency in detecting complex anomalies, they often incur high computational costs and suffer from a lack of interpretability—the so-called "black box" problem. In Operational Technology (OT) environments, where computational resources may be limited and rapid, transparent diagnostics are critical, alerts generated by AI models without clear causal explanations can be problematic. System operators need not only to know that an anomaly has been detected but also to understand the rationale behind the alert.

In contrast, the approach proposed in this work is grounded in the principle of direct interpretability (white box). The cause of an alarm is unequivocally linked to a violation of a statistical threshold in fundamental and comprehensible metrics, such as packets or bytes per second. This simplicity is not a limitation but a strategic advantage in Industrial Internet of Things (IIoT) environments. The modest computational requirements for calculating means and standard deviations in real time make the method suitable for implementation on edge devices or resource-constrained network gateways, serving as an efficient, low-latency first line of defense.

Additionally, the proposed approach is largely application protocol agnostic. While many Intrusion Detection Systems (IDS) require specific rules to parse protocols such as MQTT, OPC UA, or HTTP, data rate monitoring operates at a more fundamental level, being sensitive to anomalies regardless of the particular protocol employed. This confers greater flexibility and applicability to the method, especially in heterogeneous industrial environments that often deploy a mixture of legacy and modern technologies.

Despite the demonstrated effectiveness and advantages, it is essential to acknowledge the limitations of this study, which open avenues for future research. The primary limitation arises from the nature of the experimental environment, as validation was conducted within a controlled Docker simulation. While this approach ensures high reproducibility and variable isolation, it does not encapsulate the full complexity and unpredictability of a physical industrial network, such as hardware jitter, electromagnetic interference, or the heterogeneous behavior of legacy systems.

Furthermore, although the attack scenarios considered represent distinct threat classes, they are not exhaustive. More sophisticated attacks, such as low-and-slow attacks or certain Advanced Persistent Threats (APT), may generate data rate anomalies that do not breach simple statistical thresholds. Detecting such stealthy threats would require more sensitive and nuanced analytical techniques beyond basic threshold-based monitoring.

Given these limitations, future work can pursue three main directions. The first, and most immediate, is the validation of the proposed approach in a physical testbed encompassing industrial hardware components such as programmable logic controllers (PLC), sensors, and network switches, to assess performance under real-world operational conditions. The second direction involves expanding the detection scope by evaluating the method's sensitivity to a wider array of stealthy attack types. Finally, the third direction would explore hybridization strategies, employing data rate monitoring as a low-cost, preliminary trigger to activate more computationally intensive and in-depth analysis techniques—such as deep packet inspection or machine learning models—only upon the detection of an initial anomaly, thereby enabling an efficient, layered, and robust defense system.

 doi:10.20944/preprints202510.1127.v1

5. Conclusions

This paper investigated the viability of a non-intrusive and computationally lightweight approach for detecting cyberattacks in Digital Twin communication channels, an increasingly critical threat vector in Industrial Internet of Things (IIoT) environments. Through a controlled simulation environment, we demonstrated that monitoring and statistical analysis of fundamental network metrics—specifically packet rate (PPS) and byte rate (BPS)—are highly effective in identifying a diverse range of malicious activities. The method successfully detected attacks, identifying an increase exceeding 50-fold in packet rate during the DoS simulation, as well as unique statistical signatures characterizing the MiTM and Intrusion attacks, thus proving its efficacy against multiple threat classes.

The principal contribution of this work is the validation that data rate analysis serves as a robust, interpretable, and easily implementable first line of defense, addressing a gap in the literature which tends to emphasize computationally intensive solutions. The results suggest that this approach can significantly enhance the resilience and security of Digital Twin systems by providing an effective early warning mechanism. Practically, this method can be deployed as a lightweight network sensor, monitoring traffic at critical points within OT/IT networks. The generated anomaly alerts can be seamlessly integrated into existing security platforms, such as Security Information and Event Management (SIEM) systems, thereby enriching the security team's situational awareness without overburdening control infrastructure. Future work will focus on validating the method in physical testbeds and exploring adaptive thresholding techniques to improve its detection sensitivity.

Data Availability Statement: The complete source code, Docker configuration files ($docker - compose.yml$), and scripts used to generate the results presented in this article are publicly available in a GitHub repository at the following address: https://github.com/woliveira1728/digital-twin/tree/main/digital_twin.

Acknowledgments: In this section you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments). Where GenAI has been used for purposes such as generating text, data, or graphics, or for study design, data collection, analysis, or interpretation of data, please add "During the preparation of this manuscript/study, the author(s) used [tool name, version information] for the purposes of [description of use]. The authors have reviewed and edited the output and take full responsibility for the content of this publication".

Abbreviations

The following abbreviations are used in this manuscript:

DT	Digital Twin
DTs	Digital Twins
IIoT	Industrial Internet of Things
OT	Operational Technology
DoS	Denial-of-Service
MiTM	Man-in-the-Middle
PPS	Packets Per Second
BPS	Bytes Per Second
SIEM	Security Information and Event Management
APT	Advanced Persistent Threat
IDS	Intrusion Detection System
CIA	Confidentiality, Integrity, and Availability
PLC	Programmable Logic Controller

 doi:10.20944/preprints202510.1127.v1

References

1. Grieve, M. W. *Digital Twin: Manufacturing Excellence through Virtual Prototyping*; University of Michigan, 2003; White Paper.
2. Tao, F.; Cheng, J.; Qi, Q.; Zhang, M. Digital twin-driven product design, manufacturing and service with big data. *Int. J. Adv. Manuf. Technol.* **2018**, *94*(5–8), 1509–1520. https://doi.org/10.1007/s00170-017-0233-1.
3. Botín-Sanabria, D.M.; García-Méndez, L.C.; Gaviria-López, C.A.; Muñoz-Guerrero, J.D.; Arango-Serna, M. Digital twins for smart cities: a review of current applications and future trends. *Sustain. Cities Soc.* **2024**, *109*, 105652. https://doi.org/10.1016/j.scs.2024.105652.
4. Hosamo, H.; Al-Hussein, M.; Almashaqbeh, A.; Al-Kasasbeh, B. A Review of the Digital Twin Technology in the AEC-FM Industry. *Adv. Civ. Eng.* **2022**, *2022*, 2185170. https://doi.org/10.1155/2022/2185170.
5. Al-Fawwaz, A.; Al-Qaralleh, A.; Al-Majali, A.; Qadan, M. A Comprehensive State-of-the-Art Review for Digital Twin: Cybersecurity Perspectives and Open Challenges. *Sensors* **2023**, *23*(8), 4635. https://doi.org/10.3390/s23084635.
6. Bhushan, M.; Kumar, A.; Kumar, A.; Prakash, S. Advancing Security with Digital Twins: A Comprehensive Survey. *arXiv* **2025**, arXiv:2505.17310.
7. Liu, C.; Ren, Y.; Wang, H.; Yu, G.; Xu, X.; Su, B. Federated Learning for Intrusion Detection in Industrial IoT and Digital Twin. *IEEE Trans. Ind. Informatics* **2024**, *20*(8), 9205–9215. https://doi.org/10.1109/TII.2023.3330386.
8. Liu, W.; Li, D.; Guo, Q.; Zhang, H.; Lv, Y.; Chen, J. Blockchain-Enabled Digital Twin for Secure and Resilient Industrial Systems. *IEEE Trans. Ind. Informatics* **2024**, *20*(4), 3841–3852. https://doi.org/10.1109/TII.2023.3303721.
9. Belay, M.A.; Rasheed, A.; Rossi, P.S. Digital Twin Knowledge Distillation for Federated Semi-Supervised Industrial IoT DDoS Detection. *IEEE Internet Things J.* **2025**, doi:10.1109/JIOT.2024.3402120.
10. Zainudin, A.; Paramartha Putra, M.A.; Alief, R.N.; Kim, D.S.; Lee, J.M. Blockchain-aided Collaborative Threat Detection for Securing Digital Twin-based IIoT Networks. In Proceedings of the ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA, 9–13 June 2024; pp. 4656–4661.
11. Li, S.; Zhang, Z.; Shi, H.; Wang, X. A Digital Twin Anomaly Detection Method Based on a Spatiotemporal Fusion Graph Convolutional Network. *Sensors* **2024**, *24*(4), 1253. https://doi.org/10.3390/s24041253.
12. Pan, J.; Chen, J.; Su, Z. Digital Twin-Based Anomaly Detection in Industrial Control Systems. *IEEE Trans. Ind. Informatics* **2023**, *19*(12), 11571–11580. https://doi.org/10.1109/TII.2023.3270921.
13. Yu, G.; Zhang, J.; Cao, Y.; Yu, H.; Zhang, Y. A Survey on Digital Twin-Empowered Anomaly Detection in Cyber-Physical Systems. *IEEE/CAA J. Autom. Sin.* **2024**, *11*(4), 833–852. https://doi.org/10.1109/JAS.2024.124231.
14. Wang, L.; Liu, C.; Li, Y.; Li, B. Digital Twin-Based Collaborative Anomaly Detection for Industrial IoT. *IEEE Internet Things J.* **2023**, *10*(13), 11466–11477. https://doi.org/10.1109/JIOT.2023.3243177.
15. Koroniotis, N.; Moustafa, N.; Schiliro, F.; Gauravaram, P.; Janicke, H. A holistic review of cybersecurity and intrusion detection systems in securing smart cities: a survey and future directions. *J. Netw. Comput. Appl.* **2023**, *213*, 103607. https://doi.org/10.1016/j.jnca.2023.103607.
16. Xie, J.; Zuo, H.; Fu, S.; Liu, S. IoT and Digital Twin assisted Deep Reinforcement Learning for Cyber-Physical Industrial Control Systems Security. *IEEE Trans. Ind. Informatics* **2023**, *19*(12), 11571–11580. https://doi.org/10.1109/TII.2023.3248888.
17. Zuo, H.; Xie, J.; Fu, S. Digital Twin-Driven Threat Detection for Industrial Control Systems via Dynamic Graph Learning. *IEEE Trans. Ind. Cyber-Phys. Syst.* **2024**, doi: 10.1109/TICPS.2024.3364741.
18. Liang, Z.; Tang, B.; Liu, Y.; Wang, S.; Chen, S. Hybrid Anomaly Detection for Industrial Control System Based on Digital Twin. *IEEE Trans. Circuits Syst. II Express Briefs* **2024**, *71*(2), 999–1003. https://doi.org/10.1109/TCSII.2023.3305459.
19. Wang, J.; Li, W.; Li, X.; Li, M. Digital Twin—A Review of the Evolution from Concept to Technology and Its Analytical Perspectives on Applications in Various Fields. *Sensors* **2024**, *24*(13), 5454. https://doi.org/10.3390/s24135454.
20. Yang, Y.; Wang, H.; Li, M.; Liu, Z.; Zhang, C. Anomaly detection in industrial IoT based on digital twin and deep learning. *Digit. Commun. Netw.* **2023**, *9*(5), 1276–1286. https://doi.org/10.1016/j.dcan.2022.11.002.
21. Li, H.; Ota, K.; Dong, M. Digital Twin-Based Intrusion Detection for Industrial Cyber-Physical Systems. *IEEE Netw.* **2023**, *37*(4), 180–186. https://doi.org/10.1109/MNET.2023.3259837.
22. Li, S.; Zhang, Z.; Shi, H.; Wang, X. A Digital Twin Anomaly Detection Method Based on a Spatiotemporal Fusion Graph Convolutional Network. *Sensors* **2024**, *24*(4), 1253. https://doi.org/10.3390/s24041253.

23. Ma, R.; Labbe, A.; Malo, A.; G-B. de Lamotte, F. Digital twin for situational awareness in industrial cybersecurity: A review and a new concept. *Comput. Ind.* **2023**, *148*, 103901. https://doi.org/10.1016/j.compind.2023.103901.
24. Puerto-Santana, F.; Puerto-Santana, E.; O'Leary, P.; Gutierrez-Estevez, M. A Digital Twin with HMMs for Industrial Anomaly Detection. *Sensors* **2022**, *22*(19), 7436. https://doi.org/10.3390/s22197436.
25. Shukla, S.; L-F. Pau, L.F.; Balasubramaniam, S.; Mustafa, M.A. Digital Twin-Based Anomaly Prediction in Industrial Control Systems. In Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 29–31 October 2021; pp. 836–845.
26. Abolfazi, S.A.; Tabaee, T.; G-B. de Lamotte, F. Digital-Twin-Enabled Intrusion Detection System for Industrial Control Systems: A GAN-Based Implementation. *Sensors* **2023**, *23*(6), 3209. https://doi.org/10.3390/s23063209.
27. Gnanaprakasam, A.; Anand, S.J.S.; Balasubramanian, S.; Akila, D. A trust management model using digital twin and blockchain for industrial IoT networks. *Peer-to-Peer Netw. Appl.* **2024**, *17*, 118. https://doi.org/10.1007/s12083-024-01648-z.
28. Sharma, A.; Singh, H. Digital Twin Empowered Autonomic Security Management in Industrial IoT Network. *IEEE Internet Things J.* **2024**, doi: 10.1109/JIOT.2024.3390890.
29. Niyonzuima, R.; Al-Maqbali, A.; Al-Bahri, Y.; Al-Barami, B.; Al-Hinai, M. Digital twin: a unified definition, issues, challenges, and opportunities. *J. Cyber Secur. Data Prot.* **2024**, *1*(1), 1–15.
30. Zhang, S.; Yang, J.; Hu, Z.; Yan, S.; Liu, Y. A systematic review of the digital twin technology in buildings, landscape and urban environment from 2018 to 2024. *Buildings* **2024**, *14*(11), 3475. https://doi.org/10.3390/buildings14113475.
31. Niyonzuima, R.; Al-Maqbali, A.; Al-Bahri, Y.; Al-Barami, B.; Al-Hinai, M. Digital twin: a unified definition, issues, challenges, and opportunities. *J. Cyber Secur. Data Prot.* **2024**, *1*(1), 1–15.
32. National Institute of Standards and Technology (NIST). Security and trust considerations for digital twin technology. *NISTIR 8356* **2025**. https://doi.org/10.6028/NIST.IR.8356.
33. Digital Twin Consortium. Understanding DTC's digital twin platform stack architectural framework. Technical Report, November 2023. Available online: https://www.digitaltwinconsortium.org/2023/11/understanding-dtcs-digital-twin-platform-stack-architectural-framework/.
34. Orange, J. Network digital twin: concepts and reference architecture. *IETF Internet-Draft draft-irtf-nmrg-network-digital-twin-arch-10* **2025**. Expires August 31, 2025.
35. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A systematic survey of industrial internet of things security: requirements and fog computing opportunities. *IEEE Access* **2020**, *8*, 123456–123478.
36. Herath, J.D.; Yan, G. Real-Time Evasion Attacks against Deep Learning-Based Anomaly Detection from Distributed System Logs. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Virtual Event, USA, 26–28 April 2021; pp. 29–40.
37. Rasheed, A.; Javed, A. R.; Habib, M. F.; Abbas, S.; Fatima, T.; Farooq, M. S. Privacy and security challenges of the digital twin: systematic literature review. *J. Univers. Comput. Sci.* **2024**, *30*(13), 1782–1806. https://doi.org/10.3897/jucs.114607.
38. International Organization for Standardization. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO, 2022.