Towards 5G-Enabled Operational Technology for Process Monitoring and Network Slicing

Jared M. Aguayo, Abel O. Gomez Rivera, Deepak K. Tosh
Department of Computer Science, University of Texas at El Paso, TX, USA
jmaguayo@miners.utep.edu, aogomezrive@miners.utep.edu, dktosh@utep.edu

***Abstract*—Cyber-Physical Systems (CPS) are deployed to monitor physical processes in critical cyber-enabled services like power generation. However, CPS ecosystems are typically designed without robust security. While it is important to ensure optimal performance of the Operational Technology (OT) environments, security cannot be overlooked. To modernize traditional OT services, 5G technology is being integrated. 5G technology offers low latency and high availability, making it a suitable infrastructure for managing and monitoring physical processes. However, integrating 5G mechanisms into large-scale OT networks introduces new implementation and performance challenges. Therefore, this paper presents a 5G-enabled CPS architecture (5G-CPS) that describes the necessary components, services, and communication protocols and conducts feasibility study to integrate 5G technology in industrial control system networks to understand the performance merits. The 5G-CPS architecture aims to minimize implementation and operational challenges associated with integrating 5G technology into constrained OT.**

***Index Terms*—Cyber-Physical Systems, 5G, SDN, OT, NFV**

I. Introduction

Cyber-Physical Systems (CPS) are responsible for supporting critical cyber-enabled services such as power generation. However, traditional CPS ecosystems are made up of legacy Operational Technology (OT) devices that lack robust security to ensure the authenticity and integrity of physical processes. Adversaries can exploit the lack of security to disrupt OT devices through data breaches and rogue runtime-system-states. Given the recent growth of cyber attacks, the modernization of CPS architectures is necessary to adopt more flexible and resilient communication technology. Next-generation network management and system process monitoring services are suitable to provide dynamic frameworks that can be adapted to heterogeneous OT devices and industrial communication protocols however next-generation communication technology needs to comply with the operational requirements and real-time data needed of for traditional CPS ecosystems.

Next-generation network management technology such as, Software Defined Networking (SDN), simplifies network management services and can also improve the resilience and fault tolerance network resources while reducing network latency and operational overhead [1]. SDN technology separates data and control planes, allowing state-of-the-art mechanisms to improve scalability and security by decoupling sensing data from health-status data of OT devices. SDN implementation for monitoring and managing large-scale networks has been discussed in [2]. SDN technology plays an important role in 5G backbone communication infrastructure to offer flexibility and management of resources and devices. 5G technology represents the next-generation network management infrastructure, focusing on maintaining operational requirements such as low latency and high availability. OT operators have the ability 5G technology to deploy end-to-end services that enable more robust security and monitoring of OT devices, using modular virtualization and containerization tools that extend the network capabilities of traditional systems. In particular, the implementation of 5G mechanisms in traditional CPS ecosystems can enable the decoupling of status information and sensing information through of separate traffic channels that monitor and transmit specific information, thus, reducing processing, latency, and noisy nature of industrial communication protocols. However, this kind of integrated architecture is currently missing in the industrial CPS environment.

This paper discusses a novel 5G-enabled CPS architecture that aims to integrate 5G technology into constrained CPS. Given that the CPS consist of constrained OT devices that limit the integration of newer communication protocols and constrain the upgrade capacity of general industrial communication services, we analyze the challenges and benefits of enabling 5G technology in legacy OT. We also discuss a new next-generation CPS ecosystem that adopts more flexible and open communication protocols. Particularly, we present a preliminary architecture design that integrates 5G communication technology in Industrial Control Systems (ICS) through an open 5G Core Network, Open5GS [3]. We also evaluate the performance and overhead of decoupling sensing information from health-state information through the implementation of mobile communication protocols such as standardized 5G links. The contributions of this paper are as follows:

- Analyze the implementation challenges and operational benefits of 5G technology.
- Discuss the operational constraints of traditional CPS.
- Design a 5G-enabled CPS architecture that aims to modernize traditional ICS through the implementation of next-gen communication protocols and services.
- Evaluate the proposed 5G-enabled CPS architecture to transmit sensing information and health-state information through traditional industrial communication protocols.

The structure of the paper is as follows. Section II high-

This material is based upon work supported by the United States Deparment of Energy's (DOE) Office of Fossil Energy (FE) Award # DE-FE0031744

2023 Resilience Week (RWS) | 979-8-3503-4747-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/RWS58133.2023.10284597

lights related works. Section III discusses an overview of the challenges of implementing 5G technology and describes the operational challenges of OT devices. Section IV discusses the proposed 5G-enabled CPS architecture. In section V we discuss preliminary results and network performance. Finally section VI concludes and provides future directions.

II. Related Work

Next-generation communication services, such as 5G technology, offer more flexible and resilient architectures that can support extreme low latency, high availability, and dynamic connectivity. A logical approach is to modernize traditional ICS networks by implementing more flexible architectures capable of enabling a more connected ICS ecosystem and providing real-time data analysis to ICS operators while also benefiting from the security attributes, such as fault tolerance and interconnection, of next-gen communication systems. However, the benefits of next-gen communication systems are limited by the deployment cost and high demands in terms of processing capabilities and resources. Additionally, ICS networks lack adequate environments to enable easy integration of next-gen communication systems due to the critical performance trade-off of behavior-based operations. Enabling necessary next-gen communication technology, such as 5G, exposes ICS networks to state-of-the-art cyber attacks that can exploit the lack of robust security in obsolete ICS networks [4], enabling adversaries to disrupt the operational hours of critical cyber services through outages and data breaches. Authors in [5] discussed the intricate challenges of designing a network infrastructure that effectively supports the progression of intelligent manufacturing propelled by Industry 4.0 and 5G. The authors in [6] discuss the security issues and overall operational requirements that traditional ICS networks need to address to achieve robust and resilient implementation of next-gen communication systems, such as 5G.

Authors in [7] addressed the challenges of adapting communication systems to the evolving technological landscape in industrial contexts, in particular, they analyzes and identified the appropriate operational parameters of the 5G network to meet manufacturing standards. In general, traditional OT architectures are not suitable for extreme upgrades that demand new communication mechanisms and topology updates. To enable 5G technology in constrained OT devices, the authors in [8] proposed integrating a digital twin with the underlying characteristics of ICS architectures. The digital twin leverages sensor real-time sensing data to enable intelligent physical processes that enable 5G mechanisms. In [9] authors investigate the viability of private 5G networks as a communication solution through smart automation to optimize manufacturing processes. In [10], the authors discussed a proof-of-concept to evaluate administrative shells that integrate VNFs to demonstrate dynamic adaptation of network characteristics. The authors in [11] proposed a fog-assisted CPS that enables 5G services through the optimization of computing nodes that need to support scalable and evolving infrastructures in CPS-based architectures. Finally, in [12], the authors proposed a vehicle monitoring service that enables the flexibility of 5G mechanisms to provide low latency and remote management tools through VNFs and onboard units.

Previous approaches have limited the implementation of 5G technology to specific ecosystems and network layers that, in general, consider only a limited set of ICS services and processes. This work introduces a purpose-driven network virtualization framework that aims to enable next-gen communication systems in traditional ICS architectures. In particular, the purpose-driven network virtualization framework provides fault tolerance and introduces data duplication through the implementation of VNFs without reducing the operational capabilities of ICS networks or becoming overly specific to a set of OT devices and industrial communication protocols.

III. 5G Integrated Operational Technology: Opportunities and Challenges

The recent development of wireless technology has become a game changer in next-generation networks [4]. In particular, 5G technology is driving the modernization of traditional CPS. 5G mechanisms can enable enterprise connectivity with ultra-reliable, high-speed, low-latency, and power-efficient features [13]. 5G is a next-generation cellular technology that aims to provide a flexible platform for enabling mobile communication protocols while achieving low latency, high availability, and fault tolerance by integrating dedicated transmission channels. In addition, 5G enables data isolation through Virtualized Network Functions (VNFs). VNFs are commonly concatenated with other VNFs and Physical Network Functions (PNFs) that provide Intelligent Network Services (INS).

We envision a 5G-enabled CPS that provides services such as protocol translation to enable the communication of industrial communication protocols to newer communication technologies like 5G standard links. Overall, traditional CPS is designed to operate in closed environments where the security and integrity of OT devices are taken for granted [14]. Therefore, legacy communication protocols such as the Modbus protocol [15] provide high-performance efficiency without considering the operational security or integrity of sensing information. However, due to the design constraints and operational requirements of legacy OT devices and CPS, adopting new technology such as 5G introduces operational and implementation challenges. Commonly, CPS ecosystems lack the capacity to support operational and security upgrades. In the following sections, we describe the challenges and requirements to enable 5G technology in OT.

A. Resilient OT Through 5G Technology

Traditional OT devices typically rely on proprietary communication protocols, with data and device trustworthiness often taken for granted. To meet critical operational requirements such as low latency and real-time data transmission, legacy communication protocols may have performance trade-offs. However, these devices often lack the capacity to integrate new technology like 5G mechanisms due to being locked by third-party mechanisms, and also lack the resources to integrate

complex operations like authentication or integrity verification. OT ecosystems rely on two types of sensing information for making critical operational decisions: OT data information, representing information gathered from the environment, and OT state information, representing the runtime-system-state of OT devices. Supervisory Control and Data Acquisition (SCADA) [16] systems are commonly used to gather and monitor this information, but they lack robust security mechanisms to ensure the integrity and provenance of sensing information due to integrating legacy industrial communication protocols.

In this paper, we propose a novel 5G-enabled CPS architecture that integrates dedicated 5G-enabled communication channels to enable 5G technology in OT devices. These channels allow for high granularity in gathering and monitoring sensing information, with a virtual network management interface decoupling OT data sensing from OT state-of-health information. This enables resilient network management of legacy industrial communication protocols and allows OT operators to monitor specific state-of-health information with a high degree of detail, reducing noise in traditional industrial communication protocols and improving the efficiency of anomaly detection and cyber attacks. However, we also acknowledge that introducing new communication standards like 5G can introduce performance and implementation challenges.

B. Infrastructure Requirements for 5G Integration in OT

Integration of 5G technology into existing systems, such as OT devices, requires additional 5G-capable components, including smart sensors, macro and small cells, which must be fully IP-enabled [6]. The deployment of 5G network intelligence at the cloud, edge, or private on-premises poses a research challenge that must be addressed before adopting 5G technology. Precise location needs of 5G devices and services introduces network latency challenges that demand reliable low latency and high data transfer rates to meet the operational requirements of critical CPS ecosystems.

CPS ecosystems transmit critical information supporting national security, so ensuring reliable control access policies is essential. Private 4G LTE networks are widely used to provide confidentiality and control access policies through Mobile Private Networks (MPNs). Therefore, 5G private networks are an expected extension. However, the significant financial cost of deploying 5G MPNs is the need for a licensed spectrum. One significant advantage of MPNs over public networks is that 5G MPNs can be configured for specific needs based on the type of work and environment. Flexible environments are particularly important in heterogeneous CPS ecosystems that monitor a diverse set of physical processes.

The presented next-gen CPS architecture aims to enhance the traditional operational layer of CPS ecosystems [17]. Our CPS architecture comprises three layers: (1) the Enterprise Layer, which includes state-of-the-art enterprise services enabling OT device monitoring, (2) a novel Control Layer that provides intelligent network management through Open 5G core technology and dedicated communication channels, (3) a data layer from where the 5G-compatible field sensors

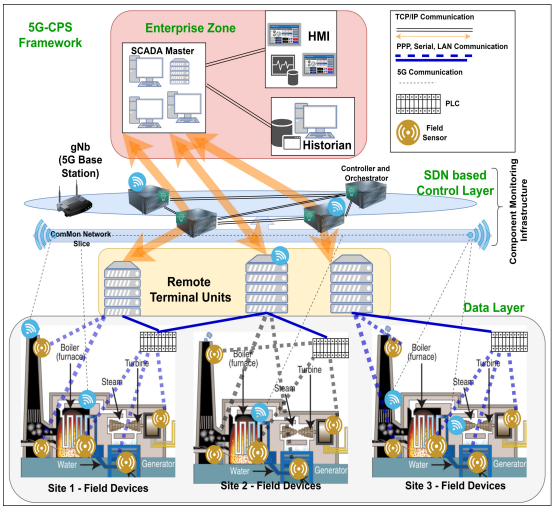

Fig. 1. 5G-CPS Framework in traditional SCADA System Study Case

can communicate with the enterprise servers to track process data and health of physical devices. The envisioned 5G-enabled CPS architecture shown in Figure 2 aims to enable 5G capabilities in constrained and legacy CPS networks without the legacy operational requirements of traditional industrial communications protocols and ICS.

C. Cybersecurity Threats of 5G Integration

Legacy communication protocols like *Modbus* assume that the sensing data is secure, which leaves them vulnerable to cyber attacks. As a result, an attacker can compromise the weak security of these traditional industrial communication protocols and introduce fake sensing information. Ensuring the continuous integrity verification of sensing information is, therefore, critical. The 5G-enabled CPS architecture can help address such attacks by integrating robust, state-of-the-art security mechanisms that authenticate OT devices and ensure the integrity of sensing information. We assume that 5G components are powerful enough to support traditional cybersecurity solutions such as cryptography and authentication mechanisms. Therefore, we envision 5G communication channels with strong security mechanisms that prevent tampering of sensing information while meeting the operational requirements of ICS ecosystems. Thus, the introduction of 5G core technology into traditional ICS brings with it a range of cybersecurity threats that must be addressed to ensure the secure and reliable operation of critical infrastructure. Some of the main cybersecurity threats associated with enabling 5G core technology in traditional ICS are [18]–[20]:

- Attack surface: With the integration of 5G technology, the number of connected devices and the data flow between them will increase, creating a larger attack surface.
- Malware attacks: Malware attacks can be used to gain unauthorized access to the network, steal data, or disrupt operations. With the increased connectivity provided by 5G technology, malware can spread more quickly and cause more damage.

- Cyber Attacks: Distributed Denial of Service (DDoS) attacks can be used to overwhelm the network with traffic, causing it to slow down or crash. With the increased bandwidth and faster speeds provided by 5G technology, DDoS attacks could be even more effective. False Data Injection (FDI) attacks [21] that can exploit to disrupt the operational hours of traditional CPS ecosystems through data breaches and damage to field devices.
- Data breaches: The increase in data flow between devices in ICS networks can create more opportunities for data breaches. In addition, the use of 5G technology may make it easier for attackers to intercept data in transit.

To mitigate these cybersecurity threats, organizations should implement a multi-layered security strategy that includes measures such as network segmentation, access controls, regular software updates through mobile communication technology.

IV. Experiment Setup

A. Architecture

The test bed for this research was developed to investigate the potential of overlaying 5G networks in industrial control systems for advanced monitoring. The goal was to determine the effectiveness of using 5G for data transfer and communication in industrial settings, particularly for Supervisory Control and Data Acquisition (SCADA) systems. In order to achieve this, we employed open-source software tools to simulate a 5G network and its associated components.

The test bed utilizes Open5GS, an open-source software suite that enables the simulation of 5G communication. Open5GS provides a complete implementation of the 5G core network, including the necessary functionality for network slicing. Network slicing allows us to subdivide our network into multiple virtual networks, each tailored to specific use-cases or applications. In this research, we focus on using network slices to facilitate the secure transmission of health data from user equipment (UE) to the SCADA server.

In addition to Open5GS, we used the open-source software UERANSIM to simulate both the user equipment (UE) and the 5G base stations (gNB). UERANSIM provides an end-to-end simulation environment for the 5G New Radio (NR) and the 5G Core Network (5GC). The integration of UERANSIM allows us to generate realistic traffic patterns and evaluate the performance of the 5G network in the context of industrial control systems.

The test bed architecture separates the control plane and user plane into distinct virtual machines (VMs) that communicate with each other. This separation enables greater flexibility in managing the traffic flows, ensuring optimal performance and reliability. Both the 5G base stations and user equipment are instantiated within VMs, allowing us to easily scale the network and adapt to different scenarios.

Furthermore, the test bed represents a slice of the network capable of transmitting process data over 5G when required. This feature enables us to evaluate the performance and reliability of the network in various industrial settings, as well as assess the potential benefits of using 5G for advanced monitoring and control in industrial systems.

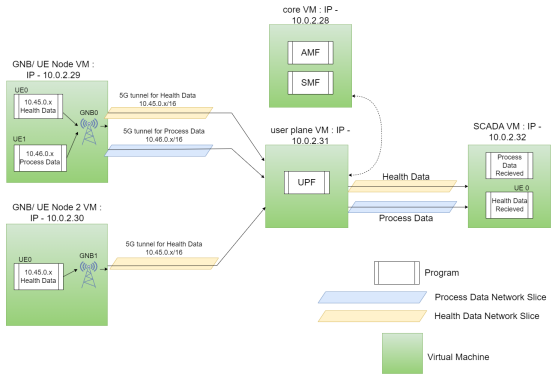

Fig. 2. 5G-enabled CPS Testbed

In the following subsections, we describe the details of the test bed setup, the specific experiments conducted, and the performance metrics used to evaluate the effectiveness of the proposed 5G-based industrial control system.

B. Experiment Setup

To evaluate the performance of the proposed 5G-based industrial control system, we conducted a series of experiments focusing on various network performance metrics. These metrics include:

- Number of packets transmitted
- Number of re-transmissions
- Average end-to-end delay
- Average amount of data per packet
- Total data sent

The experiments involved a Modbus slave and master, exchanging a total of 300 packets at varying rates: 1 packet per second (pps), 5 pps, and 15 pps. The Modbus slave, which is part of the SCADA system, and the master communicate through user equipment (UE). The experiments were designed to assess the impact of increasing the number of UEs that the slave makes requests to, ranging from 1 to 3 UEs.

To simulate a realistic network environment, we introduced a 20 percent chance of packet loss on the interface. This allowed us to examine the system's resilience and ability to handle packet loss, which is a common issue in wireless communication networks.

C. Experiment Procedure

The experimental procedure consisted of the following steps:

1) Initialize the test bed with the desired number of UEs (1 to 3), and configure the Modbus slave and master accordingly.
2) Simulate the 5G network using Open5GS and UERANSIM, with a 20 percent chance of packet loss on the interface.
3) Configure the Modbus slave and master to exchange 300 packets at the specified rates (1 pps, 5 pps, and 15 pps).

4) Record the performance metrics (number of packets transmitted, number of re-transmissions, average end-to-end delay, average amount of data per packet, and total data sent) for each experiment.

The experiments were conducted in a controlled environment, with each combination of packet rate and the number of UEs tested. This resulted in a total of 9 different experimental conditions, allowing us to examine the performance of the 5G-based industrial control system under various scenarios.

D. Data Analysis

The data collected from the experiments were analyzed to determine the impact of increasing the number of UEs and the packet rate on the performance metrics. The results provide insights into the effectiveness of using 5G for advanced monitoring and control in industrial systems, as well as the potential benefits and limitations of the proposed solution. In the next section, we present the findings of our experiments and discuss their implications for the future of 5G-based industrial control systems.

V. Results

The results of our experiments provide valuable insights into the performance of the 5G-based industrial control system under various conditions. Below, we summarize the key findings related to each performance metric:

1) Re-transmissions: As shown in Figure 5 the number of re-transmissions was found to be higher when sending at 1 pps and progressively decreased as the packet rate increased to 5 pps and 15 pps. The increase in re-transmissions as the number of UEs increased can be attributed to the higher number of packets being transferred across the network.
2) Average end-to-end delay: The lowest average end-to-end delay was observed when sending data over 1 UE and at a rate of 15 pps as shown in Figure 4. However, the end-to-end delay sharply increased as the number of UEs increased, for all rates of transmission. The highest average end-to-end delay was observed for 2-3 UEs at 5 pps, followed by 1 UE and lastly, 3 UEs.
3) Average data per packet: Throughout the experiments, the average data per packet remained relatively stable as shown in Figure 3, averaging around 13 bytes.
4) Total data sent: Figure 6 shows how the total amount of data transmitted increased steadily as the number of UEs increased, which can be attributed to the higher volume of packet exchanges between the Modbus slave and master.

These results indicate that while increasing the packet rate may reduce the number of re-transmissions, the end-to-end delay is significantly affected by the number of UEs involved in the communication. Moreover, the results highlight the importance of optimizing the communication parameters, such as the number of UEs and the packet rate, to ensure efficient and reliable data transfer in 5G-based industrial control systems.

VI. Conclusion and Future Directions

This paper discusses the challenges and operational constraints of traditional OT devices and the need for more robust and resilient architectures through novel communication protocols, such as 5G technology. The physical constraints of implementing highly dynamic and flexible protocols that require unique network operations such as low latency and high availability are analyzed. The paper describes a novel 5G-enabled CPS architecture that integrates flexible and novel communication protocols with traditional OT devices. The architecture includes dedicated 5G communication channels that enable the translation of low-level communication protocols to highly flexible and mobile protocols. Intelligent network management technologies separate network data and state-of-health data, allowing OT operators to monitor sensing data and state-of-health data with a high degree of granularity. This enables more robust systems with low latency networks. In future iterations, the authors envision a high-fidelity experimental setup that uses Open Source MANO (OSM) [22] technologies through VM and cluster management tools such as Kubernetes (K8S) [23]. This will allow OT operators to rely on the real-time operational requirements of intelligent network management.

References

[1] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, "Toward adaptive and scalable openflow-sdn flow control: A survey," *IEEE Access*, vol. 7, pp. 107 346–107 379, 2019.

[2] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2637–2670, 2019.

[3] C. S. Choudhari, R. Patil, and S. Saraf, "Deployment of 5g core for 5g private networks," in *2022 International Conference on Industry 4.0 Technology (I4Tech)*, 2022, pp. 1–6.

[4] L. Chettri and R. Bera, "A comprehensive survey on internet of things (iot) toward 5g wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2020.

[5] W. Ruoxi, H. Beshley, Y. Lingyu, O. Urikova, M. Beshley, and O. Kuzmin, "Industrial 5g private network: Architectures, resource management, challenges, and future directions," in *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022, pp. 780–784.

[6] E. O'Connell, D. Moore, and T. Newe, "Challenges associated with implementing 5g in manufacturing," in *Telecom*, vol. 1, no. 1. MDPI, 2020, p. 5.

[7] L. M. Bartolín-Arnau, J. Vera-Pérez, V. M. Sempere-Payá, and J. Silvestre-Blanes, "Private 5g networks for cyber-physical control applications in vertical domains," in *2023 IEEE 19th International Conference on Factory Communication Systems (WFCS)*, 2023, pp. 1–4.

[8] M. Groshev, C. Guimarães, J. Martín-Pérez, and A. de la Oliva, "Toward intelligent cyber-physical systems: Digital twin meets artificial intelligence," *IEEE Communications Magazine*, vol. 59, no. 8, pp. 14–20, 2021.

[9] W. O'Brien, M. Hayes, M. Penica, J. McCann, D. Moore, and E. O'Connell, "Enabling communications for industry 4.0: Private 5g in smart manufacturing," in *2023 34th Irish Signals and Systems Conference (ISSC)*, 2023, pp. 1–7.

[10] C. Contoli, D. Rossi, G. Tontini, D. Borsatti, and F. Callegati, "Demonstration of digital twins for 5g connectivity in industry 4.0," in *2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2021, pp. 102–103.

[11] K. Deep Singh and S. K. Sood, "5g ready optical fog-assisted cyber-physical system for iot applications," *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 2, pp. 137–144, 2020.

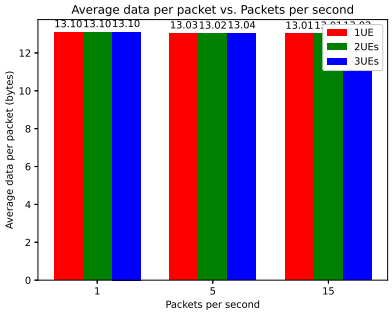

Fig. 3. Average data per packet

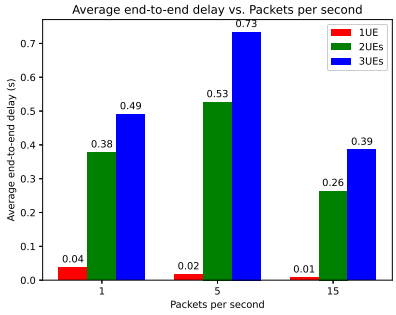

Fig. 4. Average end-to-end delay

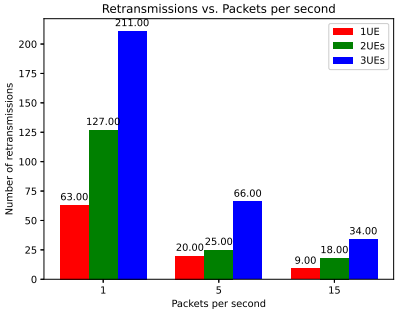

Fig. 5. Comparison of number of re-transmissions

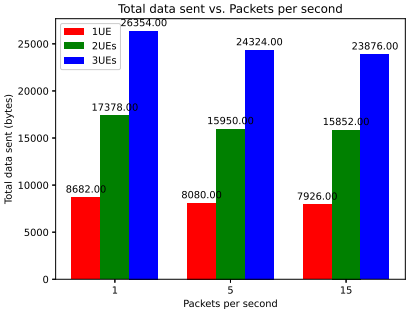

Fig. 6. Total amount of data transmitted

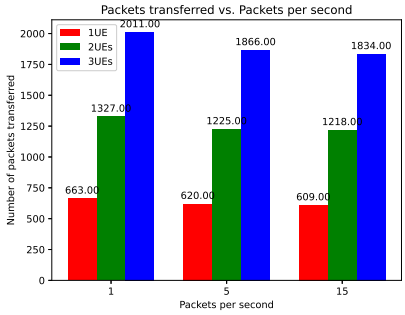

Fig. 7. Comparison of packets transferred and packets per second

[12] C. Tranoris, S. Denazis, L. Guardalben, J. Pereira, and S. Sargento, "Enabling cyber-physical systems for 5g networking: A case study on the automotive vertical domain," in *2018 IEEE/ACM 4th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, 2018, pp. 37–40.

[13] J. H. Park, S. Rathore, S. K. Singh, M. M. Salim, A. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "A comprehensive survey on core technologies and services for 5g security: taxonomies, issues, and solutions," *Hum.-Centric Comput. Inf. Sci*, vol. 11, no. 3, 2021.

[14] M. W. Hoffmann, S. Malakuti, S. Grüner, S. Finster, J. Gebhardt, R. Tan, T. Schindler, and T. Gamer, "Developing industrial cps: A multi-disciplinary challenge," *Sensors*, vol. 21, no. 6, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/6/1991

[15] C. Parian, T. Guldimann, and S. Bhatia, "Fooling the master: Exploiting weaknesses in the modbus protocol," *Procedia Computer Science*, vol. 171, pp. 2453–2458, 2020.

[16] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on scada systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[17] A. O. Gomez Rivera and D. K. Tosh, "Towards security and privacy of scada systems through decentralized architecture," in *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2019, pp. 1224–1229.

[18] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges," *Mechanical systems and signal processing*, vol. 135, p. 106382, 2020.

[19] W. Sun, X. Chen, Y. Zhao, and X. Huang, "Cybersecurity challenges and mitigation strategies for 5g enabled industrial internet of things," *IEEE Access*, vol. 8, pp. 114 149–114 160, 2020.

[20] S.-H. Han, J.-W. Lim, J.-H. Lee, and S. Lee, "A security analysis of 5g networks for industrial internet of things," *IEEE Access*, vol. 7, pp. 33 421–33 429, 2019.

[21] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane III, and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4281–4292, 2020.

[22] L. Mamushiane, A. A. Lysko, T. Mukute, J. Mwangama, and Z. D. Toit, "Overview of 9 open-source resource orchestrating etsi mano compliant implementations: A brief survey," in *2019 IEEE 2nd Wireless Africa Conference (WAC)*, 2019, pp. 1–7.

[23] Kubernetes documentation — kubernetes. [Online]. Available: https://kubernetes.io/docs/home/