Orchestrating 5G Network Slicing Through Software-Defined Network Architecture and Network Function Virtualization

Introduction

- Internet of Things (IoT), edge computing, and artificial intelligence are technologies that are being adopted in industrial environments.
- Heavy computing processes (HPCs) need data available instantly to give timely and accurate outputs used by other solutions.
- Recently, a report done by the Federal Bureau of Investigation (FBI) revealed the reception of 870 complaints on critical infrastructure being attacked with ransomware by threat actors only in 2022 [1].
- Another report by Dragos Inc. confirmed a 35% increase of threat actors targeting operational technologies (OT) [2].
- This research project contributes a solution to the need of timely data from different sources in an industrial environment while mitigating possible cyber-attacks that could impact the enterprise.

Background

- Network slicing becomes a useful tool to attend to the cybersecurity and timely data availability needs of the proposed industrial environment as a single network can be broken into others to destinate the kinds of data transferred through each partition and have rapid access to them while mitigating possible massive cyber-attacks.
- The Supervisory Control and Data Acquisition (SCADA) system is a common point for many Industrial Control Systems (ICS) architectures, which enables the creation of a 5G network slicing orchestrator that can be used for different use cases and data sources along the industrial site (see Figure 1).
- Industry 4.0 aims for an increased integration between operational technology (OT) and information technology (IT) systems, which can create more vulnerabilities and potential pathways for lateral movement by cyber-threat actors. Cyber-attacks on an industrial OT can impact the enterprise and the operability of companies and organizations [3].

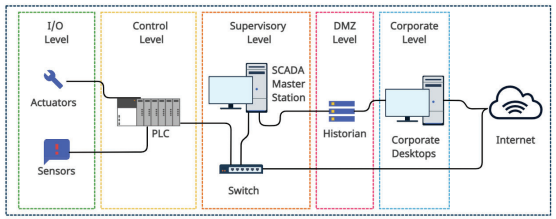

Figure 1. Operational technology ICS architecture.

Methodology

- Use the principle of Software-Defined Networking (SDN), which enables to programmatically define a network topology.
- Separate the control plane, responsible for making forwarding decisions, by making it software-based from the data plane, which is responsible for forwarding traffic (see Figure 2).
- Identify the data sources to determine the number of minimum slices necessary for the network topology.
- Design and deploy a centralized slicing management environment to decentralize the networks in an orchestrated way.
- Deploy the network slices for use in the distributed machine learning model, our HPC, for network anomalous event detection.

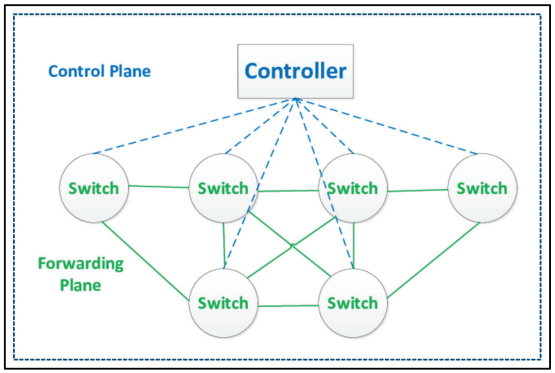

Figure 2. SDN planes diagram.

Results

- The 5G network was sliced in two partitions for the transfer of field sensor and components' health data (see Figure 3).
- Network Function Virtualization (NFV) abstracted network services, such as routing and firewalling, into software-based instances.
- Open Source MANO (OSM) was used in an Ubuntu Server Virtual Machine (VM) for NFV Management and Orchestration (MANO).
- Security measures were considered from the Cybersecurity and Infrastructure Security Agency (CISA) [4].

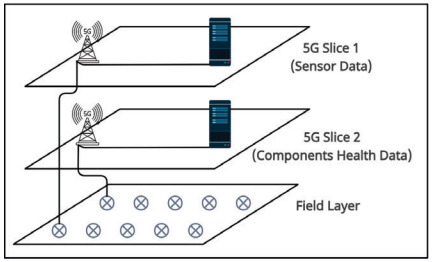

Figure 3. Network slicing scenario.

Conclusions and Future Work

- This work contributes an orchestrator for 5G network slicing in industrial environments using Open Source MANO (OSM).
- OSM was used mostly for mobile and IoT solutions, but not with an industrial or operational technology (OT) focus.
- This solution allows for time-sensitive, high throughput, and reliable transfer of critical data in industrial sites.
- Heavy computing applications can work efficiently while being in an environment that preserves the security of the enterprise level.
- In the future, I plan on deploying the solution in a private cloud environment by using a virtual machine to centralize OSM.
- Having a cloud-based platform for this solution will allow for more resources control when scaling the partitions (see Figure 4).

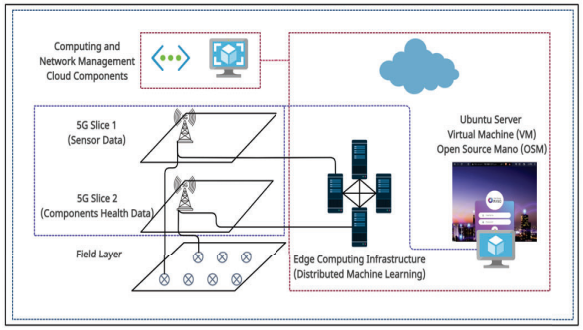

Figure 4. Implementation diagram using a private cloud environment.

References

1. Internet Crime Complaint Center (IC3). (2022). 2022 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
2. Dragos. (2022). Year in Review Report 2022. https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Report-2022.pdf?hsLang=en.
3. Hollerer, Siegfried, et al. (2022) Risk Assessments Considering Safety, Security, and Their Interdependencies in OT Environments. Proceedings of the 17th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3538969.3543814.
4. Cybersecurity and Infrastructure Security Agency (CISA). (2023). 5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance. https://www.cisa.gov/topics/risk-management/5g-security-and-resilience.

Brian G. Rodiles-Delgado, Deepak Tosh
Computer Science Department, The University of Texas at El Paso, El Paso, TX 79968