Low-overhead and Non-invasive Electromagnetic Side-Channel Monitoring for Forensic-ready Industrial Control Systems

Buddhima Weerasinghe
University of Colombo School of Computing
Colombo, Sri Lanka
ima@ucsc.cmb.ac.lk

Asanka Sayakkara
University of Colombo School of Computing
Colombo, Sri Lanka
asa@ucsc.cmb.ac.lk

Kasun De Zoysa
University of Colombo School of Computing
Colombo, Sri Lanka
kasun@ucsc.cmb.ac.lk

Mark Scanlon
School of Computer Science
University College Dublin
Dublin, Ireland
mark.scanlon@ucd.ie

Abstract

Industrial control systems (ICS) are the backbone of modern manufacturing facilities. Due to the distributed nature of ICS hardware in their deployment environment, they are often networked through Ethernet, opening up a window for network-based attacks. Preventive security measures, such as constant packet capture and inspection, are impractical due to the computational overhead required. Therefore, computationally feasible trigger mechanisms are needed that can activate security, as well as on-demand forensic readiness features, in the infrastructure. This work proposes an approach to monitor ICS network infrastructure using unintentional electromagnetic (EM) radiation emitted by Ethernet network cables during their regular operation. An empirical evaluation highlights that it is possible to detect various types of denial of service (DoS) attacks through EM emission patterns of Ethernet cables with considerable accuracy (HTTP Flood = 99.70%, TCP Flood = 73.22%, UDP Flood = 69.95%). Based on the experimental findings, this work introduces an architecture for the ICS infrastructure to be forensic-ready with minimal computational resources while being independent and non-invasive to the infrastructure itself.

CCS Concepts

• **Applied computing** → **Surveillance mechanisms**; **Network forensics**; • **Security and privacy** → *Side-channel analysis and countermeasures.*

Keywords

Industrial control systems, electromagnetic side channel analysis, network security, forensic readiness

ACM Reference Format:
Buddhima Weerasinghe, Asanka Sayakkara, Kasun De Zoysa, and Mark Scanlon. 2025. Low-overhead and Non-invasive Electromagnetic Side-Channel Monitoring for Forensic-ready Industrial Control Systems. In *Digital Forensics Doctoral Symposium (DFDS 2025), April 01, 2025, Brno, Czech Republic.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3712716.3712722

DFDS 2025, Brno, Czech Republic
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1076-6/25/04
https://doi.org/10.1145/3712716.3712722

1 Introduction

Modern industrial manufacturing facilities consist of highly complicated machinery that is required to operate around the clock to meet production targets. Industrial control systems (ICS) are the backbone of these highly demanding environments, which monitor and control factory equipment to keep them in order [10]. ICSs are typically networked together over Ethernet [5]. The significant role ICS plays attracts a host of security threats. Being network devices with time-sensitive functionalities, most of such threats are delivered through the network [3]. Network-based attacks to ICS includes, denial of service (DoS) attacks, remote malware infections, Man-in-the-Middle attacks (MitM), Spoofing, etc. These attacks can originate from both external and internal sources. For example, a DoS attack may originate from malware-infected network devices from an industrial facility that targets a critical component of their own ICS [11].

When security incidents related to ICS occur, they are subject to forensic investigations [23]. The success of such a forensic analysis depends on the availability of useful evidence retained in the ICS and other network infrastructure. This had led to the need to have a comprehensive network forensic readiness strategy in place to ensure that pertinent evidence is available when needed, but the balance of how much network traffic to store comes with considerations on performance impacts and potentially excessive data collection [17]. Various network and embedded system security mechanisms can be employed in ICS to ensure their security. Furthermore, their forensic readiness can be enabled through the continuous capture and saving of network packets, the regular preservation of the internal states of the ICS devices, and various other methods. Enabling measures for ICS security and forensic readiness have been shown to incur significant computational overhead in terms of real-time processing of network traffic and storage capacity [2]. Meanwhile, not having such measures in place can derail an investigation due to the loss of valuable evidence during the post-incident stage [1].

An ideal mechanism to ensure security and forensic readiness of ICS infrastructure should consist of a variety of measures that should be enabled on demand whenever an indication of a threat/incident is looming. This could be detected and triggered by an independent monitoring mechanism that has minimal computational overheads. The necessity for such trigger mechanisms to be independent from the ICS infrastructure itself is due to the possibility that whatever threatening the ICS infrastructure can pose the same threat to the security and forensic readiness triggering mechanisms. In these circumstances, research is needed to discover novel non-invasive, low-overhead, network-based threat detection mechanisms.

This work explores the potential of using electromagnetic (EM) radiation emitted by the ICS network infrastructure as a window to detect network-based threats and act as a trigger mechanism to activate the forensic readiness features of the ICS infrastructure. Toward this goal, through empirical experimentation, appropriate algorithms, tools, and techniques are developed and tested to evaluate the effectiveness of such an approach.

This paper makes the following contributions:

- Introduces EM side-channel analysis (EM-SCA) as a non-intrusive technique to detect network-based threats to ICS infrastructure.
- Experimentally evaluates three light-weight machine learning algorithms to process EM radiation patterns caused by malicious traffic.
- Presents a methodology to trigger security and forensic-readiness features of ICS infrastructure with minimal overhead.

The rest of this paper is organised as follows. Section 2 provides a brief overview of the state-of-the-art in this problem domain. Section 3 introduces the tools and techniques used to capture and analyse radiation data originating from Ethernet network infrastructure. Based on these techniques, Section 4 experimentally evaluates multiple machine learning algorithms to distinguish EM radiation patterns caused by malicious network traffic. Section 5 proposes a novel ICS security architecture based on the experimental findings. Finally, Section 6 discusses the conclusion and future directions of this work.

2 Related Work

Detecting network-based attacks through traffic pattern analysis is a widely studied area [16]. Specific packet types like TCP or UDP and the rate at which they flow can signal potential attacks. Neto et al. [15] created a comprehensive dataset of network attacks comprising 33 types grouped into seven categories, including DDoS, DoS, reconnaissance, web-based, brute force, spoofing, and Mirai attacks. Their study shows that machine learning algorithms can effectively distinguish between these attacks with high accuracy, underscoring the importance of network traffic data in attack classification. Similarly, Dhanya et al. [4] designed machine learning and deep learning models to detect intrusions and classify attacks, using the UNSW-NB15 dataset [14], which features nine types of attacks and 49 attributes derived from contemporary network traffic patterns.

For Industrial Control Systems (ICS), detecting anomalous behaviour often relies on data from various sensors. Tang et al. [22] used neural graph networks for anomaly detection in ICS environments, while Kim et al. [12] explored several machine learning-based techniques for the same purpose. By aggregating data from multiple sensors, such as temperature or flow sensors, these approaches produce accurate and reliable results. However, centralising and processing large volumes of sensor data poses computational challenges, especially with the increased complexity of modern machine learning models that require significant computational resources.

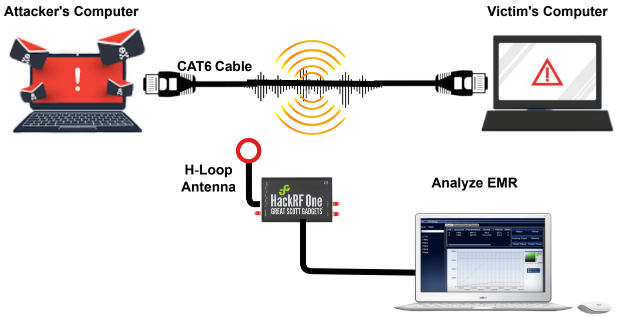

Figure 1: Overview of the experimental hardware setup.

In recent years, information leakage via EM radiation from Ethernet cables has become a significant concern in security and digital forensics. Schulz et al. [21] explored the vulnerabilities of Ethernet networks to -destructive wiretap attacks, demonstrating that attackers using a USRP X300 device can intercept and decode sensitive information, such as the preamble, start of frame delimiter (SFD) and MAC address. Further expanding on this threat, Guri introduced LANTENNA [8], an EM attack that enables data leakage from air-gapped networks by turning Ethernet cables into unintended transmitting antennas. This approach uses malware to manipulate the EM emissions of a compromised workstation's Ethernet cable, allowing covert data transmission. Similarly, Sachintha et al. [18] revealed a related EM-based attack targeting Industrial Control Systems (ICS), where compromised firmware in network controllers can encode sensitive information within network packet patterns. An attacker can capture the EM radiation from a few metres away to extract the transmitted data.

These studies highlight the evolving risk landscape, where EM radiation from wired connections becomes a potential conduit for covert data exfiltration.

3 Radiation from Network Infrastructure

Although a wide array of frequency channels have the potential to convey information about network traffic, typically only a small subset of them prove to be truly valuable. Some channels may contain redundant information, while others might not disclose any information at all. Hence, the identification of these informative frequency channels from the numerous available channels plays a pivotal role in enhancing the efficiency of EM-SCA for digital forensics [19, 20].

3.1 Experimental Hardware Setup

The experimental hardware setup involves a computer, representing the attacker, connected to another computer, representing the victim, via a Cat 6 unshielded twisted pair (UTP) Ethernet cable, simulating the ICS wired network. EM radiation signals from this setup are captured using a HackRF One [6] SDR device, paired with a magnetic H-loop antenna, and connected to the investigator's computer. The collected EM radiation data are stored on the investigator's computer for subsequent analysis. Figure 1 depicts the arrangement of the target network and the attacker's equipment in the experimental scenario. For the experimental evaluation of this phase, where the radiation emission frequency of the Ethernet cable is identified, both the attacker's computer connected to the Cat 6 cable and the investigator's computer connected to the SDR hardware are set to be the same machine.

3.2 Experimental Software Setup

In order to conduct experiments, a program with 3 parallel threads was executed on the attacker's computer for data collection in an annotated manner. The first thread is tasked with the transmission of network traffic on-demand over the Ethernet cable. Simultaneously, the second and third threads undertake the responsibility of capturing EM radiation and monitoring of network interfaces to identify outbound packets, respectively. Using this software setup, it is possible to transmit a specific network traffic pattern on the cable while capturing the same network packets as PCAP files, as well as emitted radiation data files, in a precisely timed manner.

3.3 Collection of Data

In accordance with insights from Guri's work [8], it has been established that Ethernet cables emit EM waves primarily in the frequency bands of 125 MHz and its harmonics, with 250 MHz being the most prominent among these harmonics. Consequently, in this work, the experiments were tailored to scan the frequency range spanning from 30 MHz to 260 MHz to pinpoint an information leakage channel. It is important to note that the lower operating frequency limit of HackRF is at 20 MHz, and approaching this limit may introduce interference from internal circuitry. Therefore, it was pragmatically decided to set 30 MHz as the lower limit of the frequency range for this investigation to ensure a reliable data collection.

The experimental software setup running on the hardware setup operates seamlessly to autonomously gather samples across the 30–260 MHz frequency range. The packet sender produces heavy TCP traffic using the Python Scapy library across the cable at each frequency, while the setup records the EM data in the in-phase and quadrature (IQ) data format and a corresponding PCAP file for each packet pattern. For benign traffic at each frequency, a separate IQ file and a PCAP file are recorded during the normal operation of the devices.

3.4 Dissimilarity Analysis Algorithm

Analysing the dissimilarity between two traffic patterns is a crucial component of the methodology, tasked with comparing each EM trace of heavy traffic for a given signal frequency with benign traffic EM trace of the same frequency. This comparison aims to identify the frequency at which the two network traffic patterns produce the most distinct EM radiation patterns. The procedure to achieve this task, as shown in Algorithm 1, begins by computing the Fast Fourier Transform (FFT) of EM trace files and subsequently applying the resulting FFT vectors to different similarity measurement functions, namely, cross-correlation (xCor) and normalised cross-correlation (nXCor). The calculated correlation values are then recorded in a file for subsequent analysis. The algorithm considers the shortest file length as the FFT window size, accounting for discrepancies in array sizes between the two traces.

Algorithm 1 Dissimilarity Analysis Algorithm

```
Require: $Data_1$: Data set containing malicious pattern traces.
         $Data_2$: Data set containing benign pattern traces.
Ensure: Similarity measurement of patterns.
for freq ← 30 to 260 MHz do
    for $pattern_i$ from $Data_1[freq]$ and $pattern_j$ from $Data_2[freq]$ do
        windowSize ← minLength($pattern_i$, $pattern_j$)
        fft$_i$ ← getFFT($pattern_i$, windowSize)
        fft$_j$ ← getFFT($pattern_j$, windowSize)
        xCor ← crossCorrelate(fft$_i$, fft$_j$)
        nXCor ← NormalizedCrossCorrelate(fft$_i$, fft$_j$)
        results[ ] ← (xCor, nXCor)
    end for
end for
output ← minimumSimilarity(results[ ])
```

The results of the analysis were saved to a CSV file and later plotted to visualise the variation of correlation values across different suspicious emission frequencies. As is evident in Figure 2, the xCor parameter exhibits a lower correlation than nXCor, and the most dissimilarity of two traffic patterns occurs at 240 MHz. After manually validating these results, the emitting frequency for the Cat 6 UTP cable was determined as 240 MHz. In Figure 3, the radiation pattern for attack traffic is depicted in red, while benign traffic is represented in green. A distinct contrast is evident between the two packet patterns within these PSD graphs.

4 Detection of Network Attacks

Once the emission frequency of the EM radiation was identified for the target Ethernet cable, the same hardware and software setup was used to emulate realistic network-based attack scenarios. In order to produce realistic attack traffic patterns on the Ethernet cable, the CICIoT2023 dataset [15] network attack dataset was used. The CICIoT2023 dataset is available in two different file formats: PCAP [9] and CSV. The PCAP files comprise the original data generated and collected in the CIC IoT network, which is the IoT infrastructure that consists of 105 IoT devices. The PCAP files were replayed by the software setup to recreate the exact attack scenarios on the experimental hardware platform. The selected attacks include DoS HTTP Flood, DoS TCP Flood, and DoS UDP Flood.

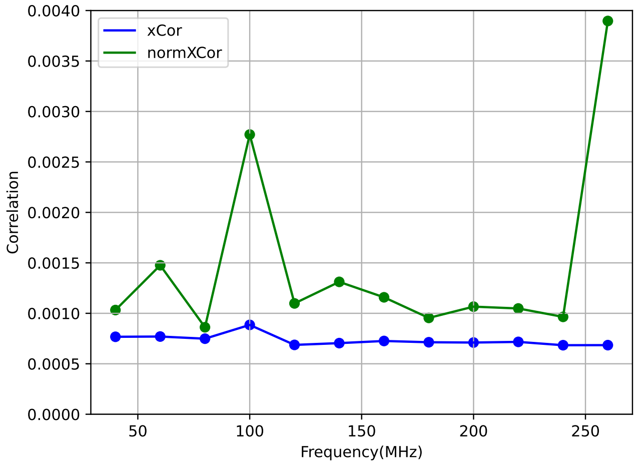

Figure 2: Variation of correlation measurements across various suspected emission frequencies.

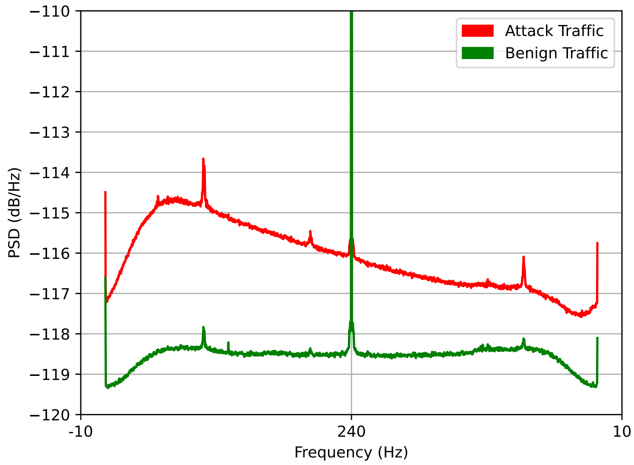

Figure 3: The power spectral density (PSD) variation of two traffic patterns at 240 MHz emission frequency.

4.1 Data Preprocessing for Machine Learning

EM radiation samples were collected at a sampling rate of 20 MHz with a target centre frequency of 240 MHz. Each trace file, representing a time-domain signal, underwent Short-time Fourier Transformation (STFT) processing to generate frequency-domain windows. In the case of MLP, RFC with AdaBoost, and SVM models, these windows were utilised as training instances, with labels corresponding to the respective network traffic.

Subsequently, individual ML models were constructed to identify malicious network activity using the resulting EM datasets for each network attack. For this purpose, 10,000 samples were extracted from each EM trace file representing a specific network attack, the relevant network attack serving as the label. Certain hyperparameters were determined on the basis of the dimensions of the EM datasets. During hyperparameter tuning, specific settings for the STFT operation, such as the FFT window size and overlapping samples, were adjusted accordingly.

4.2 Experiment 1: Impact of Probe Location

This experiment was conducted with the aim of discovering the optimal probe placement for maximising signal reception and detection. The entire data collection process was repeated 9 times, covering 3 attacks at 3 different locations, to explore various probe positions relative to the Ethernet cable. These locations were empirically selected to gauge the sensitivity of the ML models to probe placement.

Initially, the probe was positioned directly on top of the cable, in direct contact with it, marking the initial phase of analysis. Given its proximity to the primary emission source, it was expected to generate the strongest EM field, facilitating optimal signal detection. Subsequently, the probe was elevated 1cm and 10cm above the cable to simulate scenarios where cables are installed under enclosures. The results of these experiments are presented in table 1. For the initial phase, where the H-Loop antenna (EM probe) was placed directly in contact with the cable, the attacks are distinguishable from normal traffic, with DoS HTTP Flood exhibiting the highest detectability. Across all models, the highest accuracy for DoS HTTP Flood is at 99.70%. Following this, DoS TCP Flood demonstrates the highest accuracy at 73.22%, while DoS UDP Flood ranks last with the highest accuracy at 69.95%.

When the EM probe is located 1cm away from the cable, the overall accuracy in all traffic patterns falls below 60%, suggesting a detectable difference between normal and malicious operations, although less pronounced than before. Notably, the distinct gap observed in accuracy between HTTP Flood and TCP and UDP Floods diminishes. All accuracy values are within the same range, with RFC consistently demonstrating the highest accuracy. In addition, the precision and recall values align closely with the accuracy. Compared to the experiment with the probe directly atop the cable, a decrease is observed in all results, consistent with expectations that the initial location would yield higher accuracy. Meanwhile, when the EM probe is located 10cm away from the cable, the overall accuracy is recorded below 59%. However, the effectiveness of detection between normal and malicious operations remains consistent despite the change in probe location.

4.3 Experiment 2: Impact of Observation Time

When detecting network-based attacks, it is necessary to perform the detection in a minimal amount of time. The longer it takes for detection, the greater the possibility of an attack causing damage to the ICS infrastructure. With this objective, this experiment aims to determine the point in time during the attack at which it is most detectable, whether it occurs at the beginning, middle, or end of the observation time period. For this purpose, the dataset is divided into segments that correspond to the start, middle, and end of the attack sequence. Each segment is then individually analysed to assess the ability to detect it using ML algorithms. By comparing

Table 1: Performance comparison of DoS attack detection over probe placement.

Probe placement	DoS HTTP flood			DoS UDP flood			DoS TCP flood		
	RFC	MLP	SVM	RFC	MLP	SVM	RFC	MLP	SVM
On the cable	99.70	99.55	99.68	69.95	57.70	66.25	73.22	67.25	66.42
1cm away	60.42	51.90	53.99	59.38	55.15	54.26	59.50	52.00	55.57
10cm away	59.92	52.30	54.70	60.05	54.80	54.51	58.83	51.40	54.21

Table 2: Performance comparison of DoS attack detection over time splits.

Time Split	DoS HTTP flood			DoS UDP flood			DoS TCP flood		
	RFC	MLP	SVM	RFC	MLP	SVM	RFC	MLP	SVM
First third	99.58	99.40	99.73	70.43	54.20	58.95	67.70	51.65	61.60
Middle third	99.70	99.60	99.63	71.17	56.65	68.94	63.25	52.20	56.72
Last third	99.50	99.50	99.58	67.92	53.70	56.58	70.62	54.60	57.77

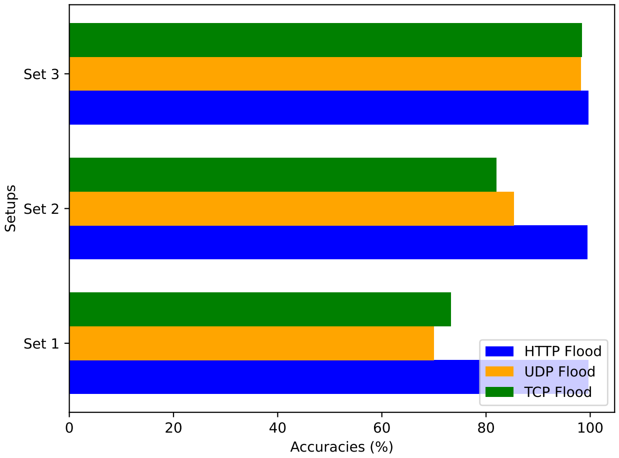

Figure 4: DoS Attack Accuracies Across Different Setups

the accuracy of detection across these segments, insights can be gained into the optimal timing to detect malicious network activity.

The analysis was performed using the dataset collected with the probe in contact with the cable. The dataset was divided into three subsets and the ML classification results were calculated for each subset. New models were trained for each subset and the results are illustrated in Table 2. In both HTTP and UDP DoS attacks, a slight increase in accuracy could be observed in the middle third time point compared to the other two time points. In contrast, TCP DoS attack exhibits a slight decrease in accuracy at the middle third time point compared to the other two time points.

4.4 Experiment 3: Impact of Sampling Rate

Capturing EM data with SDR devices requires extremely fast sample rates to capture a significant amount of information. Reducing the sample rate below a certain threshold can adversely impact the detection process. It is crucial to identify the minimum sample rate that does not compromise the effectiveness of ML-based classification for detecting malicious network activity. In this experiment, due to the lower accuracy observed (>75%) with the other two attacks, only the DoS HTTP Flood dataset collected with the probe in contact with the cable was considered. The original trace file was downsampled to 10 MHz and 4 MHz, resulting in two new trace files. These downsampled files were then used as input data for the ML models to perform the classification task.

The RFC with Adaboost and SVM models maintained close to 100% accuracy consistently at all sample rates, indicating strong performance even at lower sample rates. However, the MLP model experiences a noticeable drop in accuracy at 4 MHz, only reaching around 80%, before achieving high accuracy at higher sample rates. This suggests that while RFC and SVM are robust to lower sample rates, MLP requires a higher sample rate for optimal accuracy.

4.5 Experiment 4: Impact of the Environment

This experiment was conducted to explore the effect of ambient EM radiation in the environment on the accuracy of the classification. For this purpose, EM traces were captured under three distinct environmental conditions, i.e., Setup 1, 2 and 3, for each attack, and the accuracy of classification was assessed. The probe remained in contact with the cable during these conditions. Setup 1 corresponds to the traces used in previous experimental efforts. Setup 2 comprises data collected using the same hardware setup in a different environment, while Setup 3 encompasses traces collected in an alternate hardware configuration where the victim device was altered. RFC with AdaBoost was used for this analysis, given its superior accuracy in prior investigations. As illustrated in Figure 4, it can be seen that the DoS HTTP flood maintains a consistent accuracy across all setups. However, there is notable variability in the accuracies of DoS UDP and DoS TCP flood across different setups.

5 Monitoring Industrial Control Systems

The empirical findings in Section 4 point to the possibility of using EM radiation patterns emerging from network infrastructure to look out for network-based attacks. This section introduces a potential design blueprint for an EM-SCA-based, low-overhead, and non-intrusive ICS monitoring mechanism.

5.1 Implementation Considerations

A network-based threat detection mechanism of this nature has to include an EM radiation capturing and processing capability in real time. Although the experiments presented relied on SDR hardware to discover and capture EM emissions, it is not necessary to use them in a real-world deployment. Once the emission frequency of the infrastructure is identified, a purpose-built fixed radio receiver can be used to capture EM emission. Furthermore, the processing of captured EM data in real time can be performed onboard the signal capturing hardware using a dedicated embedded processor or a field-programmable gate array (FPGA) built into the signal capturing hardware itself [7]. Self-contained EM radiation capture and processing equipment (called a *monitor node* hereafter) can be powered using the same power supply facility in the ICS infrastructure. However, networking them with each other needs to be achieved using a communication infrastructure independent of the ICS network.

There are multiple potential approaches to connect the monitor nodes together. The obvious solution is to have a separate internal network — wired or wireless — to which the monitor nodes are connected. However, because monitor nodes do not require a high-bandwidth communication channel, having a dedicated network only to serve them is an unnecessary overhead. Alternatively, it is possible to use the existing power supply infrastructure for transferring network packets in a reliable manner, i.e., powerline communication [13]. In that approach, the monitor nodes can deliver their detection alerts and other telemetry through their power supply wiring, which is highly reliable and difficult to disrupt by an attacker.

5.2 High-level Design

Figure 5 illustrates the high-level view of an ICS infrastructure where monitor nodes are deployed in multiple locations on the network. At the highest level, i.e., Level 3, of the ICS infrastructure, there are engineering workstations that run specialised software to govern the entire manufacturing process. The level below that, i.e., Level 2, has a human-machine interface (HMI) that facilitates monitoring and controlling specific functionalities of the ICS infrastructure by allowing human technicians to interact with the devices. At Level 1, all automated devices are placed to operate the ICS infrastructure, such as programmable logic controllers (PLC), intelligent electronic devices (IED), and remote terminal units (RTU). Finally, at Level 0, the sensors and actuators that perform the manufacturing tasks are available.

5.3 Backbone-level Monitoring

The monitor nodes can be placed at different locations throughout the ICS infrastructure. Among them, an important and most obvious location is at the backbone level of the network, which connects general-purpose computers at Level 3 to other levels in the infrastructure. If packet sniffing and other security mechanisms were always active in the network at this level, the processing and storage overhead would be significantly higher. In contrast, the monitor node that works in this network segment will be processing EM emission in real time with a fixed processing overhead and no storage requirement.

5.4 Device-level Monitoring

Although the monitoring at the backbone-level of the network allows the observation of the full picture of network behaviour from outside world, it does not enable detecting subtle traffic patterns at the close proximity to different individual ICS devices. Therefore, it is important to deploy and monitor nodes at branches in the ICS network, closer to individual devices of interest. An important advantage the monitor nodes have is that regardless of where exactly they are deployed in the network, i.e., at a busy network backbone or low-traffic branch, they have the same amount of processing and other computational resource usage. Hence, the monitor nodes distributed across the ICS infrastructure will be identical in all aspects.

6 Conclusion and Future Direction

This work demonstrates the potential of using unintentional EM radiation emitted from Ethernet cables as a non-invasive tool for enhancing security and forensic readiness in ICS. By employing EM side-channel monitoring, we can detect network-based attacks without directly interfacing with the ICS infrastructure, making this approach particularly valuable for independent forensic audits. Through targeted frequency identification and EM trace analysis using efficient machine learning models, such as Random Forest classifiers with AdaBoost, our method achieved a high detection accuracy of 99.70%, supporting the feasibility of resource-conscious real-time attack detection in ICS environments.

Machine learning models such as RFC with AdaBoost, MLP, and SVM ensure low processing overhead, making them suitable for resource-constrained environments. Future developments include creating a compact self-contained hardware unit that integrates EM signal capture, embedded processing, and real-time analysis. This scalable and efficient design would enhance ICS security, providing responsive and autonomous intrusion detection capabilities.

Acknowledgments

We acknowledge the funding received from the University of Colombo School of Computing through the Research Allocation for Research and Development, under Grant No: UCSC/RQ/2024/Sec&For/01. This financial support contributed significantly to the success and publication of this research work.

Appendix A

Figure 5 illustrates the high-level view of the ICS infrastructure with the placement of the sniffer and monitor nodes. In this ICS infrastructure, the typical network security and forensic-readiness features are available, such as packet sniffers in strategic locations of the network. However, they are deactivated by default and only enabled on demand whenever a suspicious network-based threat is noticed. The network of the monitor nodes that captures EM radiation data and processes in real time for suspicious activity is placed independently of the ICS infrastructure. They communicate with each other through their own independent network, such as powerline communication, and are capable of directly communicating with security components, such as packet sniffers. These packet sniffers and any other security mechanisms are activated directly by a monitor node upon the detection of suspicious network activity.

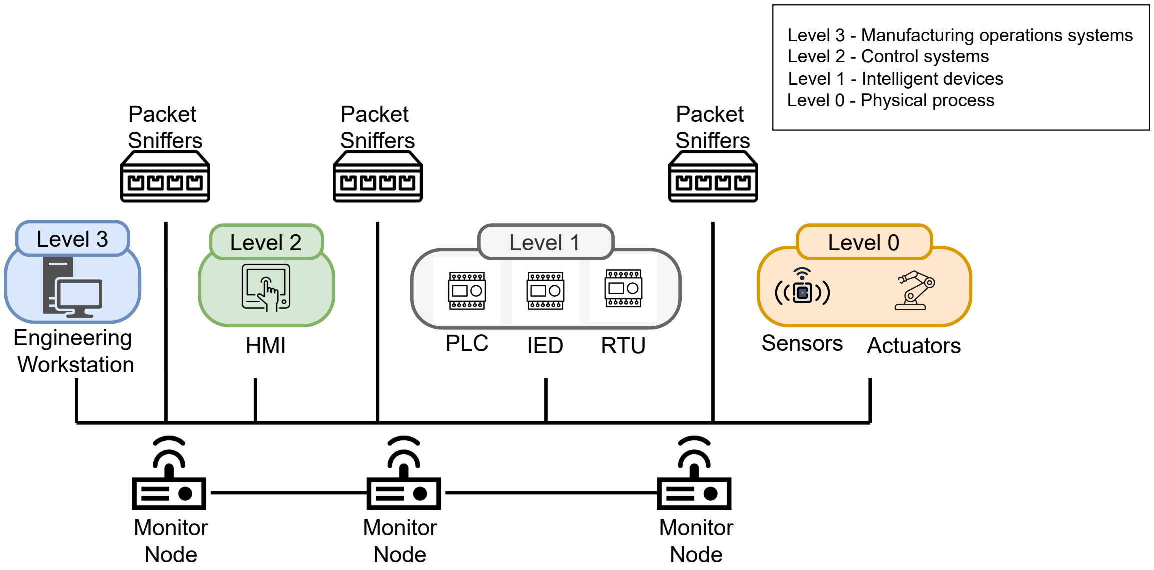

Figure 5: A high-level view of an ICS infrastructure with EM-SCA monitoring mechanism in place.

References

[1] Mohammed Asiri, Neetesh Saxena, Rigel Gjomemo, and Pete Burnap. 2023. Understanding indicators of compromise against cyber-attacks in industrial control systems: a security perspective. *ACM transactions on cyber-physical systems* 7, 2 (2023), 1–33.

[2] Mazen Azzam, Liliana Pasquale, Gregory Provan, and Bashar Nuseibeh. 2023. Forensic readiness of industrial control systems under stealthy attacks. *Computers & Security* 125 (2023), 103010.

[3] Mauro Conti, Denis Donadel, and Federico Turrin. 2021. A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials* 23, 4 (2021), 2248–2294.

[4] K.A. Dhanya, Sulakshan Vajipayajula, Kartik Srinivasan, Anjali Tibrewal, T. Senthil Kumar, and T. Gireesh Kumar. 2023. Detection of Network Attacks using Machine Learning and Deep Learning Models. *Procedia Computer Science* 218 (2023), 57–66. https://doi.org/10.1016/j.procs.2022.12.401 International Conference on Machine Learning and Data Engineering.

[5] Zaloa Fernandez, Oscar Seijo, Mikel Mendicute, and Inaki Val. 2019. Analysis and Evaluation of a Wired/Wireless Hybrid Architecture for Distributed Control Systems With Mobility Requirements. *IEEE Access* 7 (2019), 95915–95931. https://doi.org/10.1109/ACCESS.2019.2927298

[6] Great Scott Gadgets. 2024. *HackRF One*. https://greatscottgadgets.com/hackrf/one/ Accessed: April 2024.

[7] Davide Giri, Kuan-Lin Chiu, Giuseppe Di Guglielmo, Paolo Mantovani, and Luca P Carloni. 2020. ESP4ML: Platform-based design of systems-on-chip for embedded machine learning. In *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 1049–1054.

[8] Mordechai Guri. 2021. LANTENNA: Exfiltrating Data from Air-Gapped Networks via Ethernet Cables. *CoRR* abs/2110.00104 (2021). arXiv:2110.00104 https://arxiv.org/abs/2110.00104

[9] G. Harris. 2022. PCAP-NG Summary Block Compatibility Specification. https://datatracker.ietf.org/doc/id/draft-gharris-opsawg-pcap-00.html.

[10] Peng Jie and Liu Li. 2011. Industrial control system security. In *2011 third international conference on intelligent human-machine systems and cybernetics*, Vol. 2. IEEE, 156–158.

[11] Christopher Kelly, Nikolaos Pitropakis, Sean McKeown, and Costas Lambrinoudakis. 2020. Testing and hardening IoT devices against the Mirai botnet. In *2020 International conference on cyber security and protection of digital services (cyber security)*. IEEE, 1–8.

[12] Bedeuro Kim, Mohsen Ali Alawami, Eunsoo Kim, Sanghak Oh, Jeongyong Park, and Hyoungshick Kim. 2023. A comparative study of time series anomaly detection models for industrial control systems. *Sensors* 23, 3 (2023), 1310.

[13] Anindya Majumder et al. 2004. Power line communications. *IEEE potentials* 23, 4 (2004), 4–8.

[14] Nour Moustafa and Jill Slay. 2015. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). https://doi.org/10.1109/MilCIS.2015.7348942

[15] Euclides Carlos Pinto Neto, Sajjad Dadkhah, Raphael Ferreira, Alireza Zohourian, Rongxing Lu, and Ali A. Ghorbani. 2023. CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. *Sensors* 23, 13 (2023). https://doi.org/10.3390/s23135941

[16] Syed Rizvi, Mark Scanlon, Jimmy McGibney, and John Sheppard. 2022. Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions. *IEEE Access* 10 (10 2022).

[17] Syed Rizvi, Mark Scanlon, Jimmy McGibney, and John Sheppard. 2024. Pushing Network Forensic Readiness to the Edge: A Resource Constrained Artificial Intelligence Based Methodology. In *2024 Cyber Research Conference - Ireland (Cyber-RCI)*. IEEE.

[18] Shakthi Sachintha, Nhien-An Le-Khac, Mark Scanlon, and Asanka P. Sayakkara. 2023. Data Exfiltration through Electromagnetic Covert Channel of Wired Industrial Control Systems. *Applied Sciences* 13, 5 (2023). https://doi.org/10.3390/app13052928

[19] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2018. Electromagnetic side-channel attacks: potential for progressing hindered digital forensic analysis. In *Companion Proceedings for the ISSTA/ECOOP 2018 Workshops* (Amsterdam, Netherlands) *(ISSTA '18)*. Association for Computing Machinery, New York, NY, USA, 138–143. https://doi.org/10.1145/3236454.3236512

[20] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2020. EMvidence: A Framework for Digital Evidence Acquisition from IoT Devices through Electromagnetic Side-Channel Analysis. *Forensic Science International: Digital Investigation* 32 (04 2020), 300907. https://doi.org/10.1016/j.fsidi.2020.300907

[21] Matthias Schulz, Patrick Klapper, Matthias Hollick, Erik Tews, and Stefan Katzenbeisser. 2016. Trust The Wire, They Always Told Me! On Practical Non-Destructive Wire-Tap Attacks Against Ethernet. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 43–48.

[22] Chaofan Tang, Lijuan Xu, Bo Yang, Yongwei Tang, and Dawei Zhao. 2023. GRU-based interpretable multivariate time series anomaly detection in industrial control system. *Computers & Security* 127 (2023), 103094.

[23] Ken Yau, Kam-Pui Chow, and Siu-Ming Yiu. 2019. An Incident Response Model for Industrial Control System Forensics Based on Historical Events. In *13th International Conference on Critical Infrastructure Protection (ICCIP) (Critical Infrastructure Protection XIII, Vol. AICT-570)*, Jason Staggs and Sujeet Shenoi (Eds.). Springer International Publishing, Arlington, VA, United States, 311–328. https://doi.org/10.1007/978-3-030-34647-8_16 Part 6: Industrial Control Systems Security.