Cyber-Physical Anomaly Detection for ICS

Lars Wüstrich
Technical University of Munich
wuestrich@net.in.tum.de

Lukas Schröder
Technical University of Munich
lukas.schroeder@tum.de

Marc-Oliver Pahl
IMT Atlantique
marc-oliver.pahl@imt-atlantique.fr

***Abstract*—Industrial Control Systems (ICS) are complex systems made up of many components with different tasks. For a safe and secure operation, each device needs to carry out its tasks correctly. To monitor a system and ensure the correct behavior of systems, anomaly detection is used.**
Models of expected behavior often rely only on cyber or physical features for anomaly detection. We propose an anomaly detection system that combines both types of features to create a dynamic fingerprint of an ICS. We present how a cyber-physical anomaly detection using sound on the physical layer can be designed, and which challenges need to be overcome for a successful implementation. We perform an initial evaluation for identifying actions of a 3D printer.

***Index Terms*—ICS, security, cyber-physical systems, fingerprinting, anomaly detection, sound**

I. Introduction

Industrial Control Systems (ICS) interact with the real world to manage and manipulate physical processes. Examples are power grids, chemical, water treatment, or nuclear plants [1]. To ensure a safe operation, each ICS component needs to execute its task correctly. This requires to check a system's functionality and status.

A common method to find deviations from expected behavior is anomaly detection [2]. It triggers alarms in case a system's observed behavior differs from its expected behavior. The expected behavior is defined by a *reference model*. A reference model consists of selected features which are compared to new observations. Features can be compared individually or in a combined manner. The combination of features can give context to the state of the observed system. The combination of multiple features to identify entities is called fingerprinting. Fingerprints are one method of building a reference model.

Fingerprinting is performed actively or passively [3]. Active fingerprinting-techniques interact directly with the fingerprinted system to trigger necessary observations. In passive fingerprinting, features are observed without interaction.

Models in anomaly detection can be built by using machine learning methods [2], [4], or using externally provided documentation [5], [6].

Most anomaly detection systems (ADS) use either only cyber or only real-world features [2]. However, using a combination of cyber and physical features for anomaly detection has advantages. Depending on the cause of an anomaly, physical features often indicate deviations earlier than cyber features or vice versa. For example, a malfunctioning device can send back acknowledgments for executed operations even though it did not perform the acknowledged action. Such behavior can not be detected by an ADS that relies only on cyber features. Other physical issues of devices such as abrasion also cannot be detected by cyber-only ADS. For example, Stuxnet [7], in which the monitoring of the attacked system, which relied purely on cyber-only features, would have benefited from additional physical monitoring. A mismatch between physically observed behavior and the monitored cyber-values helps to spot anomalies in the operation of attacked centrifuges.

ADS purely based on physics are not able to detect a loss of control immediately. In case a robot executes a legitimate queue of commands but is not accessible via its interfaces, it will only create an anomaly if it stops operating or executing different commands.

Despite the previously motivated advantages, connecting physical and cyber-features for anomaly detection imposes various challenges. Physical measurements of processes take longer since the measurements are done over some time. The measured signals need to be processed and cleared from noise before they can be used. Finally, a cyber-physical ADS needs to correlate physical measurements with observed digital signals of the ICS.

This paper proposes cyber-physical anomaly detection for ICS. Our approach uses both, network communication and sound measurements to create a reference model of ICS. Observed network traffic is used to confirm if commands have been executed correctly, and to process and filter sound samples of a monitored ICS.

The correlation between measured physical signal and network traffic is used to detect anomalous behavior of single devices in an ICS. As a result, our system is capable of detecting anomalies in which a device executes an operation differently on the physical layer than it was instructed on the cyber-layer. It is capable of detecting attacks and faults in the monitored system.

We assume that services used in ICS environments often follow deterministic patterns. This work extends our previous work on network-based device fingerprinting [8]. The proposed method can confirm if devices have successfully executed the commands as observed control messages on the network layer suggest. Via this approach, our ADS can detect both, attacks and faults. Our contribution is introducing a multi-layer ADS that uses both, physical and cyber-features.

This research was funded by the German Federal Ministry of Economic Affairs and Energy (BMWI) in DECENT (0350024A) and the chaire Cyber CNI, supported by the FEDER development fond of the Brittany region.

978-3-903176-32-4

The rest of the paper is structured as follows. Section II covers related work on anomaly detection, fingerprinting, and sound mapping. Section III gives the necessary background on anomaly detection fingerprinting for cyber and cyber-physical systems and sound classification. Section IV explains the necessity of such a system and shows how it is realized. It also points out the challenges of such an approach. Section V gives an overview of initial evaluations of parts of the proposed system.

II. Related Work

The fields related to our work are anomaly detection, physical fingerprinting techniques in general, and sound detection in particular. Anomaly detection and fingerprinting are well-studied topics over the last decades. Both topics are intertwined since ADS use reference models to detect abnormal behavior. Some systems rely on fingerprints for creating a reference model.

A. Anomaly Detection

ADS use a reference model to classify observations as anomalous or benign. There are two methods to create a reference model for ICS settings. One is the statistical analysis of observations during the operation of a plant. The reference model can also be created via the specification of the system. Statistic-based anomaly detection can use machine learning to create the reference model. [4] gives an overview of machine learning based anomaly detection methods for cyber-physical systems (CPS). The input to the presented modeling approaches are features from various observations that can be made within a CPS. Some approaches [9], [10] directly use observations related to the physical process to create the reference model. [11] use accumulated process logs to derive models for an observed IoT system. Some approaches make use of the observed communication for finding patterns [12], [13]. Specification-based anomaly detection processes existing documentation to create a model. [5], [6] present how documentation can be leveraged to build reference models.

B. Fingerprinting

A fingerprint is created by processing multiple features into a single signature that can then be used for comparison. The fingerprint can be used to uniquely identify a piece of software [14], [15], hardware [16], [17] or process [18]–[20]. Depending on the type of fingerprinting, different features can be used for fingerprint creation. This type influences how a fingerprint can be collected.

Software-based fingerprints such as Browser-Fingerprinting [14] or TLS fingerprinting [15] use features from observation of parameters in single network packets. An example for fingerprints from network communication in ICS is presented in [21].

In hardware-based fingerprinting techniques, features used for creating a fingerprint are observed during the execution of a process by a device. During execution, physical features are recorded and used as input for the fingerprint. Some features, like electromagnetic emission, require expensive hardware to be measured. Others require physical access to devices. [17] demonstrates a passive fingerprinting technique based on command execution-time. In [22], physically unclonable functions are used to create attestations of physical properties, like the temperature of a device. When looking at single devices, it can be feasible to consider the electromagnetic emission during the execution of a command [23], [24]. Other physical features for fingerprinting are the power intake [18], [25], the physical characteristics of communication [26] or sound emission [27]. [19], [20], [28] show that the creation of sound fingerprints for processes in CPS is feasible, and can be used to detect attacks. Sound can be measured by setting up a microphone in proximity while others like the measurement require expensive additional hardware.

C. Sound Classification

The use of sound measurements for fingerprints is closely related to sound classification technology. The biggest challenges in this field are the filtering and enrichment of recordings with further information. An overview of the properties of sound fingerprinting is given in [29]. A large portion of current research focuses on music fingerprinting [30], in which a song should be identified from a short sample [31]. The field of environmental sound classification has not received much attention until 2014. [32] give an overview about challenges for environmental sound classification. [33] argues the feasibility of machine learning methods for environmental sound recognition, [34] presents its successful application. The central challenge in this field is the correct preprocessing of recordings, such that they can be used for fingerprinting.

Each sensing field has its challenges that need to be considered when combining cyber and physical monitoring. ADS built purely on cyber-features fail to detect issues in the physical. Physical measurements are aimed at single devices and are prone to noise. This issue is particularly challenging when dealing with sound samples as there are various external sources of noise. In our proposed anomaly detection scheme, we combine methods from both domains. We create a 2-layer ADS. The feasibility of and advantages of a multi-layer system for CPS are discussed in [35]. However, the description remains vague.

III. Background

In this section we give an overview of techniques and challenges in anomaly detection, fingerprinting, and sound classification. Anomaly detection is concerned with finding patterns that deviate from expected behavior. A comprehensive overview of this topic is given in [2], [36]. To make anomaly detection work, a reference model has to be created to distinguish between normal and abnormal behavior. Models can be created via statistical approaches or by using a system's specification [6], [36]. After a model was built, new data points are classified if they conform to it. A model can enable

context-aware, behavioral or statistical anomaly detection [36]. The classification is done by comparing selected features to the reference model. If the compared feature is not within an expected range or conforms to created rules it is considered anomalous.

One reference model type is a fingerprint. Fingerprinting can be done actively or passively. Active fingerprinting techniques rely on direct interaction between the fingerprinter and the fingerprinted devices to obtain the required features. The interaction with a device for signature creation can have effects on it, influencing the fingerprint in an unwanted way. Especially in ICS environments with low powered devices, additional interaction can have strong effects on fingerprinted devices [17].

Therefore it is desirable to use a passive fingerprinting method in ICS. Passive fingerprinting relies on features that are observed without directly interacting with a device, e.g. parameters in a network packet or emitted sound. Selected features should be robust, unique, and easy to access to be suitable for creating a fingerprint. The robustness is needed to reliably identify similarities. Uniqueness is required for distinguishing occurrences. Features should be easily accessible such that the method can be scaled to be used for many devices. Input for the fingerprint generation are the selected features. Depending on its nature, a feature might need to be preprocessed and cleared of noise before it can be processed. Additionally captured noise in a signal can falsify the resulting fingerprint. To clear noise, different sorts of transformations or filters can be used, depending on the signal. This step especially important for physical measurements. [37] points out the influence noise has on fingerprinting performance. Noise reduces characteristics that separate different signatures from each other. From the preprocessed features a fingerprint is then generated, resulting in a signature of an observation. Similar to anomaly detection, there exist two phases: a model building phase, and a classification phase. In model building, a created signature is stored along with a label in a database. In the classification phase, the signature is compared to the stored signatures. The closest match or no match is returned. Due to the ease of access and scalability, we choose audio for creating a physical fingerprint for this part of our ADS. The captured recordings need to be cleared of background noise. Background noise can be caused by interference on a recording device or other sound sources in proximity. Simple background noise can be removed by using one of the various filters [29]. To remove other sound sources from the input more sophisticated methods are required. We elaborate in Section IV how this is done in our selected environment.

Finally, a recorded sample must be cut such that the beginning and end align with the reference recording. After preparing the recording it can be processed for fingerprint generation. Common techniques as presented [38], [39] can be used for this step.

IV. Approach

In this section, we describe how our approach to perform cyber-physical anomaly detection for ICS. We describe the general structure of our anomaly detection scheme and elaborate on the advantages and challenges of the proposed method.

A. Concept

Similar to other ADS, our approach consists of a model generation phase and a classification phase. The created reference model consists of a mapping between a command observed on the network layer, and a corresponding sound signature on the physical layer.

1) Model Generation Phase:

In the model generation phase, the reference model is created. The input are sound recordings of command executions and network-captures containing the packets used to issue the command. We assume that recording of the executed operation can be performed isolated from background noise. The first step is filtering the recording from background noise. In our scenario, frequencies on the lower spectrum are most unique to each action. Therefore our method applies a low-pass filter. To reduce the amount of data that needs to be processed each recording is down-sampled. It is also cut to such that it only contains the command execution. The resulting data is a background noise-free recording of a device performing a specific operation. Each recording is then analyzed concerning signal energy and occurring frequencies. From this information, a weighted average per frame of the recording is generated. The weighted average per frame, reduced to the 40 most significant frequencies, becomes the fingerprint. This number of frequencies is within in the range used in other related work [40], [41].

From the network capture, the command used to issue the recorded execution is extracted. The fingerprint, extracted command, and preprocessed recording are stored in a model database. The fingerprint along with the extracted command makes up combined cyber-physical fingerprint that identifies an action. This information is stored in a model-database for reference and further filtering in the classification phase. The process of creating a mapping between network communication and sound fingerprint can be seen in Figure 1.

In the model generation phase, the reference for each possible command is generated. The creation of signatures can be done when testing and evaluating a device before it is integrated into the ICS. In case the fingerprinted device interacts with different types of objects, a reference for each type has to be created. This additional mapping has to be created since the execution of the same command might sound different depending on the interaction. For example, a robot picking up a heavy object might sound different from the same robot picking a lightweight object.

2) Classification Phase:

The classification phase confirms that a device in the ICS has correctly executed a command. The input for this phase is a recording of the last n seconds, the corresponding network

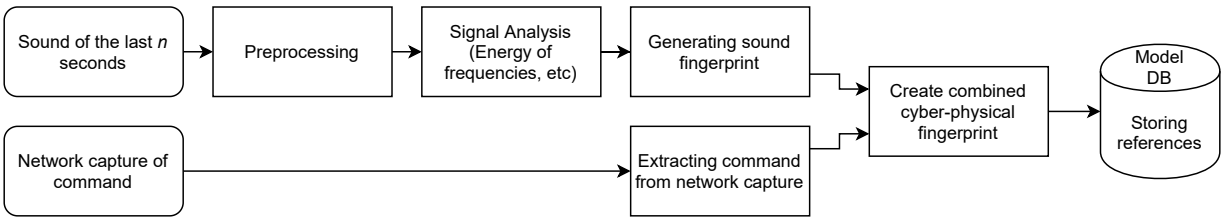


Fig. 1: Steps of the model generation phase

capture, and a synchronized timestamp for the beginning of both inputs. There are two sliding windows, one for each layer. There may be operations that started before the beginning of the recording. However, due to their execution time on a device, sound by previously started operations may be emitted after a recording is started. For identifying and filtering such operations, the sliding window for the network layer needs to be larger than the one for the sound recording. For simplification, we assume the execution of each operation takes up to n seconds. Therefore the length of the network capture in the simplified approach has a length of $2n$ seconds. This assumption holds because actions started at 0 of the network capture are done at ns. This ensures that all sources from a monitored ICS in a recording are known. The length of an action can also be used as an additional feature for detecting anomalies. The described process classifies an action starting at the beginning of the recording. The first step clears the recording of simple background noise. This step applies the same filters used in the model generation phase. Our system extracts issued commands along with a timestamp from the network. The model database provides references for the extracted commands. The process uses the references and timestamps of the commands to remove ICS related background noise from the recording. Therefore, is subtracts reference recordings of the extracted commands from the recording at the corresponding time stamps. This is done by using the inverse of the reference recording and adding it to the source at the specified timestamp. This creates a dynamic filtering method for the sound recording that can be used to selectively filter background noise caused by surrounding devices. All operations that should not be classified are subtracted from the signal. In our example, these are all operations that do not start at the beginning of the recording (0 for the recording, n seconds for the network capture). The remaining sound signal only contains the sound of the operation to be classified. From the remaining signal, the fingerprint is generated the same way as during the model generation. The resulting fingerprint is then used to check if it matches the signature for the extracted command from the network capture. The approach checks if the difference between the generated and the stored reference signature is within a certain threshold. In case the signatures match, the system operates as expected. In case there is no match, either the device itself, any device in proximity of the microphone or the observed network traffic deviate from the reference model. This deviation is then classified as an anomaly regardless of the cause. An illustration of the classification phase can be seen in Figure 2.

B. Advantages and challenges of the proposed approach

Using the presented cyber-physical approach has several advantages. 1) As mentioned in the introduction, such a system can detect anomalies at an earlier stage than systems that solely rely on cyber or physical features. 2) By choosing sound to passively create a fingerprinting approach for the physical layer, the method does not impact the ICS after model creation. 3) Sound is easily accessible. For our initial evaluation, we use a microphone built into a mobile phone to record audio. 4) The system is easy to set up, and 5) the filtering method can be applied to large environments. 6) By combining the observed network traffic with physical observations, the approach can identify anomalies on both layers.

Physical anomalies can be caused by abrasion, malfunctioning devices, or a stealthy attacker [2]. They can be identified by a mismatch of the recording and the corresponding signature in the model database. The correlation of network traffic with sound fingerprinting makes it possible to detect physically broken devices that appear to function correctly on the cyber-layer. In particular, broken devices that send back acknowledgments for received commands can be identified via correlation. A modularized approach using the reference recordings to dynamically filter captured recordings has several advantages. The first advantage is the simple adoption of changes in the ICS. In case a single device in the ICS is replaced¸ it is sufficient to replace the signature/command mapping in the model database. By using the network traffic in combination with observed network traffic, the background noise can be filtered dynamically since the filtering depends on the network traffic. Therefore, the anomaly detection adapts to changes in the operation of the ICS. Further, the proposed method can be seen as an extension to standard network ADS. Due to this, existing systems can be extended and keep using established methods to detect anomalies.

To realize the approach, several challenges need to be tackled. Methods to efficiently reduce the noise of the recordings need to be researched. For simplification, the current proposal assumes that noise only consists of background noise and sounds created by surrounding devices. However, there are other sources of noise. Examples are people on the shop floor or other outside factors. Therefore, the filtering step of the classification phase (Fig. 2) needs to be further improved. Another challenge is the correct evaluation of a recorded sample, especially in presence of similar devices.

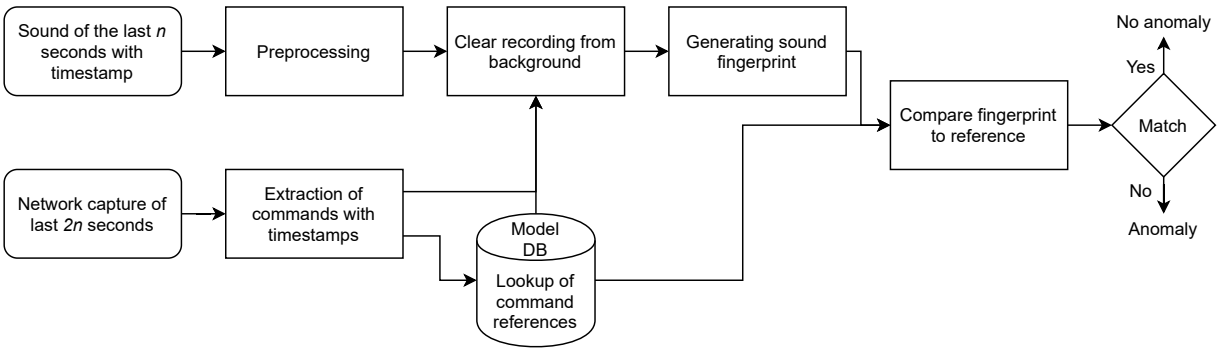
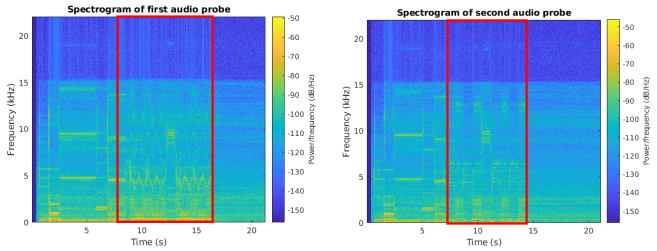


Fig. 2: Steps of the classification phase

At this moment it is unclear how two devices located right next to each other, executing the same command at the same time, can be distinguished. This problem might be solved by the use of stereo or multiple microphones. However, then additional information about a device's position is required. The optimal setup of the microphones throughout and ICS remains a challenge. Finally, our approach is not capable of differentiating attacks from faults.
In the following, we describe the initial evaluation results for classifying commands.

V. Evaluation

The most important step in the proposed approach is the generation of the correct sound fingerprints. The feasibility of fingerprinting whole processes and single devices has been demonstrated by several works mentioned in Section II. Our approach creates fingerprints for processes on single devices that are then dynamically combined during the classification phase.
For an initial test, we generate fingerprints for different movements of a 3D printer. We consider this as a mini-factory with just a single device that can perform different operations. The only source of noise in this setup is the fan on the device itself. The fan-speed can be adjusted to simulate noise.
We record different operations of the printer to distinguish them, and to create a fingerprint. For simplicity, each recording has a length of 20 seconds. Figure 3 shows a comparison of recordings when executing two different operations before filtering. Figure 3a shows the spectrogram of printing in a circle motion while Figure 3b shows printing in a square. The spectrograms show differences in the signature of the movements. The differences are marked in red. In Figure 3a a wave form can be identified after 8 seconds which is missing in Figure 3b.
The spectrogram shows which frequencies carry the most energy. This gives an insight into which frequencies can be used for defining a fingerprint or can be filtered. The generated signature from the signal is an array of 1700 floats. These are further reduced to the most significant 40 values in the sound fingerprint generation step as described in Section IV. Taking the recordings as input for the fingerprinting process it can be seen that the generated signatures differ. The generated fingerprint is then compared to signatures in the database by



(a) Spectrogram of printing a circle (b) Spectrogram of printing a square

Fig. 3: Spectrograms of a circle motion (left) and square motion (right)

calculating the Euclidean distance to each recorded signature. The sound is then identified as the closest signature in the database. Based on the sampling rate and quality of the recording, more features can be extracted for creating a fingerprint. In case multiple stereo microphones are present, the position of a device can also be identified.
In the future, we plan to develop, evaluate and validate our proposed framework in a real ICS testbed [42], especially considering additional sources of background-noise.

VI. Conclusion

We proposed a method for cyber-physical anomaly detection for ICS by leveraging observed network traffic and sound measurements to detect anomalies. These are used as input to build a reference model for anomaly detection. Thus the proposed system (Section IV) combines advantages of physical and cyber-only ADS. Since ICS often consist of low-resource devices we chose a passive fingerprinting technique. The correlation of network traffic and sound enables a dynamic adaption of the anomaly detection scheme to the operation of a system. It allows to dynamically filter noise from recordings that are used for anomaly detection. Our approach is applicable in environments in which multiple devices emit sound, for example, the shop floor of a factory. We evaluated initial findings for distinguishing operations of single devices in a small scale environment. We plan to extend the approach to a real-world ICS testbed and improve the dynamic filtering capabilities.

REFERENCES

[1] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ics) security," *NIST special publication*, vol. 800, no. 82, pp. 16–16, 2011.

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, pp. 1–58, 2009.

[3] D. Zanetti, S. Capkun, and B. Danev, "Types and origins of fingerprints," in *Digital Fingerprinting*. Springer, 2016, pp. 5–29.

[4] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *arXiv preprint arXiv:2003.13213*, 2020.

[5] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, "Specification-based anomaly detection: a new approach for detecting network intrusions," in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 265–274.

[6] M. Caselli, E. Zambon, J. Amann, R. Sommer, and F. Kargl, "Specification mining for intrusion detection in networked control systems," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016, pp. 791–806.

[7] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[8] M.-O. Pahl and F.-X. Aubet, "All eyes on you: Distributed multi-dimensional iot microservice anomaly detection," in *2018 14th International Conference on Network and Service Management (CNSM)*. IEEE, 2018, pp. 72–80.

[9] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[10] W. Aoudi, M. Iturbe, and M. Almgren, "Truth will out: Departure-based process-level detection of stealthy attacks on control systems," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 817–831.

[11] Q. Wang, W. U. Hassan, A. Bates, and C. Gunter, "Fear and logging in the internet of things," in *Network and Distributed Systems Symposium*, 2018.

[12] M.-K. Yoon and G. F. Ciocarlie, "Communication pattern monitoring: Improving the utility of anomaly detection for industrial control systems," in *NDSS Workshop on Security of Emerging Networking Technologies*, 2014.

[13] S. J. Saidi, A. M. Mandalari, R. Kolcun, H. Haddadi, D. J. Dubois, D. Choffnes, G. Smaragdakis, and A. Feldmann, "A haystack full of needles: Scalable detection of iot devices in the wild," in *Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 87–100.

[14] K. Boda, Á. M. Földes, G. G. Gulyás, and S. Imre, "User tracking on the web via cross-browser fingerprinting," in *Nordic conference on secure it systems*. Springer, 2011, pp. 31–46.

[15] M. Husák, M. Čermák, T. Jirsík, and P. Čeleda, "Https traffic analysis and client identification using passive ssl/tls fingerprinting," *EURASIP Journal on Information Security*, vol. 2016, no. 1, p. 6, 2016.

[16] S. Aneja, N. Aneja, and M. S. Islam, "Iot device fingerprint using deep learning," in *2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS)*. IEEE, 2018, pp. 174–179.

[17] D. Formby, P. Srinivasan, A. M. Leonard, J. D. Rogers, and R. A. Beyah, "Who's in control of your control system? device fingerprinting for cyber-physical systems." in *NDSS*, 2016.

[18] S. Wei, A. Aysu, M. Orshansky, A. Gerstlauer, and M. Tiwari, "Using power-anomalies to counter evasive micro-architectural attacks in embedded systems." in *HOST*, 2019, pp. 111–120.

[19] C. M. Ahmed, A. P. Mathur, and M. Ochoa, "Noisense print: detecting data integrity attacks on sensor measurements using hardware-based fingerprints," *ACM Transactions on Privacy and Security (TOPS)*, vol. 24, no. 1, pp. 1–35, 2020.

[20] C. M. Ahmed, M. Ochoa, J. Zhou, A. P. Mathur, R. Qadeer, C. Murguia, and J. Ruths, "Noiseprint: Attack detection using sensor and process noise fingerprint in cyber physical systems," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, 2018, pp. 483–497.

[21] M. Caselli, D. Hadžiosmanović, E. Zambon, and F. Kargl, "On the feasibility of device fingerprinting in industrial control systems," in *International Workshop on Critical Information Infrastructures Security*. Springer, 2013, pp. 155–166.

[22] U. Rührmair, J. Martinez-Hurtado, X. Xu, C. Kraeh, C. Hilgers, D. Kononchuk, J. J. Finley, and W. P. Burleson, "Virtual proofs of reality and their physical implementation," in *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 70–85.

[23] Y. Cheng, X. Ji, J. Zhang, W. Xu, and Y.-C. Chen, "Demicpu: Device fingerprinting with magnetic signals radiated by cpu," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1149–1170.

[24] N. Sehatbakhsh, M. Alam, A. Nazari, A. Zajic, and M. Prvulovic, "Syndrome: Spectral analysis for anomaly detection on medical iot and embedded devices," in *2018 IEEE international symposium on hardware oriented security and trust (HOST)*. IEEE, 2018, pp. 1–8.

[25] J. H. Reed and C. R. A. Gonzalez, "Enhancing smart grid cyber security using power fingerprinting: Integrity assessment and intrusion detection," in *2012 Future of Instrumentation International Workshop (FIIW) Proceedings*. IEEE, 2012, pp. 1–3.

[26] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 787–800.

[27] G. Baldini and I. Amerini, "Smartphones identification through the built-in microphones with convolutional neural network," *IEEE Access*, vol. 7, pp. 158 685–158 696, 2019.

[28] C. M. Ahmed, J. Zhou, and A. P. Mathur, "Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in cps," in *Proceedings of the 34th Annual Computer Security Applications Conference*, 2018, pp. 566–581.

[29] P. Cano, E. Batlle, T. Kalker, and J. Haitsma, "A review of audio fingerprinting," *Journal of VLSI signal processing systems for signal, image and video technology*, vol. 41, no. 3, pp. 271–284, 2005.

[30] R. Typke, F. Wiering, and R. C. Veltkamp, "A survey of music information retrieval systems," in *Proc. 6th international conference on music information retrieval*. Queen Mary, University of London, 2005, pp. 153–160.

[31] A. Wang, "The shazam music recognition service," *Communications of the ACM*, vol. 49, no. 8, pp. 44–48, 2006.

[32] S. Chachada and C.-C. J. Kuo, "Environmental sound recognition: A survey," *APSIPA Transactions on Signal and Information Processing*, vol. 3, 2014.

[33] K. J. Piczak, "Environmental sound classification with convolutional neural networks," in *2015 IEEE 25th International Workshop on Machine Learning for Signal Processing (MLSP)*. IEEE, 2015, pp. 1–6.

[34] J. Salamon and J. P. Bello, "Deep convolutional neural networks and data augmentation for environmental sound classification," *IEEE Signal Processing Letters*, vol. 24, no. 3, pp. 279–283, 2017.

[35] D. Stock and D. Schel, "Cyber-physical production system fingerprinting," *Procedia CIRP*, vol. 81, pp. 393–398, 2019.

[36] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *computers & security*, vol. 28, no. 1-2, pp. 18–28, 2009.

[37] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan, and T. W. Rondeau, "Radio transmitter fingerprinting: A steady state frequency domain approach," in *2008 IEEE 68th Vehicular Technology Conference*. IEEE, 2008, pp. 1–5.

[38] J. S. Seo, M. Jin, S. Lee, D. Jang, S. Lee, and C. D. Yoo, "Audio fingerprinting based on normalized spectral subband centroids," in *Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.*, vol. 3. IEEE, 2005, pp. iii–213.

[39] M. D. Kamaladas and M. M. Dialin, "Fingerprint extraction of audio signal using wavelet transform," in *2013 International Conference on Signal Processing, Image Processing & Pattern Recognition*. IEEE, 2013, pp. 308–312.

[40] J. Haitsma and T. Kalker, "A highly robust audio fingerprinting system." in *Ismir*, vol. 2002, 2002, pp. 107–115.

[41] S. Belikovetsky, Y. A. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici, "Digital audio signature for 3d printing integrity," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1127–1141, 2018.

[42] M.-O. Pahl, A. Kabil, E. Bourget, M. Gay, and P.-E. Brun, "A mixed-interaction critical infrastructure honeypot," *European Cyber Week CAESAR, 2020, Rennes, France*, 2020.