SpecForce: A Framework to Secure IoT Spectrum Sensors in the Internet of Battlefield Things

Article *in* IEEE Communications Magazine · October 2022

DOI: 10.1109/MCOM.001.2200349

CITATIONS
5

READS
126

5 authors, including:

Pedro Miguel Sánchez Sánchez
University of Murcia
55 PUBLICATIONS **411** CITATIONS
SEE PROFILE

Alberto Huertas
University of Zurich
143 PUBLICATIONS **1,363** CITATIONS
SEE PROFILE

Gregorio Martinez Perez
University of Murcia
339 PUBLICATIONS **3,960** CITATIONS
SEE PROFILE

Burkhard Stiller
University of Zurich UZH
631 PUBLICATIONS **5,813** CITATIONS
SEE PROFILE

SpecForce: A Framework to Secure IoT Spectrum Sensors in the Internet of Battlefield Things

Pedro Miguel Sánchez Sánchez[1], Alberto Huertas Celdrán[*2], Gérôme Bovet[3], Gregorio Martínez Pérez[1], Burkhard Stiller[2]

***Abstract*—The battlefield has evolved into a mobile and dynamic scenario where soldiers and heterogeneous military equipment exchange information in real-time and wirelessly. This fact brings to reality the Internet of Battlefield Things (IoBT). Wireless communications are key enablers for the IoBT, and their management is critical due to the spectrum scarcity and the increasing number of IoBT devices. In this sense, IoBT spectrum sensors are deployed on the battlefield to monitor the frequency spectrum, transmit over unoccupied bands, intercept enemy transmissions, or decode valuable information. However, IoBT spectrum sensors are vulnerable to heterogeneous cyber-attacks, and their accurate detection is an open challenge in the literature. Thus, this paper presents SpecForce, a security framework for IoBT spectrum sensors based on device behavioral fingerprinting and ML/DL techniques. SpecForce considers heterogeneous data sources to detect the most dangerous and recent cyber-attacks affecting IoBT spectrum sensors, such as impersonation, malware, and spectrum sensing data falsification attacks. To evaluate the SpecForce detection performance, it has been deployed on 25 real spectrum sensors, and results show almost perfect detection for the three cyber-attack families previously mentioned.**

***Index Terms*—IoT, Battlefield, Spectrum Monitoring, Fingerprinting, Cybersecurity, Identification.**

I. Introduction

TODAY'S battlefield and military operations are highly dependent on wireless communication technologies. Aircraft, warships, vehicles, weapons, and soldiers are equipped with connectivity capabilities to send and receive confidential information enabling successful offensive and defensive tactics. These deployments make up the so-called Internet of Battlefield Things (IoBT) [1], which combines the Internet of Things (IoT) characteristics with the requirements of military scenarios where properties such as security, privacy, and availability are even more critical than in civil scenarios. The dynamism of the IoBT, where troops, vehicles, and military equipment are constantly moving, requires wireless communications [2]. Here, Cognitive Radio Networks (CRN) [3] play a key role, endowing communications with programmability and high mobility in terms of used frequencies. Therefore, CRN should manage the radio frequency (RF) spectrum securely and adequately to select unoccupied frequency bands, establish secure transmissions, intercept enemy messages, and decode valuable information. In the IoBT, one of the most common approaches to enforce the previous tasks is to deploy resource-constrained spectrum sensors able to monitor and decode transmissions in different radio bands [4]. These sensors have numerous advantages, such as portability, accuracy, simplicity, and reduced cost, but they are vulnerable to cyber-attacks.

In the modern battlefield, cyberwar and cyber-attacks are common hostile acts aiming to penetrate strategic targets such as enemy communications, area defense, or critical infrastructures [5]. In this context, IoBT spectrum sensors are perfect targets due to their computational and storage constraints to maintain updated software and deploy cybersecurity mechanisms. Looking at cyber-attacks affecting IoT spectrum sensors, they can be categorized into three main families: *(i) identity-focused attacks*, whose goal is to impersonate legitimate IoBT spectrum sensors by deploying malicious ones with the same hardware and software configuration to extract sensitive military information and perform malicious activities; *(ii) vulnerability-based attacks*, where typical threats such as malware are encompassed to disrupt military services, steal battlefield information, or initiate attacks to other military targets; and *(iii) Spectrum Sensing Data Falsification (SSDF) attacks*, aiming to modify spectrum data reported by sensors to hide illegal transmissions, provoke interference and collisions, or create fictitious transmissions persuading enemies communication.

In the IoBT, the detection of the previous cyber-attack families has been tackled separately by the literature. Most works analyze software operations to detect malware and exploit vulnerabilities in generic IoT devices deployed in military scenarios [6]. However, only a few solutions deal with SSDF attacks detection in IoBT cognitive radio networks [7], and identification of IoBT devices [8]. Besides, outside the battlefield scenario, the previous three cyber-attack families have been covered in a wider manner [9] since they also affect other critical scenarios such as Industrial IoT or network management. In summary, and as can be seen in TABLE I, the main limitation in the IoBT is that solutions detecting malware are not able to detect SSDF and spoofing attacks, and solutions detecting SSDF are useless for malware detection and identical device identification. Therefore, the main focus of this work is to explore novel approaches to detect all the previous attack families when they occur in IoBT spectrum sensors. One of the most promising and recent approaches to improve this situation

*Corresponding author.
[1]Pedro Miguel Sánchez Sánchez and Gregorio Martínez Pérez are with the Department of Information and Communications Engineering, University of Murcia, 30100 Murcia, Spain (pedromiguel.sanchez@um.es; gregorio@um.es).
[2]Alberto Huertas Celdrán and Burkhard Stiller are with the Communication Systems Group (CSG) at the Department of Informatics (IfI), University of Zurich UZH, 8050 Zürich, Switzerland (huertas@ifi.uzh.ch; stiller@ifi.uzh.ch).
[3]Gérôme Bovet is with the Cyber-Defence Campus within armasuisse Science & Technology, 3602 Thun, Switzerland (gerome.bovet@armasuisse.ch).

is to combine device behavioral fingerprinting with Machine and Deep Learning (ML/DL) techniques [10]. In this context, different data sources, such as system calls, logs, hardware events, or clock skew, can be leveraged to characterize the *normal* behavior of spectrum sensors and detect anomalies or classify the three main cyber-attack families detailed before.

TABLE I: Related Work Comparison.

Work	Scenario	Device type	Attack	Approach
[7]	IoBT	Spectrum Sensors	SSDF	Blockchain
[8]	IoBT	Generic	Generic security and trust	Blockchain
[9]	Generic	Computers	Identity	Hardware fingerprinting
This work	IoBT	Spectrum Sensors	Identity, Malware, SSDF	Behavior analysis + ML/DL

However, despite the achievements of existing work dealing with cybersecurity in the IoBT, and more specifically in IoBT spectrum sensors, there are still several open challenges that require further research efforts. Among the main ones, the following ones are highlighted: *(i)* there is no definition of the threat model that IoBT spectrum sensors face, as previous solutions have analyzed their threats in a separated manner; *(ii)* data sources and events accurately detecting normal and heterogeneous under-attack behaviors of IoBT spectrum sensors have not been investigated; *(iii)* as TABLE I shows, there is no global solution detecting both system- and data-oriented cyber-attacks while evaluating the resource consumption in IoBT spectrum sensors.

In order to improve the previous challenges, the main contributions of this work include:

- The creation of a scenario where 25 real IoBT spectrum sensors are employed for radio transmission monitoring and decoding. In such a scenario, the threat model faced by these sensors is defined, and 18 heterogeneous cyber-attacks related to the thread model are considered to infect the IoBT spectrum sensors.
- The design and implementation of SpecForce, a security framework for IoBT spectrum sensors that combines device behavioral fingerprinting and ML/DL techniques. The implementation of SpecForce includes the analysis of the most suitable behavioral data sources and the ML/DL techniques for the defined threat model.
- The validation of SpecForce while detecting the cyber-attacks considered in the proposed scenario for *(i)* identity-based attacks, achieving an average 91.92% True Positive Rate (TPR); *(ii)* heterogeneous malware detection, achieving ≈90% TPR and 96% True Negative Rate (TNR); and *(iii)* SSDF attack detection, achieving 96-99% TNR and 92-100% TPR, depending on the attack.

II. Cybersecurity Threats of IoBT Spectrum Sensors

This work presents a scenario composed of 25 IoBT spectrum sensors based on Raspberry Pi (RPi) devices belonging to the ElectroSense platform [11] and deployed in different locations between Switzerland and Spain. The sensors are randomly deployed in the field since their location does not affect the framework performance (spectrum data is not leveraged for cyber-attack detection). Ten of these sensors are Raspberry Pi 3 Model B+ and 15 are Raspberry Pi 4 Model B. Each sensor is equipped with an RTL-SDR (RealTek Low cost - Software Defined Radio) USB kit and proper software to scan the RF spectrum (from 20 MHz to 1.6 GHz). Such functionality allows these sensors to monitor and decode heterogeneous wireless communications occurring between military equipment such as base stations, convoys, aircraft, helicopters, or satellites. The upper part of Fig. 1 gives a simplified representation of the military equipment that can be found in the IoBT.

Despite the benefits of IoBT devices, they present some cybersecurity issues and vulnerabilities that have been already identified in [12]. In addition, some other cybersecurity issues related to spectrum sensing and hardware/software aspects of IoBT spectrum sensors need to be analyzed more in detail. In this sense, TABLE II summarizes the main threats identified after analyzing the vulnerabilities of the sensors considered in the proposed scenario. This table also provides a description and attack classification per threat.

Once the threats affecting IoBT spectrum sensors are identified, several representative and recent attack vectors per family are selected to infect the sensors. Details regarding each attack vector behavior are provided below.

- *Identity-focused*. This type of cyber-attack impersonates legit IoT spectrum sensors to steal data or execute malicious actions. For that, it utilizes identical hardware and software configurations to legit IoBT spectrum sensors [13].
- *Malware*. This type of malicious software causes harm to IoBT spectrum sensors by performing diverse malicious actions. From each malware type, different vector samples are executed in each sensor.
  - *Rootkit*. Allow a malicious entity to gain remote control over IoBT spectrum sensors while providing self-hiding capabilities. The samples selected for testing are Beurk, Diamorphine, and Bdvl.
  - *Botnet*. Generate a network of infected IoBT spectrum sensors to perform malicious activities, such as denial of service, in a coordinated manner. The samples selected are Bashlite and Mirai.
  - *Backdoor*. Provide malicious actors with unintended IoBT spectrum sensor access and control. The samples selected for the present work are HttpBackdoor, Python Backdoor, and TheTick.
  - *Ransomware*. Encrypt sensitive files and asks for economical ransoms for data recovery. Ransomware_PoC is the sample selected for this malware family.
- *SSDF*. This type of cyber-attack tampers the data scanned by IoBT spectrum sensors to disrupt the spectrum optimization, monitoring, and decoding services. The following SSDF attacks are executed after manipulating the ElectroSense source code [11]. The implementation details of each attack can be found in [14].
  - *Noise*. Add random noise to the spectrum data.

TABLE II: IoBT Spectrum Sensor Threat Model

Threat	Description	Attack		
		Identity	Malware	SSDF
Data Disclosure	Publish or access sensitive information sensed or maintained by IoBT spectrum sensors.	✗	✓	✓
Spoofing	Replace legitimate spectrum sensors with malicious devices using the same identity. Usually, it is the starting point for further cyber-attacks like data injection.	✓	✗	✗
Sybil	Send a lot of fake data with many different IoBT sensors identities to alter the decisions generated by the IoBT platform.	✓	✗	✗
Jamming	Generate fake or repeated wireless signals to interrupt ongoing communications between legitimate sensors and the IoBT platform or disturb the collected data.	✗	✗	✓
Denial of Service (DoS)	Exhaust or degrade resources of the IoBT platform or spectrum sensors. It can affect at network level or directly at application level. Many devices can be coordinated to increase the impact of the attack, resulting in a Distributed DoS (DDoS).	✓	✗	✓
Advanced Persistent Threat (APT)	Launch sophisticated, continuous, and targeted attacks over the IoBT platform or its spectrum sensors for a large time period.	✓	✓	✗
Data Poisoning	Modify spectrum data monitored by IoBT sensors. It leads to wrong decisions while optimizing spectrum occupancy or decoding transmissions. Two variants are differentiated: Availability Attack and Targeted Attack.	✗	✗	✓
Smart Attacks	Use of machine learning techniques and security analysis devices to gather insights about the IoBT platform defense countermeasures and attack it.	✓	✓	✗

- *Spoof*. Copy the spectrum data of one RF band into another band and add random noise.
- *Repeat*. Replicate the same spectrum data in all affected RF bands.
- *Confusion*. Swap the spectrum data between affected RF bands.
- *Mimic*. Copy the spectrum data of one RF band into another one.
- *Delay*. Sense different outdated spectrum data of affected RF bands.
- *Freeze*. Sense the same outdated spectrum data in affected RF bands.
- *Hop*. Add noise to random parts of affected segments.

Analyzing the different threats and cyber-attacks affecting the IoBT spectrum sensors proposed in the scenario, there is a clear need for solutions proving cybersecurity in a unified and homogeneous fashion.

III. SpecForce Framework

The SpecForce framework covers the previous limitations by combining device behavioral fingerprinting with ML/DL to detect heterogeneous cyber-attacks affecting IoBT spectrum sensors. In particular, the main objectives of SpecForce are to *(a)* identify malicious spectrum sensors, *(b)* detect heterogeneous malware, and *(c)* detect SSDF attacks manipulating spectrum data. To achieve these goals, SpecForce can be deployed in a hybrid way, where IoBT sensors host the behavior monitoring functionality and the server focuses on ML/DL-based detection. Additionally, all framework components can be deployed on the IoBT sensors.

Fig. 1 shows the four main modules making up SpecForce. From an up-down prism, the *Data Gathering* module hosts three components able to periodically monitor the sensor behavior from different perspectives. These perspectives have been selected with the goal of covering the internal behavior of the IoBT in a broad fashion in terms of device components, events granularity level, and complexity. In particular, the *Kernel Software Events* component monitors activity from resources

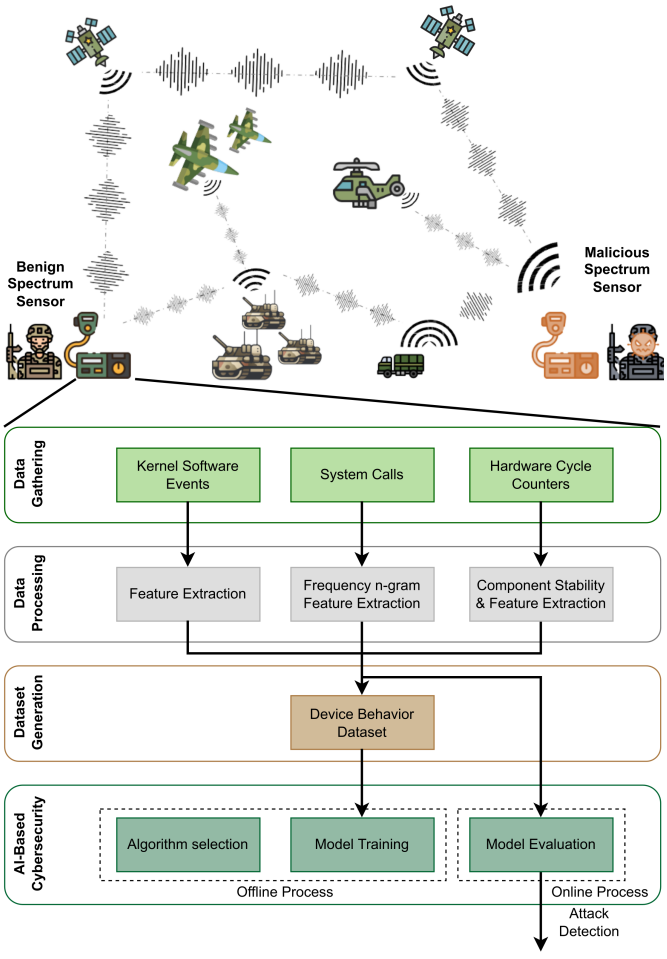

Fig. 1: SpecForce Architectural Design and IoBT Scenario

such as CPU, memory, network interfaces, or file system, among others. The *System Calls* component gathers the system calls performed by the processes of the sensor scanning the spectrum. Finally, the *Hardware Cycle Counters* component focuses on hardware manufacturing variations by monitoring

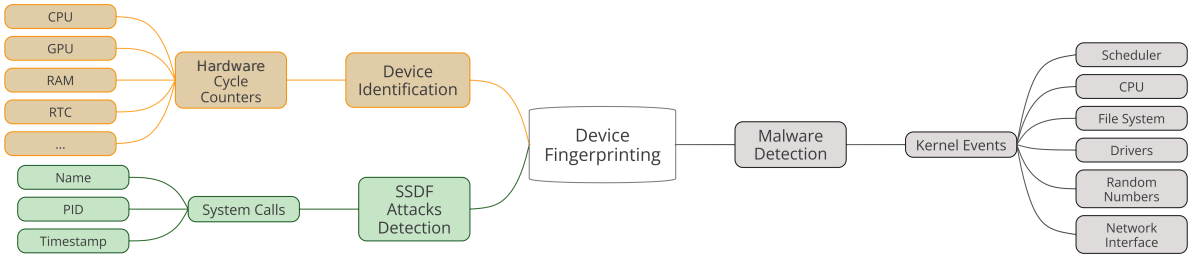

Fig. 2: Collected Data Sources for Device Behavior Fingerprinting.

the cycle counters of different hardware components. Fig. 2 shows the data sources collected by each component to detect the cyber-attacks indicated in Section II.

The Data Gathering module periodically sends the collected raw data to the *Data Processing* module, which is in charge of extracting valuable information and creating feature vectors with them. This module contains three different components with suitable feature extraction techniques for each data source type. As an example of their functionality, *(i)* highly correlated features are filtered for kernel software events, *(ii)* different sequence and frequency (n-gram) features are calculated from raw system calls, *(iii)* and window-based statistical features are extracted from hardware cycle counters. After that, the *Dataset Generation module* compiles all feature vectors generated by the previous module, generating datasets with the sensor behavioral data. Finally, the *AI-based Cybersecurity module* trains and evaluates supervised and unsupervised ML-based models identifying devices and cyber-attacks. For that, *Offline* and *Online* processes are considered. First, the *Offline process* selects suitable ML/DL algorithms and trains them with the created datasets. It generates the ML/DL models used by the framework. Secondly, the *Online* one evaluates the current device behavior using the trained ML/DL models to detect cyber-attacks.

IV. SpecForce Implementation and Results

To analyze the performance of SpecForce, it has been deployed on the 25 IoBT spectrum sensors of the scenario described in Section II. Then, the following three use cases have been analyzed: *(i)* device identification to avoid spoofing attacks, *(ii)* detection of heterogeneous malware, and *(iii)* detection of SSDF attacks.

A. Identity-focused Attack

This use case focuses on chip imperfections affecting the hardware performance of IoBT spectrum sensors, which allow the generation of unique fingerprints per sensor to detect device spoofing attacks. Ideally, different physical oscillators should be used to analyze these imperfections, but Raspberries Pi acting as sensors only contain one oscillator used by all hardware as base frequency. Therefore, this work leverages the imperfections in circuits employed to multiply the base oscillator frequency for the device CPU and GPU separately.

After analyzing the hardware components, the *Hardware Cycle Counter* component of SpecForce monitors the data sources indicated in Fig. 2 for device identification. Then, it measures the skew between the CPU and the GPU cycle counters. To obtain stable fingerprints, different functions are executed on the CPU while the GPU cycle counter is monitored. Concretely, the functions selected are: *(i)* sleep during 120 seconds, *(ii)* hash calculation of a string, and *(iii)* random number generation. To have stability in these values, process isolation measures are taken in the sensor to avoid kernel interruptions from other processes while the functions are running. TABLE III contains the details about the data gathering, data processing and evaluation steps of this use case. In total, a dataset with 10 fingerprints per device is generated (8 for training and 2 for testing). To identify the different IoBT spectrum sensors, the *AI-Based Cybersecurity* module employs ML/DL classification algorithms since the number of sensors in the scenario is constant. Once trained and evaluated, the average TPR of each model is 71.40% for k-NN, 89.65% for SVM, 91.92% for XGBoost, 86.47% for DT, 91.64% for RF, and 85.32% for MLP. As can be appreciated, RF and XGBoost are the best performing models, with +91% TPR. To identify those IoBT spectrum sensors having more and less similarity, Fig. 3 shows the XGBoost confusion matrix for the fingerprints used during testing. The results show how using a 50% TPR threshold, all IoBT spectrum sensors can be perfectly identified. Besides, XGBoost shows that the most important features to perform the identification are the median and average values of the 120 second sleep function.

This use case has demonstrated that SpecForce is able to uniquely identify 25 IoBT spectrum sensors by leveraging hardware manufacturing imperfections and ML classification techniques. In other words, SpecForce solves the issue of identity-focused attacks, as new or duplicated devices would be recognized before they can cause further harm.

B. Malware Detection

This second use case deals with the detection of heterogeneous malware. As starting point, a literature review is performed to study the data sources available in Raspberry Pis and the behavior of well-known malware. Due to the activity of running malware, the internal behavior of a device changes. This behavior can be reflected from several perspectives, such as syscalls, running processes or kernel events. In this sense, some known malware samples include evasion techniques that hide the malicious processes and syscalls. However, lower-level sources such as kernel events are harder to modify [10].

As output of such review, the SpecForce *Data Gathering* module is implemented to monitor in a periodic manner

TABLE III: Technical Details of the Use Cases Implementation.

	Data Gathering			Data Processing		Dataset Generation	AI-Based Cybersecurity	
Use Case	**Source**	**Freq.**	**Resources**	**Technique**	**Feature Vector**	**Dataset**	**Approach: Algorithms**	**Results**
Identity-focused Attack	CPU/GPU Cycle Counters	≈120 s	1 CPU Core	Sliding window (100 values)	18 features: Average time, standard deviation, minimum, maximum, or mode of selected functions	10 fingerprints per device, 300 vectors per fingerprint	Classification: k-NN, SVM, XGBoost, DT, RF, MLP	91.92% avg. F1-Score
Malware Detection	Kernel Events	5 s	1-4% CPU, 6.14MB RAM	Nothing	≈ 80 features: CPU, RAM, file system, drivers, and network events	6 hours per behavior, ≈2160 vectors per behavior	Anomaly Detection: Autoencoder, IF, COPOD, LOF, OC-SVM	+97% TNR, +97% TPR
SSDF Attack Detection	System Calls	60 s	20.2-30% CPU, 6.5MB RAM	Bag-of-Words 1-gram	17 features: number of repetitions per minute of each syscall	6 hours per behavior, 360 samples per behavior	Anomaly Detection: Autoencoder, IF, COPOD, LOF, OC-SVM	+99% TNR, +92% TPR

k-NN: k-Nearest Neighbors, SVM: Support Vector Machine, XGBoost, DT: Decision Tree, RF: Random Forest, and MLP: Multi-Layer Perceptron
IF: Isolation Forest, COPOD: Copula-Based Outlier Detection, LOF: Local Outlier Factor, OC-SVM: One-Class Support Vector Machine

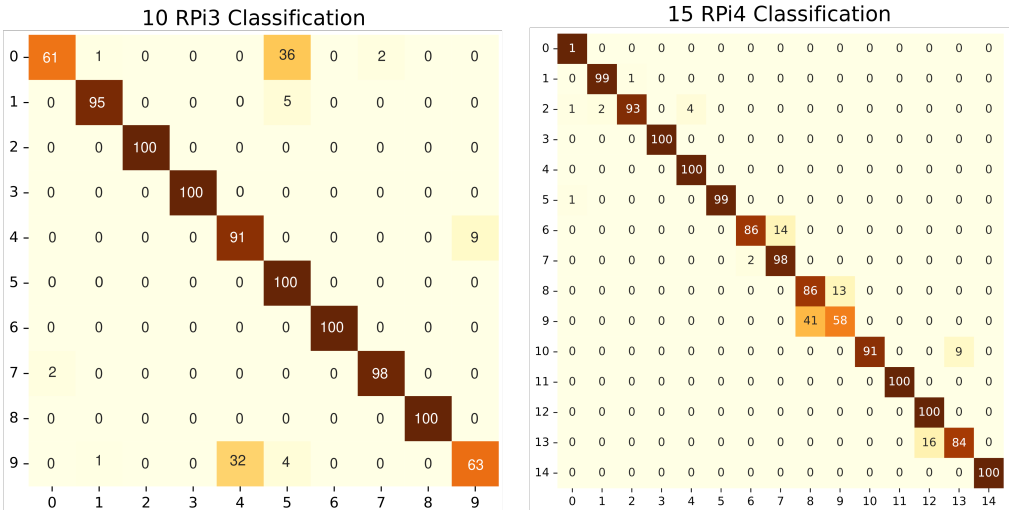

Fig. 3: Confusion Matrices (in percentages) for Device Identification using XGBoost

about 80 kernel events belonging to the usage of resources, hardware, and software activities produced in the IoBT sensors. Fig. 2 shows the event families selected for malware detection. After that, one dataset with ”normal” behavior of each IoBT spectrum sensor is collected for six hours. Then, the rootkits (Beurk, Diamorphine, and Bdvl), botnets (Mirai and Bashlite), backdoors (HttpBackdoor, Python Backdoor, and TheTick), and ransomware (Ransomware_PoC) mentioned in Section II are executed in each IoBT spectrum sensor. Later, all malware samples are monitored for six hours while running in a passive way (without harmful actions being made) and some of them (backdoors and ransomware) performing command execution or data leakage. Anomaly detection is performed because usually attack behaviors are unknown. Therefore, deviations in the normal device behavior can allow detecting attacks not seen during training or zero-day attacks, which are novel attacks leveraging an unknown vulnerability. 80% of the normal data is employed for algorithm training, and the remaining 20% and the malware behavior for testing. TABLE III shows the implementation and experimentation details of this use case.

Fig. 4 shows the detection performance of OC-SVM, the best model. Normal sensor behavior should be evaluated as “Normal” (in the X axis), and the rest of the attack behaviors should be evaluated as “Abnormal”. Therefore, the higher the values in that case, the better the framework works. More than 95% of samples belonging to the different normal behaviors are correctly detected as ”Normal.” Looking at the rootkits, the passive and innocuous behavior of Diamorphine is not detected, but when it establishes an SSH connection every five seconds (Diamorphine5S), it is identified as malicious. In the case of passive behavior of Bdvl, it is detected only half of the time. In terms of Backdoors, the samples belonging to Data Leak behavior executed by TheTick are detected correctly. Similarly, it is important to highlight that the rest of the malicious behaviors are detected in an almost perfect fashion.

This use case has demonstrated the capabilities of SpecForce to detect malicious activities performed by different malware affecting resource-constrained IoBT spectrum sensors. Using software kernel events and anomaly detection techniques, it is possible to characterize the behavior of the IoBT spectrum sensors and detect heterogeneous malware when they are in active and harmful mode.

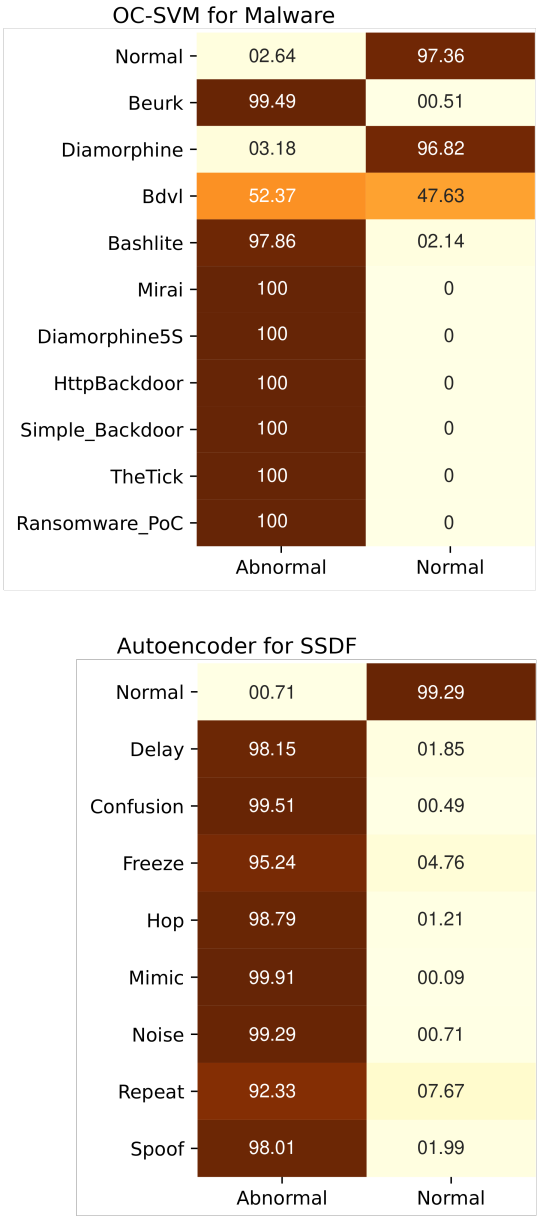

Fig. 4: Confusion Matrices (in percentages) for Malware and SSDF Attacks

C. SSDF Attacks Detection

The last use case focuses on detecting attacks affecting spectrum data. As in the previous ones, a literature review is conducted to identify and select behavioral data sources and events of IoBT spectrum sensors characterizing the activity of the spectrum scanning processes affected by SSDF attacks [15]. As these attacks are based on the modification of a legitimate process, the *system calls* generated by the software are features able to reflect the variations in normal activities.

The result of this step highlighted the suitability of *system calls* to perform such task in a precise way. Therefore, the SpecForce *Data Gathering* module uses *perf* to collect the system calls generated by a given set of processes scanning the spectrum (see Fig. 2 for SSDF attacks detection). Once the data source is selected, the different normal and SSDF attack behaviors are monitored for ≈6 hours. The system calls are then processed to generate a feature vector modeling the activities of the IoBT spectrum sensing process. Then, the *AI-Based Cybersecurity* module selects, trains, and evaluates anomaly detection algorithms. TABLE III gives the technical details of this use case experimentation.

Fig. 4 shows the Autoencoder True Negative Rate (TNR) for normal behavior and the TPR of the different SSDF attacks when modifying 20 MHz of the 1.6 GHz collected spectrum band. It can be seen how the normal behavior is recognized with high performance, showing +99% TNR. Besides, all SSDF attacks are detected with a +92% TPR.

This use case has demonstrated that SpecForce is able to successfully detect the different SSDF attacks executed in IoBT spectrum sensors with a low resource consumption. In particular, system calls have shown a precise characterization of the spectrum scanning process. Furthermore, when they are combined with ML/DL-based anomaly detection techniques, it is possible to detect heterogeneous SSDF attacks.

V. Conclusions

This work presents SpecForce, a framework combining behavior fingerprinting and ML/DL techniques to detect heterogeneous cyber-attacks affecting IoBT spectrum sensors. SpecForce has been deployed in a realistic battlefield scenario composed of 25 IoBT spectrum sensors based on Raspberry Pi. In such a scenario, first, the cybersecurity threats affecting the IoBT spectrum sensors have been analyzed to later choose identity attacks, malware, and SSDF attacks exploiting these threats.

The detection results obtained by SpecForce for each attack family affecting IoBT spectrum sensors demonstrate the suitability of the framework in a battlefield scenario. More in detail, for spoofing attacks, 25 IoBT spectrum sensors (10 identical RPi3 and 15 identical RPi4) have been individually identified based on their hardware chip variations. Regarding malware attacks, software kernel events and ML-based anomaly detection techniques have detected rootkits, botnets, backdoors and ransomware. Finally, eight different SSDF attacks have been detected by combining the system calls generated by the spectrum scanning process with anomaly detection techniques.

As future work, it is planned to deploy and validate the SpecForce framework in other scenarios, not only on spectrum sensors. Additionally, further objectives and research questions arise associated with the privacy management of the collected data, seeking to apply Federated Learning for distributed model generation without data sharing between sensors.

Acknowledgments

This work has been partially supported by *(a)* the Swiss Federal Office for Defense Procurement (armasuisse) with the CyberTracer and RESERVE (CYD-C-2020003) projects and *(b)* the University of Zürich UZH.

References

[1] J. M. Stocchero, C. A. Silva, L. de Souza Silva, M. A. Lawisch, J. C. S. dos Anjos, and E. P. de Freitas, "Secure command and control for internet of battle things using novel network paradigms," *IEEE Communications Magazine*, 2022.

[2] D. Papakostas, T. Kasidakis, E. Fragkou, and D. Katsaros, "Backbones for internet of battlefield things," in *2021 16th Annual Conference on Wireless On-demand Network Systems and Services Conference (WONS)*. IEEE, 2021, pp. 1–8.
[3] A. S. Hamood and S. B. Sadkhan, "Cognitive radio network security status and challenges," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*. IEEE, 2017, pp. 1–6.
[4] M. Suchanski, P. Kaniewski, J. Romanik, E. Golan, and K. Zubel, "Electronic warfare systems supporting the database of the radio environment maps," in *XII Conference on Reconnaissance and Electronic Warfare Systems*, vol. 11055. SPIE, 2019, pp. 180–189.
[5] E. Izycki and E. W. Vianna, "Critical infrastructure: A battlefield for cyber warfare?" in *ICCWS 2021 16th International Conference on Cyber Warfare and Security*. Academic Conferences Limited, 2021, p. 454.
[6] P. Théron and A. Kott, "When autonomous intelligent goodware will fight autonomous intelligent malware: A possible future of cyber defense," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 1–7.
[7] M. Patnaik, G. Prabhu, C. Rebeiro, V. Matyas, and K. Veezhinathan, "Probless: A proactive blockchain based spectrum sharing protocol against ssdf attacks in cognitive radio iobt networks," *IEEE Networking Letters*, vol. 2, no. 2, pp. 67–70, 2020.
[8] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, "Blockchain-empowered secure internet-of-battlefield things (iobt) architecture," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 593–598.
[9] I. Sanchez-Rola, I. Santos, and D. Balzarotti, "Clock around the clock: Time-based device fingerprinting," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1502–1514.
[10] P. M. S. Sanchez, J. M. J. Valero, A. H. Celdran, G. Bovet, M. G. Perez, and G. M. Perez, "A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, p. 1048–1077, 2021.
[11] S. Rajendran, R. Calvo-Palomino, M. Fuchs, B. V. den Bergh, H. Cordobés, D. Giustiniano, S. Pollin, and V. Lenders, "Electrosense: Open and Big Spectrum Data," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 210–217, January 2018.
[12] I. Agadakos, G. F. Ciocarlie, B. Copos, J. George, N. Leslie, and J. Michaelis, "Security for resilient iobt systems: Emerging research directions," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019, pp. 1–6.
[13] P. M. S. Sánchez, J. M. J. Valero, A. H. Celdrán, G. Bovet, M. G. Pérez, and G. M. Pérez, "A methodology to identify identical single-board computers based on hardware behavior fingerprinting," *arXiv preprint arXiv:2106.08209*, 2021.
[14] A. Huertas Celdrán, P. M. Sánchez Sánchez, G. Bovet, G. Martínez Pérez, and B. Stiller, "Cyberspec: Intelligent behavioral fingerprinting to detect attacks on crowdsensing spectrum sensors," *arXiv e-prints*, pp. arXiv–2201, 2022.
[15] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things*, vol. 14, p. 100129, 2021.

Pedro M. Sánchez Sánchez is pursuing his PhD in computer science at University of Murcia. He received the MSc degree in Computer Science from the University of Murcia, Spain. His research interests focus on continuous authentication, networks, 5G, cybersecurity, and machine learning and deep learning.

Alberto Huertas Celdrán is senior researcher at the Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH. He received the MSc and PhD degrees in Computer Science from the University of Murcia, Spain. His scientific interests include cybersecurity, machine and deep learning, continuous authentication, and computer networks.

Gérôme Bovet is the head of data science for the Swiss Department of Defense. He received his PhD in networks and computer systems from Telecom ParisTech, France. His work focuses on Machine and Deep Learning, with an emphasis on anomaly detection, adversarial and collaborative learning in IoT sensors.

Gregorio Martínez Pérez is Full Professor in the Department of Information and Communications Engineering of the University of Murcia, Spain. His scientific activity is mainly devoted to cybersecurity and networking, where he has published 160+ papers.

Burkhard Stiller chairs the Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH, as a Full Professor. He received the MSc and PhD degrees, respectively, from the University of Karlsruhe, Germany. His main research interests include fully decentralized systems, including Blockchains, network and service management, IoT, and telecommunication economics.