Toward a realistic Intrusion Detection System dedicated to smart-home environments

Olivier Lourme, Michaël Hauspie

Toward a realistic Intrusion Detection System dedicated to smart-home environments

Olivier Lourme, Michaël Hauspie
Université de Lille, CNRS, IRCICA, Centrale Lille, UMR9189 - CRIStAL
Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille
firstname.lastname@univ-lille.fr

***Abstract*—The Internet of Things (IoT) is a recent and ever growing model in data processing. In terms of security, the heterogeneity and specificity of protocol stacks, the variety and low resources of objects, combined with commercial pressures, lead to less mature and less robust solutions than those available in traditional Information Technologies, hence providing a new attack surface, often exploited.**

In this context, the development of Intrusion Detection Systems (IDS) dedicated to IoT is an abundant research field. Inside it, many works claim to tackle the peculiar and promising IoT smart-home segment. Sadly, a lot of them do not deal with its specific characteristics compared to other IoT fields: 1) its multiple protocol stacks in a small volume, 2) its reinforced economic stress and 3) the lack of technical skills from users waiting primarily for things to work without any hassle.

In this paper, we propose a smart-home IDS design, driven by the aforementioned characteristics of smart-home environments (technical, economic and human). For example, acquisitions and demodulations of signals should be performed by low-cost multi-protocols dongles, not needing any calibration. The anomaly detection algorithm, implemented in an updatable centralized host, should be taken among the unsupervised learning methods, less expensive and simpler than supervised alternatives. We believe that this new holistic approach, if it meets satisfactory performance metrics, may contribute significantly to a wide adoption of IDS in smart-home environments.

***Index Terms*—Internet of Things Security, Intrusion Detection Systems, Anomaly Detection, Unsupervised Machine Learning, Smart Homes**

I. Introduction

A. IoT today and its inherent security weaknesses

IoT devices, "hosts" or "objects", bridge the physical world to the virtual one of supervision. They are made of sensors and actuators, handled by microcontrollers able to communicate wirelessly thanks to their radio transceiver chips. These objects are organized in networks, often linked one to another and to the Internet via gateways. By fostering fast decision making, IoT makes system management more efficient. Logically, this new paradigm pervades all scientific and technical fields like health, transport, agriculture, or home (this paper concern), all of them becoming instantly "smart" topics. IoT modifies our private behaviors while redrawing the social and economic environments. Estimations for 2025 figure 21.5 billion objects and $1.500 billion sales[1].

[1]https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

As a corollary of this massive deployment, numerous attempts to compromise the security of IoT systems occur, leading to devices takeovers, leaks of private data or availability disruptions [1], [2]. Protecting IoT networks is more than ever necessary but it is a tough challenge. Indeed, IoT devices faces immediately two weaknesses, not present in traditional Information Technologies (IT) and making them first-choice targets [3]:

- constrained resources: microcontrollers storage (down to the KB range) and processing capabilities, as well as communication reliabilities and throughputs, are often really low, mostly fitted for the main collect and transmit task. Performing the execution of standard security algorithms used for instance in an authentication phase is almost impossible. This situation is often accentuated by the low-power requirements of devices running on batteries,
- heterogeneities: protocol stacks (also termed "communication technologies" or "technologies" in this paper) used in IoT are numerous and present different openness, ranges, modulations, topologies and also various threats at each layer of stacks. Diversities of microcontrollers and operating systems yield to a great number of combinations as well. These multiple lacks of standardisation participate to IoT opaqueness [4] and scatters security efforts.

B. Peculiar characteristics of the smart-home ecosystem

Among the IoT fields presented above, the one called "smart home" allows house tenants to subtly manage the connected devices populating it: appliances, heaters, lights, safety systems, etc. This management is often conducted via smartphone applications from inside or outside the house. Not surprisingly, device sellers promise to consumers higher degrees of comfort and security as well as substantial financial savings.

Figure 1 is an example of a simple smart-home installation featuring devices using several communication technologies, with their own topology: Ethernet, Wi-Fi, Bluetooth Low Energy (BLE) and Zigbee. When Smartphone 1 sends an order to Bulb 1, this message takes Wi-Fi, Ethernet and Zigbee paths. Complements for a full description of this figure are given in Section IV.

Concerning the two general IoT weaknesses presented at the previous subsection, smart-home environments naturally inherit from them. Combined with the typical smart-home user

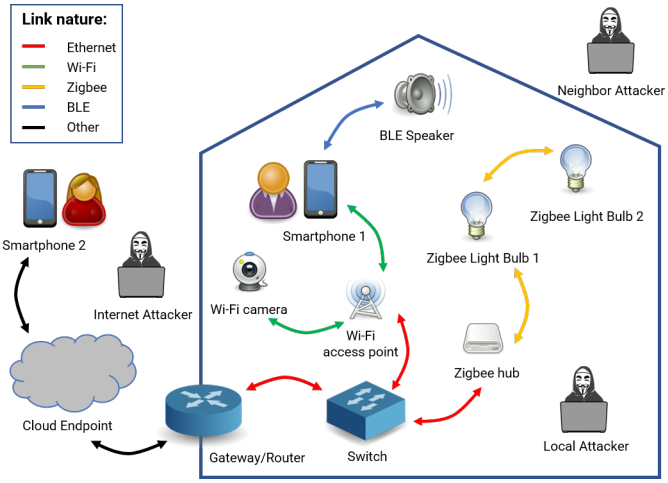

Figure 1. A smart-home implementation

profile, we finally identify, from a security perspective, three specific characteristics for the smart-home ecosystem:

1) Several communication technologies: in other IoT fields, there is often a unique communication technology for a delimited part of a project. On the contrary, a typical smart home necessarily features in a small volume heterogeneous networks of devices. Wi-Fi, BLE and Zigbee are the most widespread but others might be taken into consideration too: Z-wave, LoRaWAN, OS4I[2], etc. Additionally, some devices are stationary but others enter and go out with users, making the devices configuration always changing.

2) Cost-driven market: Even if manufacturers become more and more aware of the importance of introducing safe products to the market, several biases remain. Often, these manufacturers do not come from the IT world and hence have little security culture and a low expertise in writing safe firmwares. Furthermore, the update possibility of these latter (for an upgrade or for patching a discovered vulnerability) is often neglected, either for constraints reasons, economic ones or by fear of breaking retro-compatibility [2]. In this mass consumption segment, reduction of cost and time to market prevails to the detriment of security. Manufacturers are more preoccupied by seducing consumers, always proposing new low-cost functionalities running seamlessly. At the end, many smart-home devices present really degraded security implementation such as insecure wireless communications or custom authentication practices [5].

3) Non-technical users: Unlike in an industrial context, smart-home users are not all engineers or technicians. Most of the time, they have little security culture (adopting for instance permanent weak passwords), and rare technical skills (preventing any subtle calibration during setup or maintenance phases). A smart-home user only legitimately wants its devices to perform their tasks without flaws or annoyance. In case of an attack, it is even probable that this one does not notice anything for a long time.

[2]Open Stack for Internet of things

C. Motivation: a Smart-Home Intrusion Detection System

These three characteristics of the smart-home ecosystem induce the three following requirements for the design of a realistic protecting solution:

- it must handle the most widespread protocol stacks and easily accept new ones, hence being updatable,
- its cost must be in relation with the ones of the protected objects,
- it has to be standalone when placed in an already deployed environment; lightweight, it should not ask too complex actions from user.

Even if projects and organisations like [6] and [7] provide lists of good practices regarding IoT security, it is not surprising that successful and frequent attacks still occur, like the ones identified in [8] or layer-classified in [3]. For a safer IoT, numerous and clever Intrusion Detection Systems (IDS) are proposed in the literature as a first line of defense[3]. Nevertheless, to our knowledge, none of them proposed a global approach considering the smart-home ecosystem in its entirety.

The main contributions of this work in progress are summarized below:

- we consider a holistic approach of the smart-home ecosystem (technically heterogeneous, cost-constrained and end-used by non-specialists) in order to design a well-adapted IDS, providing sufficient added value so that it could be massively adopted by consumers,
- we establish the characteristics and architecture of that IDS thanks to an IDS taxonomy and the peculiarities of the smart-home ecosystem. Several technical choices are also motivated. For instance, concerning wireless signal acquisition, the available solutions are compared. Concerning the intrusion detection algorithm, it is chosen among those of the unsupervised learning family, dispensing from the costly and unpracticable labelling required in supervised learning,

D. Paper organisation

The remainder of this paper is organised as follows: in Section II, a topology of IDS is recalled. In Section III, we summarize relevant works in relation with smart-home IDS. Section IV introduces a threat model. In Section V, the characteristics and architecture of a realistic smart-home IDS are established from previous sections. At last, Section VI concludes this paper and presents future work.

II. Background

A. IDS definition

An IDS is a tool aiming at detecting attacks against hosts of a network. For that purpose, it collects with probes data related to the states of network and/or hosts and analyses these data in search for attacks. When an attack is detected, the IDS can log it and generate an alert. Data can be collected and

[3]Mitigation is the next step to intrusion detection. It consists in taking countermeasures reducing the harmful effects an infected device could provoke.

analysed from two different places: from the network or from hosts, leading respectively to Network IDS (NIDS) or Host IDS (HIDS), that can also possibly be combined together.

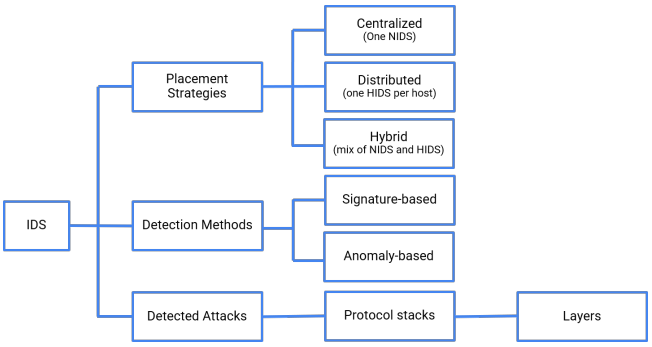

Figure 2. A taxonomy of IDS in IoT

B. Criteria for a taxonomy of IDS in IoT

The three criteria of a commonly accepted taxonomy for IDS in IoT [9] are illustrated in Figure 2 and described below:

1) "Placement strategies" criterion: This criterion corresponds to the repartition made between HIDS and NIDS to obtain the complete IDS. An HIDS is placed on the host, shares its low resources with the main task and must also conform to its operating system. It has logically access to intimate host data such as consumed bandwidth, logs or system calls, and sometimes even to side channel data like power consumption or temperature. Exploiting deciphered data is also possible. On the contrary, being integrated into a network node such as the gateway or in a dedicated system, NIDS have generally larger processing and storage capacities than HIDS, letting anticipate a comfortable use of the demanding detection methods discussed thereafter. They have access to more global data than HIDS but this data may be ciphered, regarding the analysed layer. Combining HIDS and NIDS to form a complete IDS, we may obtain:

- a "distributed placement" with a light HIDS implemented in each object [10],
- a "centralized placement" with a unique NIDS exploiting data from its probes [11],
- a "hybrid placement" with a NIDS and several HIDS, collaborating together in this case [12].

2) "Detection methods" criterion: Used for instance in [13], the "signature-based detection" (or "misuse detection") compares the payload of messages to attack signatures stored in a database. This method only detects known attacks and has logically few false positives. However, keeping a low false negative rate relies on a challenging and rigorous maintenance of the database. It also suffers from significant costs of storage and processing, which is often incompatible with constrained systems. On the other side, the "anomaly-based detection" (or "behavioral detection"), more frequent in research papers, compares the behavior of the system to a model of normal functioning. Exceeding a deviation threshold indicates an anomaly, i.e., an attack [11]. This method is effective in detecting new attacks, numerous in the IoT, including zero-day ones. However, if the model is too simple, it suffers from an excessive number of false positives since any situation deviating from the model is considered abnormal. Avoiding the complex synthesis of a legitimacy model by a human expert, artificial intelligence learning techniques, supervised or unsupervised, are often employed in anomaly-based methods but they can of course only be hosted in nodes with sufficient resources. Hybrid approaches mixing both methods exist in the literature [12].

C. "Detected attacks" criterion

Most of the time, addressed attacks presented in "IDS for IoT" papers are first related to a specific communication technology, then, inside this one, a solution to detect an attack at a specific layer is presented, leading for instance to "Addressing sinkhole attacks in 6LoWPAN[4]". Surveys dealing with IDS for IoT identify a lot of IDS positioning themselves that way [9]. These approaches often present bright solutions and are valuable contributions to IDS knowledge but, to our opinion, we should not have the same approach to design a realistic smart-home IDS. At first, because the communication technology heterogeneity is not addressed in these works and secondly because the cost and human aspects are not tackled as well, preventing such IDS propositions to be adopted in real smart-home contexts. On the contrary, the next Section focuses on the rare works that have a significant contribution toward the design of some realistic smart-home IDS.

III. Related work

Protecting a network of connected devices often implies a first axis whose aim is to correctly identify present devices, or at least their types (e.g., brand and model of a communicating light bulb), allowing for instance an administrator to isolate a device infected by a malware. A second axis, complementary to the first one, is intrusion detection in the IoT network. Both often rely on some classification works performed by supervised methods of Machine Learning (ML). A rare third axis aims at classifying the attacks once they have been detected [14] providing useful information to plan efficient mitigations.

In [15], Helluy-Lafont et al. focus on the first axis by use of physical fingerprinting, achieving 99.8% recognition accuracy in a set of ten Bluetooth devices from different types. Using a communication technology-agnostic Software-Defined Radio (SDR) for signal acquisition, they construct their ML classifiers using features such as packets preamble duration, hopping clock skew and carrier clock skew. The recognition rate is excellent, initiating a strong authentication, but on the other side, the features, extracted from the physical layer, are necessarily specific to the studied technology. Also, as the authors say, SDR require expensive computation and are complex to handle by newcomers.

In IoTSentinel [16], the authors focus also on the first axis: for each device introduced to the network, a "Security

[4]6LoWPAN is the network protocol of OS4I.

Gateway" performs a fingerprint based on the device initial network traffic. As part of a cloud "IoT Security Service" receiving the fingerprint, a set of behavioral classifiers (one per device type) recognizes the type of the introduced device. Then, given this information, the vulnerability assessment part of the "IoT Security Service" tells the "Security Gateway" for known vulnerabilities within that device type. From this information, the "Security Gateway" performs if necessary a customized isolation of the introduced device. Not properly speaking an IDS, this "exclusion before damage occurs" solution obtains good results at identifying correctly a large range of device types. Moreover, it is rather hassle-free for users thanks to its automatization. But, as drawbacks (from our perspective of building a smart-home IDS), it only supports IP devices (as many "smart-home" works), relies on known vulnerabilities and its cost, though not evaluated, must be significant because of the global architecture and the necessity to train new device-type classifiers as new devices appear on the market.

IoTScanner [4] is one of the first paper handling a real heterogeneous environment, featuring Wi-Fi, BLE and Zigbee technologies. Using one dedicated passive probe per technology, IoTScanner provides real-time analysis of the complex scanned network, without prior knowledge about it. It establishes nodes identification (thanks to their MAC addresses), links between them and at last the network structure, providing interesting insights for a technician user. Also, the authors say it is able to distinguish several types of devices without ML, using simple heuristics like sent-to-received ratio. Then, as IoTScanner uses low-cost off-the-shelf components, it makes it an affordable solution for smart-home contexts. IoTScanner brings interesting advances in smart-home protection but it remains fundamentally an analysis solution, not an IDS.

RadIoT [11] is a non-invasive IDS aiming at detecting anomalies in an heterogeneous radio environment. It observes the power spectrum by bands of 100 MHz and possibly thinner ones to listen for existing channels (e.g., a specific Zigbee one). The power spectrum on a frequency band is represented by a few statistical properties. During several days without attacks, these properties feed an autoencoder that learns to compress its inputs and to reconstruct them. The anomaly detection is based on the observed error between the reconstructed data and the input data. In this interesting agnostic approach, a SDR is a tool of choice. It is used in sweep mode to measure power over the frequency bands. The protocol independency of this approach, its non-invasiveness on IoT hosts and its low hardware cost seems to make it a good candidate for a smart-home IDS. Moreover, Deny of Service (DoS) and rogue access point attacks, both conducted in Wi-Fi, are excellently detected. But on the other side, Zigbee attacks are almost not detected because this technology has lower power compared to the coexisting Wi-Fi. As another drawback, ensuring several days without attacks at installation phase and for each newly introduced device is significantly constraining. At last, the authors say a security expert should install and calibrate the solution, driving away the perspective of a cheap solution.

IoTHound [17] is probably to date the most advanced work toward the desired IDS. Using one dedicated probe per technology (Wi-Fi, BLE and Zigbee), it automatically performs identification by grouping within clusters devices of the same type, according to their network behavior. The identification rates are promising. Also, the uncommon choice of an unsupervised method participates to an agnostic approach of the protecting solution and to its cost containment. A second contribution, illustrated with Wi-Fi, is that a continuous clustering analysis can act as an IDS by detecting a device abnormal behavior. Indeed, if a point, representing a device traffic characteristics in a n-dimension space, moves away significantly from its original cluster centroid, it might be an evidence of malicious activity. Sadly, this feature is not tested on BLE and Zigbee. At last, in another contribution, IoTHound uses the Received Signal Strength Indications given by the different antennas of a Wi-Fi router to approximately localize a Wi-Fi device. This allows to differentiate between instances of the same device type even in case of MAC randomization (sometimes adopted for privacy) or spoofing, hence providing an interesting authentication for static devices. Though brilliant, we are more sceptical about the practicability of this feature only tested on Wi-Fi, because it requires a multi-antenna open router and a Support Vector Machine device direction classifier per type of router.

In this paper, we focus on giving guidelines for the design of a realistic smart-home IDS that covers more than mainstream Wi-Fi, that has a reasonable cost by avoiding expensive upstream work and inadequate technical choices and that guarantees simplicity for users.

IV. Threat model

Alrawi et al., in their wide security evaluation of home-based IoT deployments [18], see four main components for smart-home devices:

- the device itself,
- the mobile application interacting with it,
- some cloud endpoints (the Internet services that the device or the mobile application communicate with),
- network communications (the local networks and Internet traffics between the first three components).

For each of the four components, they identify possible attack vectors, possible mitigations and the stakeholder responsible for each of these latter. Then, as depicted on Figure 1, they complete their threat model by seeing three attacker types (from high to low risk of occurrence):

- the off-path attacker, working from the Internet,
- the on-path attacker, working from the local networks,
- the neighbor attacker, exploiting means made possible thanks to the open nature of the wireless communications medium: eavesdropping, message injection and jamming.

Threats are therefore ubiquitous. But given the cost and simplicity requirements a smart-home IDS should necessarily meet, a monitoring of only the smart home inner networks may be considered to detect intrusions. Our large assumption is that attacks performed from any of the three aforementioned

attackers will induce a behavior change that a home IDS can detect. Of course, this will have to be assessed.

V. IDS CHARACTERISTICS AND ARCHITECTURE

A. IDS characteristics obtained via IDS taxonomy

Crossing the requirements of a smart-home protection established in Section I-C with the two first IDS taxonomy criteria presented in Section II leads to the following first two IDS characteristics:

1) A centralized NIDS: Host IDS (both in distributed and hybrid placements) are inappropriate. Indeed, developing an additional IDS firmware for each type of deployed device and considering its upload process are not conceivable tasks because of the amount of work, the devices lack of resources and the non-openness of certain parts of protocol stacks. HIDS should also be avoided because they present a common path for both main task data and intrusion-relative data. This lack of independency can legitimately make us wonder if a device victim of a DoS attack would be able to signal it as it only benefits from degraded resources in that situation. On the contrary, a centralized NIDS presents the following advantages: its resources can be sized to the used detection algorithms and to the firmware update process (e.g., for supporting a new protocol stack and/or new attack detections); typically, a 60 Euros Raspberry Pi 4 should fit these purposes. The uniqueness of the IDS ensures mastered costs for design, maintenance and consumption. Also, like described in [13], it is possible to consider a wired link between the acquisition probe(s) and the IDS processing part, making the IDS still working in case of jamming of the house. Of course, as a drawback, a centralized NIDS is itself the unique point of failure in the protection.

2) An anomaly-based detection: maintaining a significative attack signature database in the heterogeneous context of IoT is unrealistic. Also, the desired IDS should detect new attacks. At last, as an IoT device performs most of the time the same well-defined task, its normal behavior is rather regular [19]. For these reasons, we opt for anomaly detection methods, keeping in mind to maintain a low rate of false positives. ML algorithms are deemed to be efficient in such topics, but they are also resource demanding.

B. Other IDS characteristics

The multi-technology coverage, low-cost and simplicty requirements also induce the following remaining characteristics:

1) An agnostic IDS: having an IDS able to deal with several communication technologies and accept new ones implies an IDS agnostic from protocol stacks. In that purpose, the IDS should be furtive and perform, if possible, only passive eavesdropping. Additionally, the IDS should have no initial knowledge of the used communication channels and eventual network identifiers.

2) A clustering algorithm for anomaly detection: as we saw, many intrusion detection solutions make use of supervised learning algorithms. In these methods, training and validating data obtention, features extraction and normalization, followed by the labelling of each point as characterizing a "presence of intrusion" or an "absence of intrusion", are expensive manual upstream steps, especially if they have to be repeated for different technologies. Useful and efficient in certain situations, this workflow is inappropriate in the cost-constrained context of our smart-home IDS (using already labelled datasets is an option but it is hard to find some dedicated to other traffics than IP). On the contrary, in an IT context [20], Terzi et al. chose for their IDS an unsupervised learning. Data points do not have to be classified; they make clusters based on the resemblance of their features. Making the reasonable assumption that attacks are rare and statistically different from normal situations, the points representing the attacks, even unseen ones, will be located in specific clusters with low density, allowing their detection. In addition to being inexpensive, clustering fosters an agnostic approach.

3) Features extracted from OSI link layer: for agnosticism and reusability, features extracted to perform the detection should be common to all considered technologies. The most relevant communication layer where to extract features alimenting the ML model appears to be the link layer of the OSI model. First because the physical layer is too much technology-dependent. Then, because data above link layer is often ciphered. Deciphering it via the obtention of a key is inappropriate, at least for privacy reasons. Link layer packet headers (MAC addresses and packet type or length, etc.), conjugated with metadata like timestamps, provide interesting basis to construct features.

4) Inexpensive and efficient acquisition probes: two options may be considered concerning the wireless data acquisition and its processing:

- Software-Defined Radio (SDR): SDR are transceivers having only the physical layer implemented in hardware. In acquisition mode, they capture wide bandwidths of signal in a technology-agnostic way while the upper layers are implemented in software, running on a CPU. At first sight, they look like the ideal tool, supporting potentially all protocols, even new ones by software updates. Unfortunately, the data they collect is huge (several MB/s, depending on SDR sample rate and resolution) and as SDR is not yet a mature field, a lot of time must be spent writing resource-costly demodulators and setting calibration gains. Furthermore, the price of an efficient SDR may reach several hundreds of Euros. Globally, it is difficult to obtain a really economical tool optimised for all considered communication technologies.
- Dedicated transceivers used as sniffers: Sniffers dedicated to a communication technology are low-cost (10 to 20 Euros), low-power and efficient. They directly provide link layer data in reliable conditions. Moreover, a set of different sniffers (e.g., CC2531 for Zigbee, etc.) can nowadays be replaced by a unique multi-protocol chip (e.g., nRF52840 handling 7 stacks, Pycom boards, etc.) ensuring containment of consumption, development time and cost. This option seems the best candidate for the acquisition part of a smart-home IDS, even if adding initially unplanned technologies during the IDS life

Figure 3. Architecture of the proposed smart-home IDS

appears non-practical. The overall hardware cost of the smart-home IDS should be under a hundred of euros, compatible with prices met in this segment.

5) A hassle-free IDS: in case of an attack in progress, the user should be alerted by a relevant notification on its smartphone, to possibly itself quarantine the infected host (as mitigation has not been tackled in this work). The IDS should be hardwired to the output router to prevent the notification transmission from being jammed. Also, complex setup or calibration should not be asked to the user, implicating to consider IDS ease of use from the beginning of the design.

The architecture of the proposed IDS is given Figure 3. It respects the characteristics established in the current Section.

VI. Conclusion and Future Work

In this work, we considered a holistic approach of the smart-home ecosystem in order to establish the detailed characteristics an IDS should present to widely enter real smart-home environments: This IDS must handle the most widespread protocol stacks, be cheap and simple for users. These constraints led to decisive technical choices, presented in this paper. The future work will have for first mission to implement the proposed guidelines in a solution covering at least two technologies, proving a possible generalization. Then, a test protocol considering different attack types (observing the threat model we elected) will be set up in order to assess this "demonstrator" with the classical metrics: accuracy, recall and precision. At this stage, we will be able to say if our approach conducts to a worthwhile intrusion detection solution, bringing added value to smart-home security.

References

[1] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017, conference Name: Computer.

[2] T. Zillner, "ZigBee exploited - The good, the bad and the ugly," *Magdeburger Journal zur Sicherheitsforschung*, no. 12, pp. 699–704, 2016.

[3] C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *2014 IEEE Conference on Communications and Network Security*, Oct. 2014, pp. 67–72.

[4] S. Siby, R. R. Maiti, and N. O. Tippenhauer, "IoTScanner: Detecting Privacy Threats in IoT Neighborhoods," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, ser. IoTPTS '17. New York, NY, USA: Association for Computing Machinery, Apr. 2017, pp. 23–30. [Online]. Available: http://doi.org/10.1145/3055245.3055253

[5] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things Security "Hands-On"," *IEEE Security Privacy*, vol. 14, no. 1, pp. 37–46, Jan. 2016, conference Name: IEEE Security Privacy.

[6] OWASP, "OWASP Internet of Things Project - OWASP," 2018. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

[7] ENISA, "Baseline Security Recommendations for IoT," 2017, library Catalog: www.enisa.europa.eu. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[8] N. Dhanjani, "Abusing the Internet of Things [Book]," 2015, library Catalog: www.oreilly.com. [Online]. Available: https://www.oreilly.com/library/view/abusing-the-internet/9781491902899/

[9] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, Apr. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517300802

[10] T.-H. Lee, C.-H. Wen, L.-H. Chang, H.-S. Chiang, and M.-C. Hsieh, "A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LowPAN," in *Advanced Technologies, Embedded and Multimedia for Human-centric Computing*, ser. Lecture Notes in Electrical Engineering, Y.-M. Huang, H.-C. Chao, D.-J. Deng, and J. J. J. H. Park, Eds. Dordrecht: Springer Netherlands, 2014, pp. 1205–1213.

[11] J. Roux, E. Alata, G. Auriol, M. Kaâniche, V. Nicomette, and R. Cayre, "RadIoT: Radio Communications Intrusion Detection for IoT - A Protocol Independent Approach," in *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, Nov. 2018, pp. 1–8.

[12] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.

[13] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct. 2013, pp. 600–607, iSSN: 2160-4894.

[14] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, Oct. 2019, conference Name: IEEE Internet of Things Journal.

[15] E. Helluy-Lafont, A. Boé, G. Grimaud, and M. Hauspie, "Bluetooth devices fingerprinting using low cost SDR," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, Apr. 2020, pp. 289–294.

[16] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT," in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Jun. 2017, pp. 2177–2184, iSSN: 1063-6927.

[17] P. Anantharaman, L. Song, I. Agadakos, G. Ciocarlie, B. Copos, U. Lindqvist, and M. E. Locasto, "IoTHound: environment-agnostic device identification and monitoring," in *Proceedings of the 10th International Conference on the Internet of Things*, ser. IoT '20. New York, NY, USA: Association for Computing Machinery, Oct. 2020, pp. 1–9. [Online]. Available: http://doi.org/10.1145/3410992.3410993

[18] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security Evaluation of Home-Based IoT Deployments," in *2019 IEEE Symposium on Security and Privacy (SP)*, May 2019, pp. 1362–1380, iSSN: 2375-1207.

[19] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," in *2018 IEEE Security and Privacy Workshops (SPW)*, May 2018, pp. 29–35.

[20] D. S. Terzi, R. Terzi, and S. Sagiroglu, "Big data analytics for network anomaly detection from netflow data," in *2017 International Conference on Computer Science and Engineering (UBMK)*, Oct. 2017, pp. 592–597.