Toward an Intrusion Detection Approach for IoT based on Radio Communications Profiling

Jonathan Roux, Eric Alata, Guillaume Auriol, Vincent Nicomette, Mohamed Kaâniche

Toward an Intrusion Detection Approach for IoT based on Radio Communications Profiling

Jonathan Roux, Éric Alata, Guillaume Auriol, Vincent Nicomette, Mohamed Kâaniche
LAAS-CNRS, Université de Toulouse, CNRS, INSA, Toulouse, France
Email : {jonathan.roux, eric.alata, guillaume.auriol, vincent.nicomette, mohamed.kaaniche}@laas.fr

***Abstract*—Nowadays, more and more Internet-of-Things (IoT) smart products, interconnected through various wireless communication technologies (Wifi, Bluetooth, Zigbee, Z-wave, etc.) are integrated in daily life, especially in homes, factories, cities, etc. Such IoT technologies have become very attractive with a large variety of new services offered to improve the quality of life of the endusers or to create new economic markets.**

However, the security of such connected objects is a real concern due to weak or flawed security designs, configuration errors or imperfect maintenance. Moreover, the vulnerabilities discovered in IoT products are often difficult to eliminate because, most of the time, they cannot be patched easily. Therefore, protection mechanisms are needed to mitigate the potential risks induced by such objects in private and public connected areas.

In this paper, we propose a novel approach to detect potential attacks in smart places (e.g. smart homes) by detecting deviations from legitimate communication behavior, in particular at the physical layer. The proposed solution is based on the profiling and monitoring of the Radio Signal Strenght Indication (RSSI) associated to the wireless transmissions of the connected objects. A machine learning neural network algorithm is used to characterize legitimate communications and to identify suspiscious scenarios. We show the feasibility of this approach and discuss some possible application cases.

***Index Terms*—Internet of Things, IoT, Security, RSSI, IDS, Smarthome, Detection**

I. Introduction

The Internet of Things (IoT) has received increasing interest in the last few years. Indeed, the use of smart connected objects has become a reality in most of the activities of our daily life, at home as well as in public and professional spaces. It is estimated that the number of IoT objects will exceed 25 billions in the next 5 years [1]. Many of such objects (speakers, TVs, cameras, doors, shutters, lightbulbs, screwdrivers, etc.), that used to lack connectivity in the past, have nowadays the possibility to interact with other objects in the vicinity or remotely through the Internet, using heterogeneous communication protocols, such as Zigbee, Bluetooth or Z-Wave. While such evolution enables the development of new attractive services for the users, serious concerns can be raised with respect to the new opportunities offered by IoT objects to attackers to threaten the security and privacy of the users [2]. Indeed, IoT devices are relevant attack targets because they often collect critical information about the network (such as usage, environmental data, location, other connected devices), which can endanger the privacy of users in case of compromission. Some of these devices also have the ability to control objects used to ensure physical security, like locks and windows. Consequently, seriously considering the security of such connected objects is a crucial objective.

Nevertheless, new vulnerabilities involving connected IoT devices are daily reported. This is related to the fact that several IoT objects are designed without thoroughly addressing security concerns due to short lifecycles and economic pressure, or simply because of a lack of security expertise. The user motivation is rather related to the service offered by the device, its communication capabilities or its ergonomy. This does not motivate the IoT companies to invest on the security issues. Finally, specific constraints inherent to IoT devices prevent the integration of traditional security solutions in their design and implementation due to their limited resources [3]. Also, the lack of standardisation in this area led to a profusion of new IoT-specific and heterogeneous communication protocols which may have not been thoroughly tested from the security perspective [4].

Implementing security practices such as those recommended by the NIST [5] and the US Department of Homeland Security [6] contribute both to securely produce and securely use connected objects. However, such preventive measures are not sufficient and should be complemented with intrusion detection or intrusion tolerance solutions to cope with residual security threats.

In this paper, we investigate a novel intrusion detection approach aimed at addressing the challenges raised by the use of IoT devices in smart places such as smart homes or smart factories. The objective is: i) to automatically detect illegitimate behaviors and communications through the local network that might be initiated from compromised devices of the corresponding network, or from external devices inside or outside the network, and ii) to provide a solution that can be easily used by the end-users with the lowest impact on the delivered services. State-of-the art network intrusion detection techniques generally focus on TCP/IP communications. Some solutions have been also proposed to monitor specific IoT and short range communication protocols. However, these techniques cover partially the large set of protocols and communication links used in such environments. To address this problem, our technique is based on the monitoring and profiling of radio communication signals in the smart area to be protected (smart home, smart factory, etc.). The classification of legitimate and illegitimate communications is based on machine learning algorithms using neural networks. This approach is independent of the IoT protocols used and

can be deployed in various environments using heterogeneous wireless communication technologies.

This paper is organized as follows. Section II first presents a state of the art of IoT attacks and network solutions to detect them. Section III presents the adversary model and the main concepts behind our proposed intrusion detection approach and preliminary experiments. Finally, Section IV discusses future work and the experiments planned to validate our approach.

II. Related work

In this section we discuss related work, focussing first on IoT related attacks and then on the security protection mechanisms proposed to cope with such attacks.

Some classifications of the vulnerabilities of IoT devices already exist. The Open Web Application Security Project (OWASP) lists the potential attack surface that an attacker can exploit: memory leak, network, web interface, etc. [7]. Most of these vulnerabilities concern the objects design and production. Some examples are discussed in [8]. The massive DDoS IoT botnet attack based on the Mirai malware is another relevant example [9]. However, this classification does not show any particularity compared to vulnerabilities that can be found in classical IT, except those related to low resources of IoT devices.

The classification proposed in [10] categorizes the attacks according to their impact on the functionality provided by the IoT device. Four different categories are distinguished:

- Ignoring the functionality
- Reducing the functionality
- Misusing the functionality
- Extending the functionality.

This classification enables a direct interpretation of the consequences of attacks as perceived by the end-users (e.g., open a door, increase the temperature, shutdown a device, etc.).

Other papers focus on the vulnerabilities and attacks targeting the short distance IoT communication protocols. Such attacks on the local network open new possible attack surfaces not yet well explored by the scientific community. For example, M. Ryan [11] presents a vulnerability in Bluetooth Low Energy allowing attackers to brute-force encryption keys just by listening to the association phase. T. Zillner [12], presents a Zigbee security testing tool that is aimed at identifying potential vulnerabilities in IoT devices that implement this protocol. E. Ronen and al. [13] investigate the possibility to create an IoT worm in Philips Hue lightbulbs.

In respect of possible protection solutions against attacks involving IoT devices, the IoT specific characteristics such as ad-hoc communication, low resources and frequent design weaknesses require to reconsider the traditional security mechanisms. For example, antivirus solutions may not be practically feasible in IoT context, due to the impossibility to fix or install new software on most of connected devices. Moreover, the low power and limited resources (CPU, memory,...) available on these devices is a significant barrier to implement these solutions. Other mechanisms such as blacklisting or firewalls suffer from the same problems. Furthermore, they are not adapted to IoT communications. Instead of implementing the security mechanisms in the devices, a more practical solution would be to deploy them on dedicated components such as on a gateway connected to the IoT network. This approach has been investigated in some research works aimed at developing intrusion detection systems for the IoT.

The IoT SENTINEL proposed in [14] is designed to probe the WiFi and Ethernet traffic flows in an IoT network. The connected devices are identified by their MAC address. By analyzing the traffic flows, the tool can identify the type of the device as well as its potential vulnerabilities. All vulnerable objects are isolated from the other ones using filtering rules. These objects may also be prevented from connecting to the Internet. However, this solution does not cover the communication flows through other IoT protocols such as Bluetooth or ZigBee. Moreover, the proposed filtering mechanism is problematic due to the impacts on the device functionalities. Indeed, as IoT devices can not be easily patched, a vulnerable object could become useless if the vulnerabilities are not fixed.

Another intrusion detection system able to detecting attacks on IPv6 and 6LoWPAN networks was proposed in [15] which is interesting from the WAN point of view. Nevertheless, since most of connected devices only communicate up to the link level (e.g. 802.15.4), potential attacks on these communication links may not be detected.

To conclude, current solutions to monitor the activities and to detect attacks on the IoT networks cover partially the large set of protocols and communication links that are typically used in such environments. These solutions also require the development of specific probes for each relevant protocol. In the following section we propose a complementary solution that is aimed at filling this gap. It consists in monitoring and profiling the radio communication signals at the physical layer, especially by observing the Received Radio Signal Indication (RSSI). This solution can cover all the communication protocols available in the target IoT network. In the literature, the RSSI is mostly used for indoor localization [16], [17]. Yet, the possibility to use it to detect a physical intrusion within a Bluetooth connected area was explored in [18]. In our case, we extend this approach to detect not only physical intrusions, but also logical ones such as those discussed in the beginning of this section.

III. Intrusion Detection approach

The proposed intrusion detection system (IDS) essentially targets smart places connected to IoT devices. Its main goal is to detect potential attacks that can occur through wireless communications. In order to design an efficient IDS, we must consider together the behavior of the attackers, the behavior of the users themselves and the dynamic evolution of the smart places. This design is discussed in the first subsections. The last subsection is dedicated to a preliminary experimentation.

A. Attacker model and hypothesis

We consider that the attacker can proceed remotely or near the smart place, without physical interaction with the

devices of the smart place. Its objective may be to modify the information system to prepare a future physical intrusion, to collect confidential information, or to control a device of the smart place in order to bounce elsewhere. To achieve these objectives, he can either use his own device (in the case of a proximity attack), or he can use an already compromised device of the smart place (via the Internet wired connection for instance). His behavior can follow one of the following scenarios, considering the location where the attack is initiated, the time of the attack or the protocol used. The attack can be initiated:

1) from a location that is never occupied by legitimate users during legitimate communications (e.g.,from the garbage chute);
2) from a so-called "legitimate" location using a wireless technology never used by legitimate users;
3) from a legitimate location using an usual wireless technology (from the legitimate users point of view), but at an unusual period of the day (e.g., at night).
4) from a legitimate location using an usual wireless technology at an usual period of the day, though following an unusual scenario (e.g., by targeting shutters with XBee without disabling the alarm first with BlueTooth);
5) in accordance with legitimate users behaviors.

This paper focuses on the four first malicious behaviors. This requires the characterization of the behavior of legitimate users as well as the dynamic evolution of the smart place (with the addition of future wireless technologies).

B. IDS Design

The proposed approach is based on the monitoring of wireless activities using probes and on the identification of misbehaviors. The probes are deployed in strategic locations of the smart place, by a security expert (as for a classic alarm). We do not need to consider the content of the messages themselves. However, the probes are used to characterize the radio communication activities on the bandwidths of interest (those that are used by wireless technologies). Our goal is not to geo-locate the emitter devices. The identification of attacks is based on a comparison of the observations by the different probes of wireless bandwidth usage with a reference model of the behavior of legitimate users. This approach leads to three main challenges:

1) It is not easy for the legitimate users to specify their usage behavior;
2) Their usage behavior can evolve depending on the time of the day or on specific events or periods (weekend, meeting, holidays, etc.);
3) New legitimate devices, possibly with new wireless technologies, may be connected to the smart place.

The first challenge corresponds to the difficulty of defining a generic behavioral model for legitimate users of a smart place. In addition, the model may differ from one smart place to another. Machine learning techniques are well suited to address this challenge. In our study, we use neural networks. As for anomaly-based intrusion detection systems, these techniques require a learning phase.

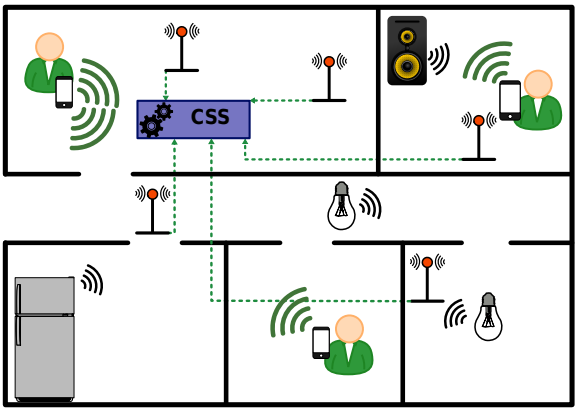

Figure 1. Architecture of the approach

To address the second challenge, different usage modes can be defined. Each mode corresponds to a model that can be different. Switching from one mode to another can be done automatically (for instance, at the beginning of the weekend) or activated by a legitimate user during a specific event or period.

To address the last challenge, three kinds of probes are considered for the design of the IDS:

- For the standard wireless technologies, we can use widely available probes (wifi, etc.).
- For other wireless technologies that are open and available today, ideally, a probe should be designed to retrieve the RSSI signal.
- To anticipate future wireless protocols without changing the deployed IDS, a Software-Defined Radio (SDR) solution should be used to observe the corresponding bandwidth.

C. IDS architecture and deployment

The architecture of the IDS is presented in figure 1. It consists of two main components: a *Central Security System (CSS)*, and the *Radio Probes*.

The CSS processes the observations collected from the probes and implements the intrusion detection algorithm to detect illegitimate behaviors. All the probes in the architecture are connected to this device via a secure channel (wired or not). The main goal of the CSS is to aggregate all the information gathered by the probes, and to process them with the neural network, that has to be initially trained to recognize what is a normal behaviour and what is not.

The Radio Probes are small sensors used to listen to all the wireless communications inside and around the smart place. They are configured to collect specific data representative of the communications behaviour, such as the RSSI (Received Signal Strength Indication), which is a power measure of the received signal of an antenna. These probes are deployed to ensure the coverage of the smart place, then their different RSSI measures are correlated to identify the location of

the broadcast emission. The neural network can be trained to recognize the legitimate areas in which devices usually communicate within the smart place. In case a transmission is observed from an illegitimate place, outside of the home for instance, where no devices are normally used, the neural network will detect an attack.

However, to avoid too many false positives, the reception timestamp and the radio activity during an interval of time are added to the RSSI information received from the probes. They are correlated with the specified detection mode to allow the neural network to detect unusual communication durations or unusual peaks of activity.

D. Preliminary experiment

To evaluate the feasibility of our solution, a first preliminary experiment has been carried out in our laboratory. The considered smart place, as described in figure 1, is representative of an appartment. At this stage, only one IoT protocol, Zigbee, is considered. Our experimental setup is composed of the following elements: 1) Five *Radio Probes* (with ZigBee tranceivers and Raspberry Pi3 boards) monitor the Zigbee traffic and extract RSSIs from the gathered communication before sending them to the CSS; 2) One *Central Security System*, a laptop which gathers the information received from the Raspberry Pi and sends them as inputs to a neural network software; 3) Some IoT devices with one Zigbee transceiver on each, to mimic the legitimate objects in the smart place; 4) A Laptop with Zigbee transmitter to communicate with the IoT devices, either to generate attacks or to perform legitimate transmissions.

Currently, a feasibility test has been carried out to check whether the RSSI perceived by the different probes is significantly modified, when communications are initiated from different places. For this purpose, one probe is moved in the environment and performs several transmissions from different places. The results show that the RSSI is significantly modified according to the position of the devices from the probes and that it is possible to correlate the information gathered by multiple probes. The table I shows the average RSSI (in -dBm) for six different transmissions collected by 2 probes. The results show that it is possible to correlate the RSSI of a transmission on two probes to learn information about the transmitter position (here Tx3 is closer to the two probes than Tx6).

Table I
AVERAGE RSSI RESULTS ON TWO PROBES FOR 6 DIFFERENT TRANSMISSIONS

	Tx1	Tx2	Tx3	Tx4	Tx5	Tx6
Probe 1	-63 dBm	-63 dBm	-64 dBm	-72 dBm	-77 dBm	-85 dBm
Probe 2	-94 dBm	-75 dBm	-70 dBm	-67 dBm	-72 dBm	-71 dBm

This first experiment, which is a fundamental prerequisite for our solution, provides some preliminary promising insights about the relevance of our approach to detect intrusions based on the modification of the radio communication patterns. More significant and comprehensive experiments are planned to validate our approach.

IV. CONCLUSION & FUTURE WORK

This paper presents a new intrusion detection solution to protect connected areas like smart homes and smart factories. It is based on the monitoring and anomaly detection of wireless radio communications through neural networks. As future work, we plan to implement the whole proposed solution and to evaluate experimentally its detection efficiency (false positives, false negatives, etc.). The planned experimentation protocol will require the definition of realistic IoT network configurations, including legitimate and malicious communication scenarios. The training period of the neural network also needs to be ajusted according to the scenarios. Finally, several heterogenous IoT communication protocols will also be investigated.

REFERENCES

[1] G. I. Analysts, "Internet of Things (IoT) Market Trends," http://www.strategyr.com/MarketResearch/Internet_of_Things_IoT_Technology_Market_Trends.asp, 2015.

[2] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning IoT Security "Hands-on"," in *IEEE IoT*, 2016.

[3] A. Keranen, M. Ersue, and C. Bormann, "RFC 7228 Terminology for Constrained-Node Networks," https://tools.ietf.org/html/rfc7228, May 2014.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys Tutorials*, Nov. 2015.

[5] R. Ross, M. McEvilley, and J. Carrier Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST, Tech. Rep., Nov. 2016.

[6] U.S. Department of Homeland Security, "Strategic Principles for Securing the Internet of Things (IoT)," U.S. Department of Homeland Security, Tech. Rep., Nov. 2016.

[7] OWASP, "OWASP Internet of Things Project - OWASP," https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project\#tab=IoT_Vulnerabilities, Mar. 2017.

[8] N. Dhanjani, *Abusing the Internet of Things*. O'Reilly, Aug. 2015.

[9] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer*, Feb. 2017.

[10] E. Ronen and A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights," in *Security and Privacy (EuroS&P), 2016 IEEE European Symposium On*, 2016.

[11] M. Ryan and others, "Bluetooth With Low Energy Comes Low Security." in *Usenix*, 2013.

[12] T. Zillner and S. Strobl, "ZigBee exploited: The good the bad and the ugly," in *BlackHat USA*, 2015.

[13] E. Ronen, C. O'Flynn, A. Shamir, and A.-O. Weingarten, "IoT Goes Nuclear - Creating a ZigBee Chain Reaction," *Draft*, Mar. 2017.

[14] 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," *arXiv:1611.04880 [cs]*, Nov. 2016.

[15] S. Raza, L. Wallgren, and T. Voigt, "SVELTE Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, Nov. 2013.

[16] E. Goldoni, A. Savioli, M. Risi, and P. Gamba, "Experimental analysis of RSSI-based indoor localization with IEEE 802.15.4," in *2010 European Wireless Conference (EW)*, Apr. 2010.

[17] X. Dang, Y. Hei, and Z. Hao, "An improved indoor localization based on RSSI and feedback correction of anchor node for WSN," in *2016 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Jul. 2016.

[18] Y. Sung, "Intelligent Security IT System for Detecting Intruders Based on Received Signal Strength Indicators," *Entropy*, Oct. 2016.