Kalpa Publications in Computing

Volume 14, 2023, Pages 121–124

Proceedings of V XoveTIC Conference. XoveTIC 2022

Building an Autonomous Portable Device to Analyse Wireless Traffic Protocols in IoT

José Á. Álvarez-Sánchez[1*], Rubén Pérez-Jove[123†], and José M. Vázquez-Naya[123‡]

[1] Facultade de Informática, Universidade da Coruña, Elviña, 15071 A Coruña, Spain
[2] Grupo RNASA-IMEDIR, Departamento de Ciencias de la Computación y Tecnologías de la Información, Facultade de Informática, Universidade da Coruña, Elviña, 15071 A Coruña, Spain
[3] Centro de Investigación CITIC, Universidade da Coruña, Elviña, 15071 A Coruña, Spain

Abstract

Monitoring wireless traffic of Internet of Things (IoT) devices can be interesting for multiple reasons, such as carrying out security audits, assisting in debugging tasks or even checking the correct state of the inventory to detect obsolete or unused equipment.

There are currently several tools available on the market that undertake this sort of functionalities, allowing devices that use these protocols to be debugged or the traffic they emit to be analysed. Some examples of this type of solutions are Ubertooth or CC2531. However, these solutions require human intervention or connection to some other hardware such as a laptop.

In this project, we developed a tool that can analyse Wi-Fi, Bluetooth and ZigBee protocols due to their increased use in IoT environments. Unlike most of the equipment available on the market, the proposed tool can work with multiple protocols and autonomously, including its own storage system and energy supply.

1 Introduction

IoT devices are available to meet a variety of needs and can be found on gadgets like smartwatches, in smart homes, offices or industrial environments and even in smart cities. Growth of such technologies is most noticeable in the industrial sector, so much so that the term "Industry 4.0" began to be coined [1].

With the rise of malware in this field, such as the Mirai botnet [2], the security of IoT networks has become critical. At its peak, Mirai infected more than 600,000 devices worldwide. The infected devices were mainly used for DDoS attacks.

The existence of tools that analyse network traffic looking for possible security attacks or allow new products to be debugged is very useful. There are currently several devices with this

[*] Developed the tool
[†] Contributed to the development and revision of the project
[‡] Contributed to the development and revision of the project

purpose, such as the Ubertooth [3] or Ellysis Bluetooth Explorer [4], among others. However, current solutions lack autonomy or they only process one protocol. Table 1 summarises the most relevant features in the context of the present project.

Taking into account the shortcomings of available solutions on the market, this project proposes the creation of a device that allows the analysis of Wi-Fi, Bluetooth and Zigbee protocols. Our tool is capable of identifying new devices or detecting the type of encryption and operating autonomously.

Device	**Portability**	**Open source**	**Required software**	**Supported protocols**
HackRF [5]	high	yes	GNU Radio	All
AWUS036ACH [6]	medium	yes	Wireshark	Wi-Fi
Bluefruit LE Sniffer [7]	medium	yes	Wireshark, nRF Sniffer for BLE	Bluetooth
Ubertooth [3]	medium	yes	Wireshark	Bluetooth
ZigBee CC2531 [8]	medium	no	whsnif	ZigBee
Ellysis Bluetooth Explorer [4]	low	no	Ellysis Bluetooth analyser	Wi-Fi, HCI
CatWAN USB Stick [9]	medium	yes	NA	LoRaWAN
Sigfox SDR Dongle [10]	medium	no	Sigfox Radio Signal analyser	Sigfox

Table 1: Tools comparison

2 Materials & Methods

Choosing a methodology that suits the needs of a project is crucial to increase the chances of project success, in this case chose an incremental model. Each was separated into a design, development and integration phase.

The project has an initial iteration to provide autonomy to the tool. A SD reader to store data, a 9V battery to supply power and an Arduino Mega 2560 as the main board were used at this stage. Moreover, Arduino IDE and Saleae Logic 2 were used for flashing boards and debugging respectively. In the following iteration we used ESP-01 to work with Wi-Fi protocol, used ArduinoPCAP to generate PCAP files, which can be analysed with Wireshark [11]. Afterwards, we integrated the Bluetooth module HC-05. It can work in master mode, therefore we can use it to scan the network for devices. Lastly, with the help of the XBee module and the xbee-arduino library, we list the different devices that are on the same network. For this purpose, the XCTU program had to be used, which allows us to modify its configuration.

Economic viability was also taken into account. Salary and material costs amount to $2.342,50.

3 Results & Discussion

With the completion of the project, a tool capable of operating autonomously and able to work with Wi-Fi, Bluetooth and ZigBee protocols was developed. The tool is capable of running for at least one day, monitor network traffic to enumerate the devices in a network, store the results in an external storage device so it can be exported to a computer later on.

The final assembly of the tool can be seen in the wiring diagram of the Figure 1. Source code is hosted on GitHub and can be found on wpm repository [12].

It is worth noting that, when designing a hardware product, a bad decision can result in a large increase in time and cost. It also highlights the lack of modules compatible with boards such as Arduino that allow PCAP files to be generated for the protocols mentioned. Finally, if you are only going to work with a specific protocol, this tool may not be of interest.

As possible future work lines, chips such as ESP8266EX, CC2541, CC2531 could be used to gain greater control over the firmware, ultimately being able to generate PCAP files. Furthermore, following this approach, instead of using the Arduino Mega board, a specific one could be created, minimising the size. Finally, a wider range of wireless protocols such as LoRa or Sigfox could be supported.

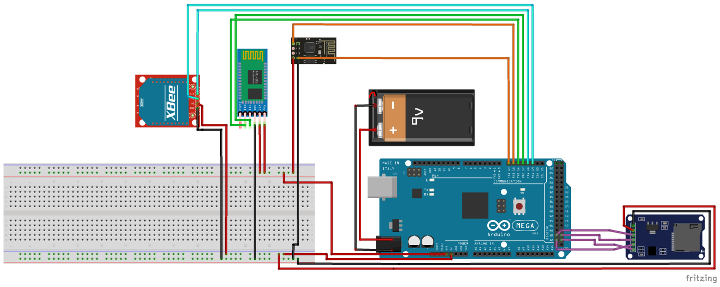

Figure 1: Wiring diagram

References

[1] Li Da Xu, Eric L. Xu, and Ling Li. Industry 4.0: state of the art and future trends. *International Journal of Production Research*, 56(8):2941–2962, 2018.

[2] Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. Ddos-capable iot malwares: Comparative analysis and mirai investigation. *Security and Communication Networks*, 2018:7178164, Feb 2018.

[3] Great Scott Gadgets. Ubertooth. https://greatscottgadgets.com/ubertoothone/. Accessed: 2022-08-27.

[4] Ellysiss. Ellysiss bluetooth explorer. https://www.ellisys.com/products/bex400/. Accessed: 2022-08-27.

[5] Jorge Rodríguez de Haro. Análisis software y hardware del sdr hackrf one, 11 2017.

[6] Alfa Network Inc. AWUS036ACH. https://www.alfa.com.tw/products/awus036ach. Accessed: 2022-08-27.

[7] Adafruit. Bluefruit LE Sniffer. https://www.amazon.es/Bluefruit-Sniffer-Bluetooth-Energy-nRF51822/dp/B00SKWGPE0. Accessed: 2022-08-27.

[8] Texas Instruments. ZigBee CC2531. https://opencircuit.es/producto/llave-usb-zigbee-cc2531. Accessed: 2022-08-27.

[9] Electronic cats. CatWAN USB. https://electroniccats.com/store/catwan-usb-stick/. Accessed: 2022-08-27.

[10] Sigfox. Sigfox sdr dongle. https://build.sigfox.com/sdr-dongle. Accessed: 2022-08-27.

[11] Wireshark. https://www.wireshark.org/. Accessed: 2022-08-27.

[12] José Á. Álvarez-Sánchez. Wireless protocol monitor. https://github.com/itasahobby/wpm, 2022.