Bluetooth Operation Classification via Low-Frequency Monitoring of the RF Output and the Power Amplifier Signals

Abdelrahman Elkanishy

Abstract

Bluetooth is a widely-used wireless communication protocol in small portable devices due to its low energy consumption and high transfer rates. Manufacturers normally buy their Bluetooth chips from third-party suppliers, which are then integrated into a complex hardware-software stack with a variety of potential vulnerabilities. Direct measurement of the output and input power signals can help security functions prevent unauthorized data transmission. This project is part of bigger project which proposes a compact supervisory circuit to classify the operation of a Bluetooth chip at low frequencies by monitoring the radio frequency (RF) output and the power input lines of the Bluetooth chip. The idea is that classification algorithm can be inexpensively fabricated on a low frequency integrated circuit in legacy technology and/or with minimal area. When the supervisory circuit detects abnormal behavior, it can be configured to shut down the Bluetooth chip. Using features extracted from the power lines, we are able to train several machine learning (ML) algorithms to classify different Bluetooth operation modes and parameters such as operation profile, distance between the paired devices, and number of connected devices. Previously, we already investigated the RF output signals and trained ML models that can separate Bluetooth advertising and transmit/receive modes with ~ 100% accuracy and classify the operation profile of the Bluetooth chip with ~ 100% accuracy. For this project, I am aiming to inspect the power input of the power amplifier which drives the chip's antenna. Also, I will investigate can the Power amplifier signal replace the RF signal to get the same classification accuracy.

Background

Bluetooth is considered the most common choice for wireless communication in compact devices such as smartwatches, headsets, fitness trackers, and smartphones. In addition, through its extensive usage in Internet of Things (IoT) devices, Bluetooth has developed over the past 20 years to provide low energy consumption and high transfer rates which fit perfectly for area- and power-limited devices [1]. Due to the complexity of the integrated smart devices that use the Bluetooth communication protocol, most manufacturers are outsourcing the chips to third-party suppliers. The integration between many outsourced chips has resulted in the need to add a hardware security layer to ensure appropriate operation. For example, in Apple's smartphones, there is a dedicated a co-processor, Secure Enclave, to handle all cryptographic operations and maintain the integrity of data protection [2].

Bluetooth, as any communication protocol, has vulnerabilities. On the other hand, researchers disclose those attacks in order to provide security updates to defend users' devices. For instance, in 2017, Armis identified a new Bluetooth attack vector called BlueBorne that can take control of the target device. BlueBorne attacks regular computers, smartphones, and IoT devices [3]. This security breach occurs without pairing to the targeted device nor even while the Bluetooth is in discovery mode. As the Bluetooth chip is responsible for establishing the connection and controlling the flow of data, BlueBorne and other security breaches could attack the Bluetooth communication chip without consent of the controller chip. Therefore, monitoring a Bluetooth chip at the hardware level is necessary to verify its correct operation. One way to monitor the chip is to consider it as a black box which consumes and transmits power. Thus, abnormal behavior can be detected by learning the normal input/output (I/O) power signatures or by parameterizing aspects of the Bluetooth connection (e.g., profile type, distance between paired devices, and number of connected devices) and comparing to the controller chip instructions. Supervisory circuits are commonly used in detecting power failures but are not common for security purposes [4]. Recently, a company called PFP Cybersecurity partnered with XILINX to detect security breaches in XILINXs devices using artificial intelligence [5]. Their work is focused on the device scope, not the chip level, and is focused on monitoring XILINX devices only.

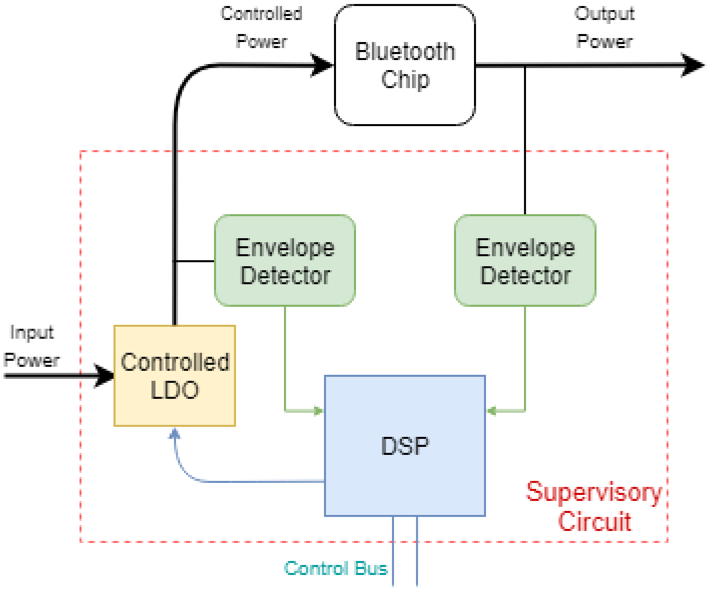

Fig. 1 Block diagram of the supervisory circuit which contains a low drop out (LDO) voltage regulator, current sensor, and envelope detector, as well as a digital signal processing (DSP) block to implement the classification algorithm.

We are concerned with creating a supervisory circuit to detect abnormal operation of a Bluetooth chip. We want a supervisory circuit that can operate at low frequency, low power, and with simple computations. This will facilitate our ability to fabricate the supervisory circuit in inexpensive circuit technology. When the supervisory circuit detects a security abnormality, the circuit can intervene and shut down the Bluetooth chip. The supervisory circuit design is split into four main parts, as shown in Fig. 1. First, the circuit that provides and controls power is comprised of a controlled low drop out (LDO) voltage regulator. LDOs are widely used in portable communications systems since they occupy a small area and provide high transient performance. Second, a current sensor monitors the output current of the LDO. Third, the envelope detector circuitry lowers the frequency of the RF output voltage signal in order to sample it at frequencies lower than 4.8 GHz, the Nyquist rate of the 2.4 GHz Bluetooth signal, so that the supervisory circuit can be implemented using low-speed technology. The output of the current sensor and the output of the envelope detector are digitized using analog-to-digital converters. Finally, a digital signal processor (DSP) will be used to extract the features from all relevant signals. At runtime the system will compute features to feed into machine learning models to determine what operation is running on the Bluetooth chip; then, we will detect abnormalities from what the supervisory circuit thinks the chip should be doing.

In this project, I will investigate another power signal domain of the Bluetooth chip which is the IVDD of the power amplifier that drives the antenna. Also, implement the digital signal processing part

(ADC, feature extraction and ML model) on a FPGA in order to accomplish a real-time classification. Thus, we can estimate the computational power of our algorithm, and to test the practicality of the algorithm.

Project plan

Lab Setup

We prototype our supervisory circuit using evaluation boards and an oscilloscope in order to collect a data set sufficient for training and testing. An evaluation board for the CYW20706 Bluetooth chip is used to program and emulate different profiles and events. The CYW920706WCDEVAL evaluation board supports pinouts for measuring the power lines of the CYW20706 Bluetooth chip. Also, it allows a USB connection with a computer for programming the chip and controlling it while running the program. The Bluetooth board is programmed to act as 2 popular profiles: hands-free and headset, in addition to customized profiles using GATT services. While each profile is running, different events are occurring (dialing, hang-up, streaming music, etc.). The events are controlled using a graphical user interface on a laptop.

Project Tasks

1- Collecting the envelope of the RF signal and power amplifier IVDD signal at the same time using the oscilloscope at a sampling rate not more than 1MHz which is the sampling frequency of the ADC on the FPGA board (DE10-Lite Board). The project is limited with this frequency rate which maybe results an aliased sampled signal. Thus, one of the biggest challenges of this project is to relay on features of the aliased signal.

2- Using MATLAB, I will extract features from the power streams that can be denote to the operation of the Bluetooth chip. The project is focused on relatively big processing window of 640ms which can include huge number of transmission events. Consequently, the aim of the algorithm is to track the overall behavior of the chip.

3- Training different Machine learning algorithms such as, such as decision tree, K-Nearest Neighbor (KNN), support vector machine (SVM), and quadratic discriminant analysis, for the purpose of comparing their accuracy and prediction speed. For all classifiers, I will use 25% holdout validation for testing the models. Then, I will choose the best algorithm in accuracy, prediction speed, and the lowest computational implementation. The training will done using the classification learner tool of MATLAB.

4- Comparing the performance of the power amplifier classifiers and the enveloped RF ones from the points of accuracy, predication speed, and the computational complexity. In order to hardware implementation of the pre-trained model.

5- Converting the pre-trained model to a VHDL code. In addition, utilizing the on board ADC to sample the power signals. And, converting the feature extraction MATLAB scripts to a VHDL code. Then, burn it on DE10-Lite Board. Next, testing the classification accuracy of the implemented model by feeding data through the serial communication with the PC. And, calculate the computational latency of the feature extraction stage.

6- Integrating the FPGA chip with measurement and power suppliers chips (LDO). Then, testing the accuracy of the system. Also, measuring the performance of the detecting the Bluetooth attacks.

Metrics for Success

For the feature extraction stage, the sign of success is to extract features that can easily differentiate between the various transmission modes and the Bluetooth profiles. For the machine learning models, 25% holdout of the collected data set will be used to validate the accuracy of the classifiers. After burning the code on the FPGA, I will test the prediction accuracy using a new collected data to feed it through the USB port. The project overall success can be measured by classification accuracy of the overall system after implementation and integration with the LDO circuit. For more testing, a well-known Bluetooth hack can be realize on the board, then see if the system will detected or not.

References

[1] K. Chang, “Bluetooth: a viable solution for iot? [industry perspectives],” IEEE Wireless Communications, vol. 21, no. 6, pp. 6–7, December 2014.

[2] iOS Security, iOS 11, January 2018. [Online]. Available: https://www.apple.com/business/docs/iOS Security Guide.pdf

[3] The Attack Vector BlueBorne Exposes Almost Every Connected Device. [Online]. Available: https://www.armis.com/blueborne/

[4] Power Fingerprinting (PFP) cybersecurity. [Online]. Available: https: //www.pfpcyber.com/

[5] T. Electronics, Coordinated Circuit Protection Schemes Help Prevent Overvoltage and Overcurrent Damage. [Online]. Available: http://www.te.com/documentation/whitepapers/pdf/eDigest-Circuit Protection Devices.pdf