A System Architecture to Detect and Block Unwanted Wireless Signals in a Classroom

Daniel Barros
Instituto Politécnico de Viana do Castelo, Portugal

Paulo Barros
Instituto Politécnico de Viana do Castelo, Portugal

Emanuel Lomba
Instituto Politécnico de Viana do Castelo, Portugal

Vítor Ferreira
Instituto Politécnico de Viana do Castelo, Portugal

Pedro Pinto
Instituto Politécnico de Viana do Castelo, Portugal
ISMAI and INESC TEC, Porto

Abstract

The actual learning process in a school, college or university should take full advantage of the digital transformation. Computers, mobile phones, tablets or other electronic devices can be used in learning environments to improve learning experience and students performance. However, in a university campus, there are some activities where the use of connected devices, might be discouraged or even forbidden. Students should be discouraged to use their own devices in classes where they may become alienated or when their devices may cause any disturbance. Ultimately, their own devices should be forbidden in activities such as closed-book exams. This paper proposes a system architecture to detect or block unwanted wireless signals by students' mobile phones in a classroom. This architecture focuses on specific wireless signals from Wi-Fi and Bluetooth interfaces, and it is based on Software-Defined Radio (SDR) modules and a set of antennas with two configuration modes: detection mode and blocking mode. When in the detection mode, the architecture processes signals from the antennas, detects if there is any signal from Wi-Fi or Bluetooth interfaces and infers a position of the unwanted mobile device. In the blocking mode, the architecture generates noise in the same frequency range of Wi-Fi or Bluetooth interfaces, blocking any possible connection. The proposed architecture is designed to be used by professors to detect or block unwanted wireless signals from student devices when supervising closed-book exams, during specific periods of time.

2012 ACM Subject Classification Computer systems organization → Architectures

Keywords and phrases campus, classroom, closed-book exam, fraud, wireless, detection, blocking, Software-Defined Radio

Digital Object Identifier 10.4230/OASIcs.ICPEC.2021.12

Category Short Paper

1 Introduction

The last decade has seen an increase in the use of personal mobile devices such as smartphones [12]. In the context of a campus environment, such devices offer several advantages as they can be used to enhance the learning experience and students performance. However, according to the survey in [16], 95% of students bring their own mobile phones to class every day, challenging the Bring Your Own Device (BYOD) policy and generating other concerns. When students use their own devices in some activities, they may become alienated, lose attention in class, and suffer from social isolation, powerlessness, meaninglessness [10]. The

classes and other events in campus can also be disturbed by the use of such devices, due to recurrent buzzing as students receive or send messages [6]. Last but not least, mobile devices can be used for exam fraud, *i.e.* students may use these devices to exchange with colleagues, information such as photographs or texts about the exam subject, during examinations [1]. Fig. 1 presents a typical scenario in a college or university where a classroom is equipped with computers/workstations connected to the campus IP network. In this classroom, on a specific time period, a group of students is about to perform a task, *e.g.* an online closed-book exam, supervised by a professor. Each student uses the college or university computer but may also bring to the classroom their own mobile phones (and/or other connected devices such as tablets, ear buds, etc). Since it is a closed-book exam, to prevent the misuse of student'

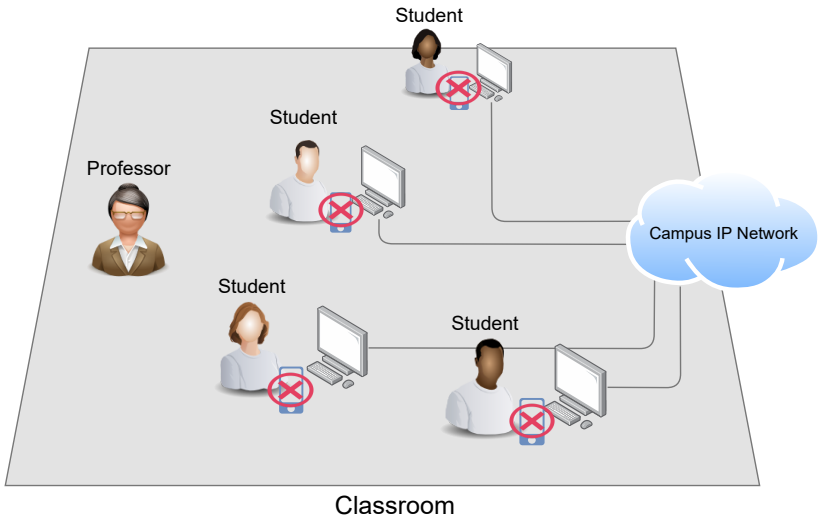

Figure 1 Classroom scenario.

communication devices, the professor would require the students to turn off their phones or to put them in "Airplane Mode". However, not all students comply with this rule. In this scenario, the students' mobile devices may use their Wi-Fi and Bluetooth interfaces. The detection of signals in the classroom environment, originated in the devices' transceivers is of great importance to detect eventual abuses and locate the abusing device. Also, blocking communications from/to these devices can be the last mile resource to assure that everyone complies with the rules of the exam. This paper presents an architecture to detect and block unwanted wireless signals in the typical scenario described. This architecture is expected to aid professors detecting non allowed devices using Wi-Fi or Bluetooth during activities such as a closed-book exam in a classroom. This paper is organized as follows. Section 2 presents the background and related work. Section 3 details the proposed architecture and discusses its implementation. Section 4 draws conclusions.

2 Background and Related Work

In a campus environment, the BYOD policy may affect infrastructure security levels [5], academic fairness and students performance. A study in [16] refers that 95% of students bring their phones to class every day, 92% use their phones to text messages during class

time, and 10% of the students admit to have texted during an exam on at least one occasion. In [14] the author highlights that young adults, such as university students with higher social media interactions, seem to feel more socially isolated than their counterparts with lower social media interaction [14], resulting in a deficit of student performance. In [7] the author surveyed a group of students to evaluate academic dishonesty, using the same anti-social behaviour pattern in [11]. The results showed that, as the students grew older, the prevailing of cheating grew exponentially higher, jumping from 10% in the age of 7, to 65-70% in the ages from 17 to 18 years old. The percentage of students that cheated multiple times hovered around 15 to 20% for students from 17 to 18 years old. The study in [1] highlights that the use of technology-facilitated learning methods is more common on college majors for their expertise and financial affluence, as well as majors that require the use of technologies are also more likely to involve technology in the cheating process. The devices used by the students in campus have mainly 3 types of interfaces to connect to the "external world": the cellular communications, Bluetooth and Wi-Fi. Cellular or mobile communications can be used in compliance with 2G standards (GSM&GPRS), operating at 900MHz, 3G standards (UMTS/IMT, IMT-2000, CDMA2000), or 4G standards (LTE), operating at 1800MHz, 2100MHz, and 2600MHz. In each country or region, cellular communications must comply with strict regulations, require specific licenses to operate, and must provide particular service availability, therefore, they are not considered in this study. Bluetooth is used to connect the device to wireless peripherals such as earphones or keyboards. It operates in a range of frequencies from 2402 to 2480MHz, uses channels of 2MHz and has a range from 4.5 to 100 meters depending on the Bluetooth version. Regarding Wi-Fi, the latest versions of its standards [8] include IEEE 802.11g and IEEE 802.11n, which operate in frequency ranges from 2401 to 2495MHz using 14 channels of approximately 20MHz, and IEEE 802.11ac, which operates only at the 5GHz band. The current proposal does not contemplate this band, since it would require different hardware. Fig. 2 resumes the spectrum used by Bluetooth Low Energy (BLE) and Wi-Fi 2.4GHz standards. In order

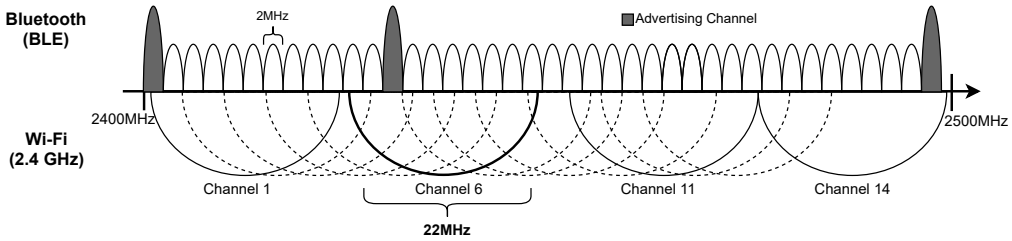

Figure 2 Spectrum utilization of Bluetooth and Wi-Fi standards.

to detect wireless signals, the frequency spectrum on frequencies used can be analysed. In [13] device detection is achieved through the periodic detection of the probe signal, used to recognize nearby networks, of Wi-Fi enabled devices. Other strategies perform passive monitoring on the network as in [4] where the author presents a solution to prevent Wi-Fi misuse by students, by checking the power of wireless signal received and controlling the network access, through passive traffic sniffing. This solution, implemented in Iowa State University Campus, allows an instructor to filter traffic, based on certain requirements. To block wireless signals, a signal blocker, also known as jammer or inhibitor can be used. A signal blocker is a device that generates a static signal or random noise over a single or a range of frequencies, at such a power level that a nearby device cannot use that spectrum anymore thus, blocking the normal operation of communications on that device. Regarding signals

blocking techniques, in [2] the authors assess the performance of Wi-Fi under the impact of jammers and present a reactive jammer that adjusts its jamming strategy according to the states of participating nodes. In [9] the authors present a comparative analysis between sweeping and non-sweeping frequency jamming, concluding that both techniques present no differences regarding jamming effectiveness, although sweeping frequency jamming is taken as more flexible. Authors in [18] describe low-layer attacks against Wi-Fi networks that can be performed using modified firmware and an inexpensive, "off-the-shelf Wi-Fi dongle". In [15] the authors assess the impact of jamming in a wireless network by varying the power and frequency of transmission along with the payload size at sender and analysing the impact on packet throughput. In [3] authors perform selective jamming of BLE advertising packages by using a low-cost, small-sized, and power efficient implementation. In order to detect or block a signal, a Software-Defined Radio (SDR) module can be used. An SDR module is a device that receives and digitizes a signal and implements by software most of the traditional signal processing components such as filters, mixers, modulators, or detectors [17]. In the opposite direction, an SDR module working as a transmitter, converts a digital input into its equivalent radio signal. These approaches enable dynamic (re)configurations of the radio, thus broadening the range of applications of their hardware. Depending on its hardware characteristics, a receiving SDR module can operate in a standalone fashion or be connected to a computer that would be in charge of processing the base-band signal and extracting any useful information. Table 1 presents common and low-cost SDR modules with relevant characteristics for the current context.

Table 1 Characteristics of surveyed SDR modules.

	ADALM-Pluto[1]	**HACK-RF One**	**LimeSDR**	**LimeSDR mini**	**BladeRF x40**	**BladeRF 2.0 micro xA4**
Price	150∼200€	250∼300€	650∼700€	300∼350€	500∼550€	550∼600€
RX-TX capability	RX & TX	RX & TX	6RX & 4TX	RX & TX	RX & TX	2RX & 2TX
Simplexity	Full-Duplex	Half-Duplex	Full-Duplex	Full-Duplex	Full-Duplex	Full-Duplex
TX power (dBm)	5.7	15	10	-	6	8
Freq. Range (MHz)	70 - 6000	1 - 6000	0.1 - 3800	10 - 3500	300 - 3800	47 - 6000
Bandwidth (MHz)	56	20	61.44	30.72	40	61.44
Interface	USB 2.0	USB 2.0	USB 3.0	USB 3.0	USB 3.0	USB 3.0

1) Expanded version (bandwidth, frequency range and dual core CPU).

3 Detection and Blocking Architecture Proposal

Fig. 3 presents the proposed architecture to detect and block wireless signals deployed on a scenario such as the one described in the Fig. 1. The scenario is composed of a classroom of around 100m^2, where the students take a closed-book exam. In this case, all students except one (in the center of the figure) have their mobile phones disconnected from Wi-Fi and Bluetooth. The proposed architecture is composed of a control device, a server, and a set of SDR modules with their antennas. The control device is a common computer where the professor, via a Web interface, configures the system settings, monitors the execution of the exam, and may check the location of a not-allowed connected device. The server is a computer that hosts an Web server, a back-end script, and a database, in order to store configurations and provide the necessary Application Programming Interface (API) to the control device and for the SDR modules. The server receives the settings of the control device and configures the SDR modules for detection or blocking mode. The SDR modules are controlled to receive or block the Bluetooth or Wi-Fi signals in the 2.4GHz band and

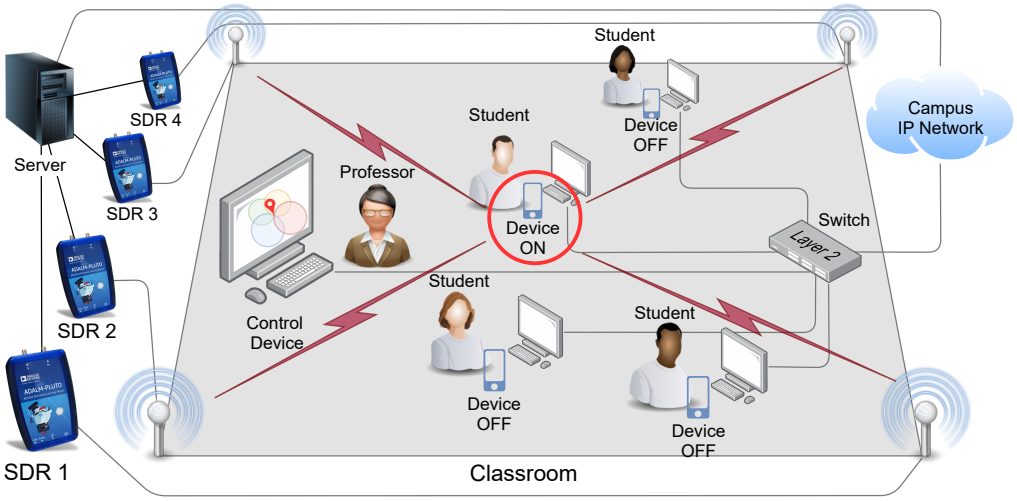

Figure 3 Proposed architecture to detect and block wireless signals.

thus, from the set of modules presented in Table 1, the SDR module ADALM-Pluto was chosen as the most cost efficient solution. This model is able to work as a detector and as a blocker, but has a bandwidth limit of 56MHz. This means that, in the current scenario, the SDR modules should work in pairs, allowing them to cover the entire 2.4GHz Wi-Fi band (of around 100MHz from 2400 to 2500MHz), as presented in Fig. 4. A detailed schematic of the

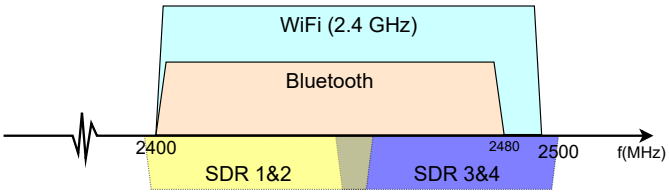

Figure 4 Wi-Fi and Bluetooth signals covered by two pairs of SDR modules.

proposed architecture is presented in Fig. 5. The professor accesses the system configuration interface in a browser on the Control Device, which is connected via Ethernet to the campus IP network and the Server. The Server connects to each SDR module via USB and each SDR is connected to an antenna using a coaxial cable. In case the system is configured by the professor in the Detection Mode, each SDR module is configured by the Server to work as a detector, commuting the switch to the Detection mode and enabling the Receiver block. The Server processes the signals captured by each SDR and will detect if there is any unauthorised signal from/to Wi-Fi and Bluetooth interfaces (cf. Fig. 4) in the classroom, and infer its respective device location. The detection result is presented to the professor using the Radio Monitor in the Control Device. In case the system is configured by the professor in the Blocking Mode, each SDR module is configured by the Server to work as a jammer, positioning the switch in the Blocking Mode and enabling the Emitter block in each SDR module. Each SDR module will generate a noise signal that will be amplified by the power amplifier in the same range of the Wi-Fi and Bluetooth signals (cf. Fig. 4), thus cancelling any transmission possibility. Receiving or transmitting in specific frequencies may have legal implications. Thus, the proposed architecture should comply with all the legal requirements inside campus, national (Portuguese) and European Union laws.

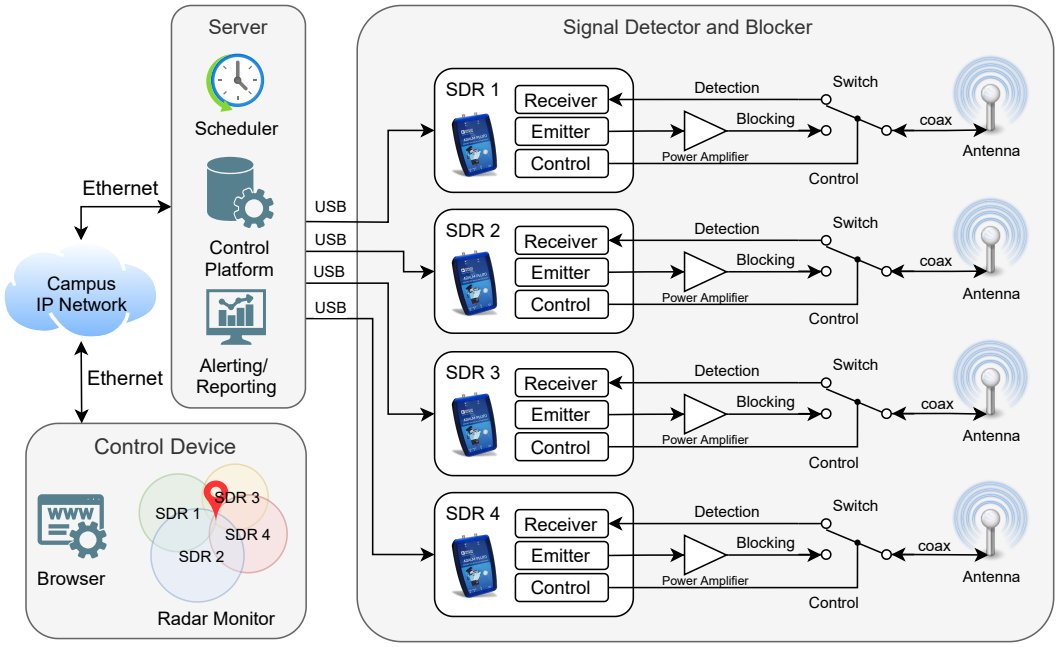

Figure 5 System Architecture.

4 Conclusions and Future Work

Nowadays, students have their own mobile devices and bring them to classes in colleges and universities, taking advantage of the BYOD policy. Although normally allowed in some learning scenarios where students are intended to be with maximum concentration, the use of such devices is not recommended, since it may lead to problems such as total alienation and classes disturbance. There are also cases where these devices are definitely forbidden, such as the case of closed-book exams. To limit the use of mobile devices during specific time frames in a particular classroom it is useful to detect and block the signals from/to these devices. This article presents a system architecture to detect and block wireless signals from Wi-Fi or Bluetooth interfaces. When in detecting mode, this architecture includes SDR modules to detect and infer location of a device transmitting/receiving unwanted signals. The proposed architecture is expected to aid professors detecting non allowed devices in a classroom in scenarios such as a closed-book exam. Further efforts will be applied to build and test a prototype of the proposed architecture. Future work should also address the legal implications and provide results of technology acceptance.

References

1 Eric M. Anderman and Tamera B. Murdock. *Psychology of Academic Cheating*. Elsevier Inc., 2007. doi:10.1016/B978-0-12-372541-7.X5000-1.

2 Emrah Bayraktaroglu, Christopher King, Xin Liu, Guevara Noubir, Rajmohan Rajaraman, and Bishal Thapa. Performance of IEEE 802.11 under jamming. *Mobile Networks and Applications*, 18(5):678–696, October 2013. doi:10.1007/s11036-011-0340-4.

3 Sebastian Bräuer, Anatolij Zubow, Sven Zehl, Mehran Roshandel, and Soroush Mashhadi-Sohi. On practical selective jamming of Bluetooth Low Energy advertising. In *2016 IEEE Conference on Standards for Communications and Networking, CSCN 2016*. Institute of Electrical and Electronics Engineers Inc., December 2016. doi:10.1109/CSCN.2016.7785169.

4 Andrew Daniel Buschbom and Andrew Daniel Buschbom. Restricting wireless network access within the classroom. *Iowa State University Capstones Theses And Dissertations*, 1(1):1–47, January 2007. doi:10.31274/rtd-180813-16155.

5 Paulo Costa, Ricardo Montenegro, Teresa Pereira, and Pedro Pinto. The Security Challenges Emerging from the Technological Developments. *Mobile Networks and Applications*, 24(6):2032–2037, 2019. doi:10.1007/s11036-018-01208-0.

6 Renata Adams Fernandes, Deisi Cristina Gollo Marques Vidor, and Alcyr Alves de Oliveira. The effect of noise on attention and performance in reading and writing tasks. In *CoDAS*, volume 31-4. SciELO Brasil, 2019.

7 António Castro Fonseca. Desonestidade nos trabalhos escolares: Dados de um estudo português. *Revista Portuguesa de Pedagogia*, 43(2):107–124, July 2009. doi:10.14195/1647-8614_43-2_7.

8 IEEE802. IEEE 802.11, The Working Group Setting the Standards for Wireless LANs, 2015. URL: https://www.ieee802.org/11/.

9 Zhang Jie, Wu Gang, and Yan Xiaowei. Comparative Analysis of Sweeping Frequency Jamming and Non-sweeping Frequency Jamming in Partial-band Jamming Based on Projectile-carried Communication Jamming. In *International Conference on Communication Technology Proceedings, ICCT*, volume 2020-Octob, pages 379–383. Institute of Electrical and Electronics Engineers Inc., October 2020. doi:10.1109/ICCT50939.2020.9295755.

10 Genevieve Marie Johnson. Student alienation, academic achievement, and webct use. *Journal of Educational Technology & Society*, 8(2):179–189, 2005.

11 Rolf Loeber, Jeffrey D. Burke, and Dustin A. Pardini. Development and etiology of disruptive and delinquent behavior, April 2009. doi:10.1146/annurev.clinpsy.032408.153631.

12 S. O'Dea. Smartphone users 2020 | Statista, 2020. URL: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

13 L. Oliveira, D. Schneider, J. De Souza, and W. Shen. Mobile device detection through wifi probe request analysis. *IEEE Access*, 7:98579–98588, 2019. doi:10.1109/ACCESS.2019.2925406.

14 Brian A. Primack, Ariel Shensa, Jaime E. Sidani, Erin O. Whaite, Liu yi Lin, Daniel Rosen, Jason B. Colditz, Ana Radovic, and Elizabeth Miller. Social Media Use and Perceived Social Isolation Among Young Adults in the U.S. *American Journal of Preventive Medicine*, 53(1):1–8, July 2017. doi:10.1016/j.amepre.2017.01.010.

15 Sethuraman Rao, S. Deepak, and Preeja Pradeep. Parametric analysis of impact of jamming in wireless sensor networks. In *IFIP International Conference on Wireless and Optical Communications Networks, WOCN*, 2013. doi:10.1109/WOCN.2013.6616191.

16 Deborah R Tindell and Robert W Bohlander. The use and abuse of cell phones and text messaging in the classroom: A survey of college students. *College Teaching*, 60(1):1–9, 2012.

17 Walter HW Tuttlebee. *Software defined radio: enabling technologies*. John Wiley & Sons, 2003.

18 Mathy Vanhoef and Frank Piessens. Advanced Wi-Fi attacks using commodity hardware. In *ACM International Conference Proceeding Series*, volume 2014-December, pages 256–265. Association for Computing Machinery, December 2014. doi:10.1145/2664243.2664260.