LABORATÓRIO EXPERIMENTAL PARA ESTUDO DE AMEAÇAS CIBERNÉTICAS UTILIZANDO O GNU RADIO

DOI: 10.37702/2175-957X.COBENGE.2025.6084

Autores: *RAUL GUSTAVO DE OLIVEIRA BORTOLOTO,PATRíCIA RODRIGUES DE ARAúJO,DéCIO RENNó DE MENDONçA FARIA,OTáVIO DE SOUZA MARTINS GOMES*

Resumo: *Este trabalho apresenta o desenvolvimento de um laboratório experimental utilizando dispositivos de Rádio Definido por Software e GNU Radio com o objetivo de fomentar e difundir a pesquisa científica em segurança cibernética de tecnologias de comunicações de radiofrequência no Sul de Minas, bem como apoiar a formação de engenheiros da UNIFEI de áreas como Engenharia Eletrônica, Engenharia Elétrica, Engenharia de Telecomunicações e Engenharia da Computação, desenvolvendo competências práticas em hacking de RF. O ambiente didático integra simulações e experimentações práticas para a recepção e análise espectral, nas faixas de VHF e UHF, execução de ataques cibernéticos como jamming e verificação das vulnerabilidades. Este ambiente serve como base para introduzir conceitos de cibersegurança em RF, melhorar a compreensão e entendimento crítico de riscos nas comunicações sem fio e estimular o aprofundamento de segurança cibernética em RF de infraestruturas críticas.*

Palavras-chave: *Laboratório experimental, Segurança Cibernética, Radiofrequência, GNU Radio, Rádio Definido por Software.,Laboratório experimental,Segurança Cibernética,GNU Radio*

LABORATÓRIO EXPERIMENTAL PARA ESTUDO DE AMEAÇAS CIBERNÉTICAS UTILIZANDO O GNU RADIO

1 INTRODUÇÃO

O uso crescente de dispositivos conectados à internet, como os de Internet das Coisas (IoT), tem transformado setores como indústria, governo, serviços essenciais e o cotidiano dos cidadãos. Esses dispositivos dependem de comunicações por radiofrequência (RF) para transmitir e receber dados por meio de tecnologias como Wi-Fi, Bluetooth, Zigbee e LoRa. Embora essa conectividade traga benefícios como mobilidade e automação, também aumenta os riscos de ataques cibernéticos, expondo os sistemas a falhas e ameaças que podem comprometer dados e infraestruturas críticas. As comunicações por RF apresentam vulnerabilidades que podem ser exploradas em ataques como spoofing, sniffing, man-in-the-middle, replay e jamming (URIBE; GUILLEN; CARDOSO, 2022; REDDY *et al.*, 2024; LU *et al.*, 2021).

Diante dos riscos crescentes nas comunicações por radiofrequência (RF), é fundamental a utilização de ferramentas que ajudem na compreensão prática das vulnerabilidades desses sistemas. Dispositivos baseados em Rádio Definido por Software (SDR) e o ambiente GNU Radio são recursos acessíveis e flexíveis que permitem simular, manipular e analisar sinais de RF, inclusive reproduzir ataques como o jamming e observar seus efeitos em sistemas reais (MAROJEVIC *et al.*, 2018; JOOSENS, 2024).

Muitas disciplinas da engenharia envolvem modelos matemáticos complexos focados em conteúdos teóricos e, com pouca experimentação prática. O GNU Radio pode ajudar a tornar esse aprendizado mais interativo e concreto. Além disso, a cibersegurança em RF ainda é pouco explorada de forma prática no ensino de engenharia, o que reforça a importância de preparar os estudantes para identificar e lidar com ameaças reais nas comunicações sem fio (KATZ; FLYNN, 2009; OLIVEIRA *et al.*, 2012; RODRIGUEZ; BOSCH; MAROJEVIC, 2018).

Com esse objetivo foi desenvolvido um ambiente experimental para o ensino e à pesquisa em cibersegurança aplicada a comunicações RF na Universidade Federal de Itajubá (UNIFEI), utilizando dispositivos de Rádio Definido por Software e GNU Radio, a fim de promover o melhor entendimento de conceitos como modulação, análise espectral, interferência, vulnerabilidades e ataques cibernéticos.

2 MOTIVAÇÃO E ALINHAMENTO ÀS DIRETRIZES DE CIBERSEGURANÇA

Considerando a relevância da proteção cibernética no cenário nacional e internacional, o Brasil tem avançado na consolidação de importantes marcos regulatórios nos últimos anos. Um dos principais instrumentos é o Decreto Nº 11.856, de 26 de dezembro de 2023, que institui a Política Nacional de Cibersegurança (PNCiber) e estabelece o Comitê Nacional de Cibersegurança (CNCiber), com a finalidade de alinhar as práticas nacionais às melhores referências globais em governança e resiliência digital. De forma complementar, o Decreto nº 10.222, de 5 de fevereiro de 2020, aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber) que define diretrizes para a

proteção de infraestruturas críticas, a promoção da inovação tecnológica e o fortalecimento da qualificação de recursos humanos especializados na área.

No âmbito das comunicações sem fio, a Agência Nacional de Telecomunicações (Anatel) por meio da Resolução nº 757/2022 regulamenta o uso eficiente do espectro de radiofrequências, enquanto a Resolução nº 767/2024 introduz modificações significativas no regulamento de segurança cibernética para o setor de telecomunicações, reforçando a necessidade de mecanismos de proteção tanto nos níveis físico quanto lógico das infraestruturas envolvidas.

Tendo em vista esse panorama de transformações normativas e estratégicas, torna-se evidente que a formação em Engenharia precisa acompanhar o avanço das políticas públicas voltadas à segurança cibernética no país. Profissionais capazes de compreender, analisar e mitigar riscos associados às tecnologias de comunicação por radiofrequência são fundamentais para o fortalecimento da resiliência digital e consolidação de uma cultura nacional de cibersegurança robusta e eficaz. A consulta pública realizada em 2023 pela Sociedade Brasileira de Computação (SBC) sobre os referenciais de formação para cursos emergentes em Cibersegurança evidencia essa urgência, ao destacar a crescente demanda por abordagens pedagógicas que priorizem competências práticas ao currículo tradicional.

Desse modo, o ambiente experimental desenvolvido neste trabalho, tem o objetivo de fomentar a pesquisa científica aplicada à segurança cibernética em comunicações por radiofrequência e, também, contribuir para a formação de engenheiros mais bem preparados para atuar de maneira ética, crítica e tecnicamente qualificada na proteção de infraestruturas críticas. A iniciativa conta com o apoio do projeto de pesquisa intitulado Segurança Cibernética em Sistemas de Tecnologia Operacional (Cyber OT) e Infraestruturas Críticas e dos laboratórios LabTel, LAIoT, u.AI e FronTIERS HackLab do Instituto de Engenharia de Sistemas e Tecnologia da Informação (IESTI) da UNIFEI, consolidando o compromisso institucional com a inovação e a excelência na formação técnica e científica.

3 DESCRIÇÃO DOS FRAMEWORKS DESENVOLVIDO

3.1 Hardware e software utilizados

Para o desenvolvimento dos frameworks, os equipamentos utilizados foram um dispositivo SDR (Software Defined Radio), um computador de mesa com sistema operacional Ubuntu e o ambiente de desenvolvimento GNU Radio.

O SDR, Rádio Definido por Software, é um receptor ou transmissor de rádio, onde os componentes de hardware tradicionais são substituídos por equações matemáticas definidas por software, superando as limitações dos rádios convencionais nos quesitos de flexibilidade e facilidade de adaptação. Estes sistemas permitem mudanças na modulação, largura de banda do sinal captado, entre outras, todas realizadas por software. Estes sistemas diferem quanto ao custo e a capacidade de processamento, sendo construídos basicamente a partir de conversores analógicos-digitais (ADC), conversores digitais-analógicos (DAC) e um módulo de processamento, podendo ser tanto dedicado, como um processador digital de sinais (DSP), ou uma CPU (Central Processing Unit) de propósito geral, além de uma antena e outros módulos periféricos pertinentes, como conversores USB (SADIKU, AKUJUOBI, 2004). Dessa forma, os dispositivos SDR oferecem inúmeras

ferramentas para o ensino da análise, manipulação de sinais e sistemas de telecomunicação.

Figura 1 - Hardware utilizado para realizar a recepção dos sinais em radiofrequência.

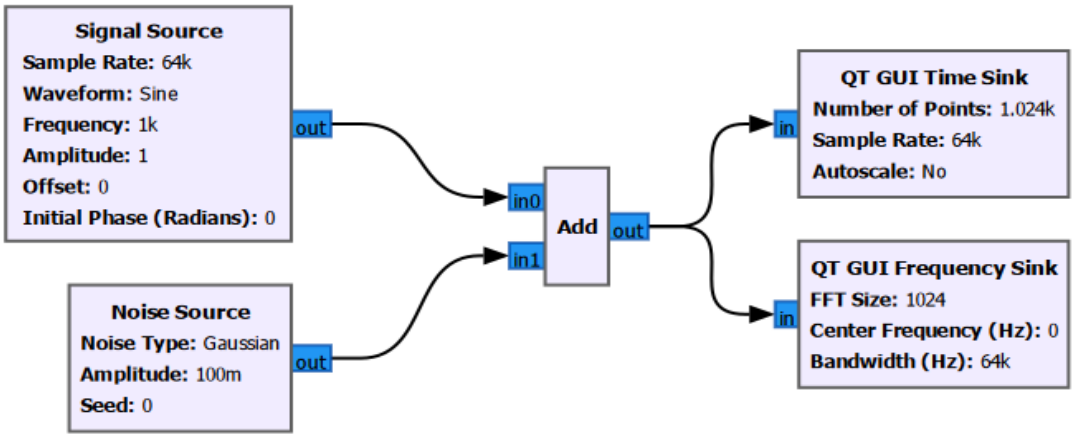
Fonte: Autor

O ambiente de desenvolvimento GNU Radio é um software gratuito e de código aberto, que permite o processamento digital de sinais por meio de blocos parametrizáveis. Ele pode ser utilizado com algum hardware externo de radiofrequência, no nosso caso o dispositivo SDR, para criar rádios definidos por software, ou até mesmo sem nenhum hardware para ambientes de simulação. É amplamente utilizado em ambientes de pesquisa e desenvolvimento, industriais e governamentais no mundo todo (“GNU Radio”, [s.d.]). A partir dele, é possível receber, converter, demodular e filtrar sinais, além de permitir a utilização de diversos outros algoritmos matemáticos utilizados nas teorias de sistemas de telecomunicação. Todo esse processo é modelado através de parâmetros descritos em cada um dos blocos, tornando-o um ótimo ambiente para cursos e aprofundamentos práticos.

3.2 Blocos de processamento de sinais do GNU Radio

A plataforma GNU Radio proposta utiliza o GNU Radio Companion, que é uma ferramenta gráfica para criar fluxogramas de processamento de sinais através de blocos parametrizáveis.

Figura 2 - Exemplo de fluxograma no GNU Radio Companion.

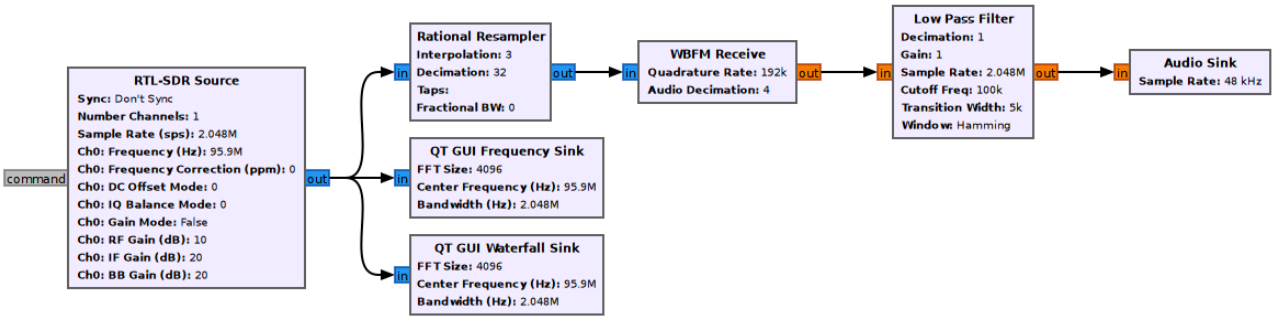


Fonte: Autor

Na figura 2, temos um exemplo de fluxograma descrito no GNU Radio Companion. Os blocos “Signal Source” e “Noise Source” são as entradas do circuito, responsáveis, respectivamente, pela geração de uma senoide de amplitude igual a 1, frequência de 1 kHz, fase nula e taxa de amostragem de 64 kHz, e um ruído gaussiano com amplitude igual a 0,1. Ambos os sinais são somados e nas saídas temos duas interfaces para observar o sinal resultante, o bloco “QT GUI Time Sink” gera uma interface para observar o sinal no domínio do tempo, já o bloco “QT GUI Frequency Sink” nos mostra o espectro do sinal, isto é, as componentes do sinal no domínio da frequência.

3.3 Framework para recepção e processamento de sinais FM

Figura 3 - Fluxograma para recepção e processamento de sinais FM no GNU Radio Companion.



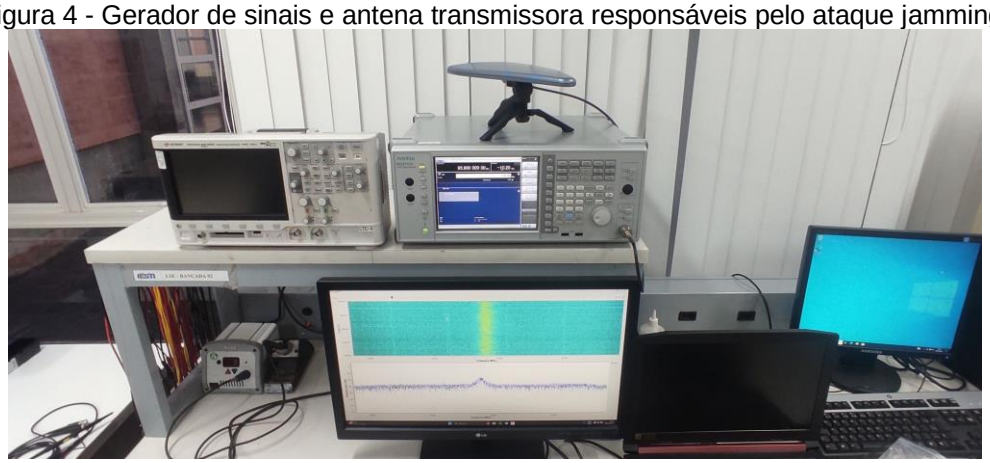
Fonte: Autor

Na figura 3, temos o fluxograma desenvolvido para aquisição de ondas moduladas em frequência no GNU Radio Companion. O bloco “RTL-SDR Source” é responsável pela aquisição dos dados digitalizados no dispositivo SDR utilizado. Para aquisição dos dados, o bloco necessita da taxa de amostragem e da frequência a ser analisada. Os dados na saída deste bloco são enviados para dois blocos GUI (Graphical User Interface), que são interfaces para visualização do sinal sintonizado. São eles o “QT GUI Frequency Sink”, responsável pela geração do espectro do sinal de forma instantânea, e o “QT GUI Waterfall Sink”, que gera o espectro do sinal ao longo do tempo, no estilo cascata.

Após a amostragem dos dados no dispositivo SDR, os dados passam por uma alteração na frequência de amostragem, através do bloco “Rational Resampler”, para adequação dos dados a serem enviados ao bloco demodulador. O bloco “WBFM Receive” é parametrizado com uma taxa de quadratura de 192 kHz, sendo este responsável pela demodulação das ondas moduladas em frequência. Após a demodulação, os dados amostrados passam por um filtro passa baixa denominado “Low Pass Filter”, parametrizado para uma frequência de corte de 100 kHz com uma faixa de transição de 5 kHz e uma janela do tipo “Hamming”. Após a filtragem, os dados são enviados à placa de áudio do computador que utiliza uma taxa de amostragem de 48 kHz.

3.4 Geração e transmissão do sinal de ataque jamming

Figura 4 - Gerador de sinais e antena transmissora responsáveis pelo ataque jamming.

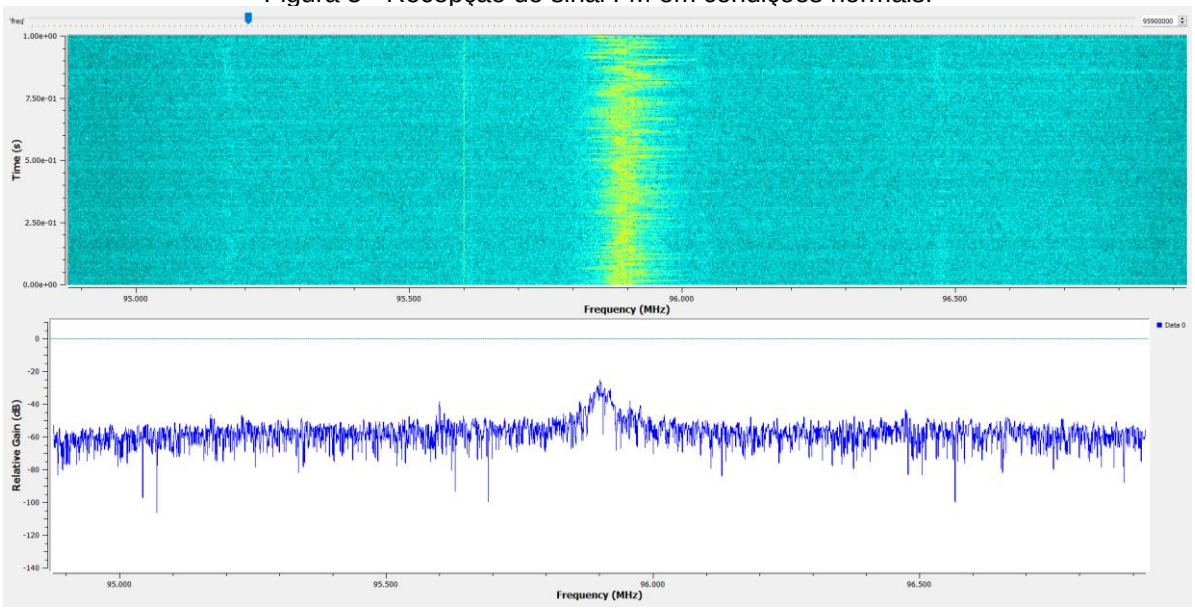


Fonte: Autor

Na figura 4, temos a ilustração da configuração realizada na ocasião. A geração do sinal de ataque foi realizada através de um gerador de sinais vetorial modelo MG3710A, da fabricante Anritsu. A onda gerada possuía amplitude e frequência variáveis na faixa necessária para o laboratório didático. A transmissão do sinal foi feita por uma antena log-periódica modelo HyperLOG 7025, da fabricante Aaronia AG, conectada ao gerador.

4 RESULTADOS OBSERVADOS NOS FRAMEWORKS

Figura 5 - Recepção do sinal FM em condições normais.

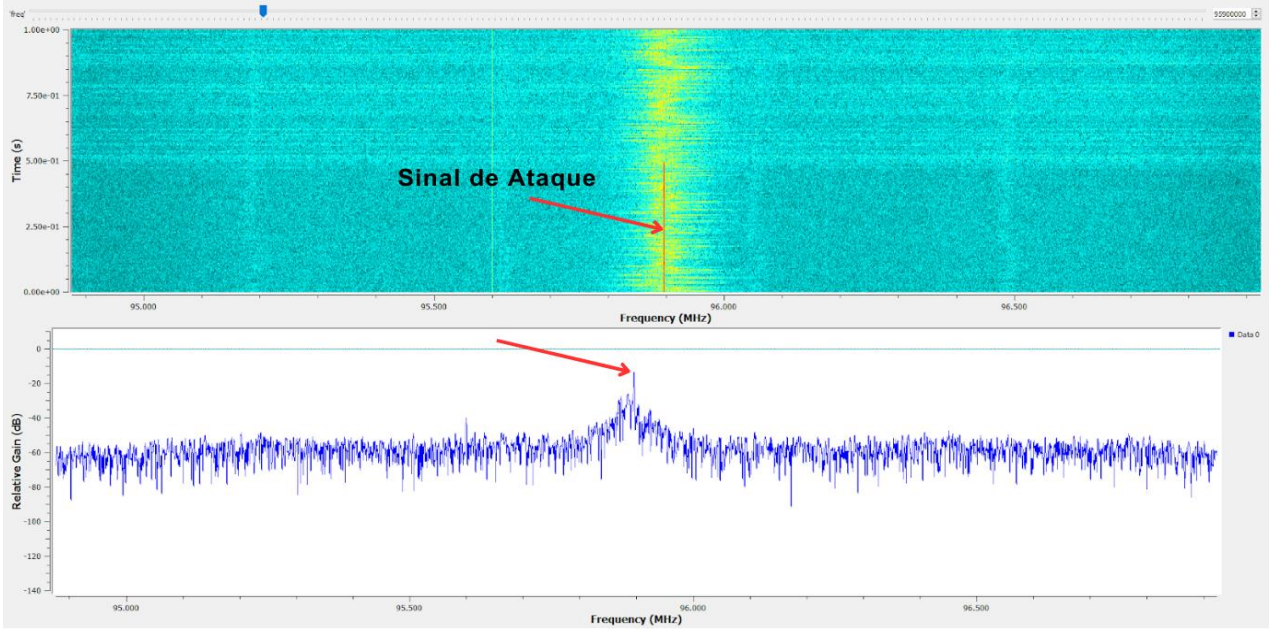


Fonte: Autor

Na figura 5, observamos a interface do programa com os dados provenientes do dispositivo SDR. Como visto anteriormente no item 2.3, foram selecionadas duas interfaces diferentes para analisar a magnitude dos dados amostrados. A interface superior é a análise espectral dos dados ao longo do tempo, conhecido como cascata, e a interface inferior é a análise espectral instantânea, sendo ambas as interfaces no domínio da frequência. Neste

experimento, utilizou-se como referência a rádio Max 95.9 FM que utiliza uma onda portadora na frequência de 95,9 MHz, transmitida no município de Itajubá no estado de Minas Gerais.

Figura 6 - Recepção do sinal FM em condições de ataque jamming.



Fonte: Autor

Na figura 6, observa-se a presença do sinal de ataque jamming na frequência de 95,9 MHz a partir dos 500 milissegundos na interface superior. Este sinal provoca na demodulação em FM o chamado “Efeito de Captura”, resultando em um silenciamento do demodulador e a impossibilidade da determinação se a estação está sendo atacada ou simplesmente com problemas de áudio.

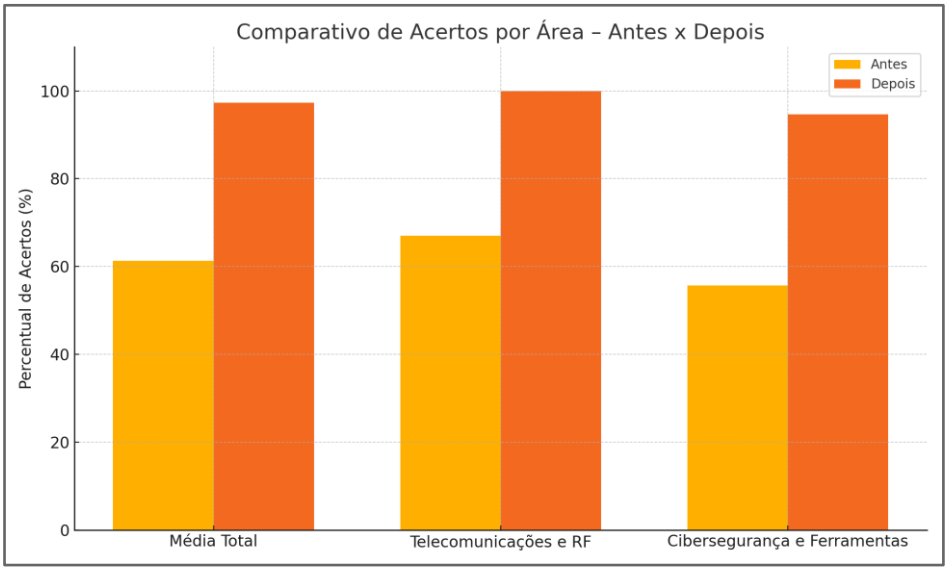
5 INDICADORES DO APRENDIZADO DE CIBERSEGURANÇA DE RF

O ambiente de ensino e pesquisa em cibersegurança em comunicações RF foi avaliado por meio da aplicação de questionários de conhecimento antes e depois das atividades práticas. A avaliação incluiu questões objetivas sobre conceitos técnicos, escalas do tipo Likert para medir a percepção de aprendizado dos participantes, e perguntas abertas destinadas à coleta de feedback qualitativo. Os conteúdos abordados nas perguntas contemplaram temas relacionados a telecomunicações, radiofrequência, cibersegurança e o uso de ferramentas práticas de hacking de RF, como os dispositivos de Rádio Definido por Software (SDR) e o ambiente GNU Radio.

A média total inicial de acertos foi de 61,33%, evidenciando conhecimento prévio limitado sobre modulação, jamming e cibersegurança em sistemas de radiofrequência (RF). Após a execução das práticas com GNU Radio e dispositivos SDR, essa média subiu para 97,33%, indicando uma evolução significativa no aprendizado. Na análise por área, os conteúdos relacionados a telecomunicações e fundamentos de RF apresentaram uma média inicial de 67%, atingindo 100% após as práticas. Já os temas ligados à cibersegurança e ferramentas práticas de hacking em RF passaram de uma média de 55,66% para 94,66%. Esses resultados reforçam o impacto positivo do ambiente experimental na assimilação dos conceitos propostos.

Essa melhoria dos indicadores do aprendizado em cibersegurança de RF pode ser visualizada na Figura 7, que compara a média de acertos antes e depois da realização das atividades práticas por área temática e total.

Figura 7 - Comparativo dos percentuais de acertos antes e depois das atividades práticas, por área temática.



Fonte: Autor

Nas respostas qualitativas dos questionários, os alunos demonstraram maior compreensão sobre vulnerabilidades reais em comunicações RF, evidenciando maior conscientização sobre a importância da segurança em ambientes urbanos inteligentes, como as *Smart Cities*, e em sistemas de controle de tráfego. Além disso, manifestaram interesse em expandir seus conhecimentos em técnicas específicas de ataques, como *spoofing e replay.*

Dessa forma, a implementação do ambiente prático mostrou-se eficaz não apenas na consolidação dos conceitos teóricos, mas também no fortalecimento da visão crítica sobre segurança cibernética em RF e no desenvolvimento de habilidades práticas relevantes no contexto da formação em engenharia.

6 CONSIDERAÇÕES FINAIS

O uso do GNU Radio e de dispositivos SDR de baixo custo demonstrou ser uma abordagem educacional acessível e eficaz, contribuindo significativamente para o aprendizado prático em cibersegurança de comunicações sem fio. O ambiente experimental desenvolvido proporcionou uma base sólida de conhecimentos sobre ameaças cibernéticas no domínio físico, promovendo a conscientização dos alunos quanto à importância da adoção de práticas seguras em sistemas de radiofrequência. Como continuidade deste trabalho, pretende-se ampliar os estudos para incluir outros tipos de ataques cibernéticos, como spoofing, sniffing, man-in-the-middle e replay, aprofundando a análise das vulnerabilidades em sistemas RF.

AGRADECIMENTOS

Os autores agradecem à Universidade Federal de Itajubá (UNIFEI), à empresa Clavis pela parceria no Projeto CyberOT e aos laboratórios LabTel, LAIoT, u.AI e FronTIERS HackLab pelo apoio técnico.

REFERÊNCIAS

BRASIL. Conselho Diretor da Agência Nacional de Telecomunicações (Anatel). **Resolução nº 757**, de 8 de novembro de 2022. Aprova o Regulamento de Condições de Uso de Radiofrequências. Diário Oficial da União: seção 1, Brasília, DF, 9 nov. 2022.

BRASIL. Conselho Diretor da Agência Nacional de Telecomunicações (Anatel). **Resolução nº 767**, de 7 de agosto de 2024. Altera o regulamento de segurança cibernética aplicada ao setor de telecomunicações. Diário Oficial da União: seção 1, Brasília, DF, 8 ago 2024.

BRASIL. **Decreto nº 10.222**, de 5 de fevereiro de 2020. Estabelece a Estratégia Nacional de Segurança Cibernética. Diário Oficial da União: seção 1, Brasília, DF, 6 fev. 2020.

BRASIL. **Decreto nº 11.856**, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Diário Oficial da União: seção 1, Brasília, DF, 27 dez. 2023.

GNU Radio. Disponível em: https://www.gnuradio.org/about/. Acesso em: 16 abr. 2025.
JOOSENS, D. et al. Software-Defined Radio-Based Internet of Things Communication Systems: An Application for the DASH7 Alliance Protocol. **Applied Sciences**, v. 15, n. 1, p. 333–333, 2024.

KATZ, S.; FLYNN, J. Using software defined radio (SDR) to demonstrate concepts in communications and signal processing courses. In: 39th IEEE Frontiers in Education Conference, p. 1–6, 2009, Texas, USA. **Anais.** Califórnia. Acesso em: 13 fev. 2025.

LU, J. et al. Machine-Learning PUF-based Detection of RF Anomalies in a Cluttered RF Environment. In: IEEE International Symposium on Technologies for Homeland Security (HST), p. 1–7, 2021, Boston, USA. **Anais**. Boston. Acesso em: 3 mar. 2025.

MAROJEVIC, V. *et al*. Measuring Hardware Impairments with Software-Defined Radios.In: IEEE Frontiers in Education Conference (FIE), p. 1–6, 2018, Califórnia, USA. **Anais.** Califórnia. Acesso em: 17 mar. 2025.

OLIVEIRA, J. P. *et al*. Uso de software livre no ensino de telecomunicações: estudo de caso com GNURADIO e USRP. In: XL Congresso Brasileiro de Educação em Engenharia, 2012, Belém. **Anais**. Belém. Disponível em: https://admin.abenge.org.br/cobenge/legado/arquivos/7/artigos/104375.pdf. Acesso em: 10 mar. 2025.

REDDY, P. M. *et al.* Detecting, Demodulating & Decoding LoRa. In: 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), p. 1–9, 2024, Kamand, India. **Anais.** Kamand. Acesso em: 16 jan. 2025.

RODRIGUEZ, R. M.; BOSCH, A. G.; MAROJEVIC, V.. A Software Radio Challenge Accelerating Education and Innovation in Wireless Communications. In: IEEE Frontiers in Education Conference (FIE), v. 36, p. 1–9, 2018, Califórnia, USA. **Anais.** Califórnia. Acesso em: 06 mar. 2025.

SADIKU, M. N. O.; AKUJUOBI, C. M. Software-defined radio: a brief overview. **IEEE Potentials**, v. 23, n. 4, p. 14–15, 2004.

SBC - SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. **Consulta pública de referenciais de formação para Cursos Emergentes Cibersegurança**. Disponível em: https://www.sbc.org.br/consulta-publica-de-referenciais-de-formacao-para-cursos-emergentes-ciberseguranca/. Acesso em: 11 fev. 2025.

URIBE, J. DE J. R.; GUILLEN, E. P.; CARDOSO, L. S. A technical review of wireless security for the internet of things: Software defined radio perspective. **Journal of King Saud University - Computer and Information Sciences**, v. 34, p. 4122-4134, 2022.

EXPERIMENTAL LABORATORY FOR STUDYING CYBER THREATS USING GNU RADIO

Abstract: *This work presents the development of an experimental laboratory utilizing Software Defined Radio devices and GNU Radio with the objective of fostering and promoting the scientific research in cybersecurity of radiofrequency communications technology in the south of Minas Gerais, as well as support the formation of engineers from UNIFEI in areas such as Electronic Engineering, Electrical Engineering, Telecommunications Engineering and Computer Engineering, developing practical skills in RF hacking. The learning environment integrates simulations and practical experiments for the acquisition and spectral analysis in the VHF and UHF Frequency ranges, execution of cyber-attacks such as jamming and vulnerabilities inspection. This environment serves as a base for introducing radiofrequency cybersecurity concepts, improving the comprehension and critical understanding of risks in wireless communication and stimulate the depth of radiofrequency cybersecurity in critical structures.*

Keywords: *Experimental laboratory, Cybersecurity, Radiofrequency, GNU Radio, Software Defined Radio.*