UNIVERSIDADE D
COIMBRA

André Alexandre Ribeiro Araújo

Transmissão BLE Segura de Sinais Vitais para Biomonitorização sem fios de Pacientes

Dissertação no âmbito do Mestrado em Engenharia Eletrotécnica e de Computadores, especialização em Computadores com subespecialização em Aprendizagem Computacional e Sistemas de Computação Eficiente de Alto Desempenho, orientada pelo Doutor David Bina Siassipour Portugal, pelo Prof. Doutor Mahmoud Tavakoli e pelo Eng. José Nuno da Cruz Faria e apresentada ao Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Setembro de 2023

FCTUC FACULDADE DE CIÊNCIAS
E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

Transmissão BLE Segura de Sinais Vitais para Biomonitorização sem fios de Pacientes

André Alexandre Ribeiro Araújo

Coimbra, Setembro 2023

Transmissão BLE Segura de Sinais Vitais para Biomonitorização sem fios de Pacientes

Orientador:

Doutor David B. S. Portugal

Co-Orientadores:

Prof. Doutor Mahmoud Tavakoli

Eng. José Faria

Júri:

Prof. Doutor Luís Alberto da Silva Cruz

Prof. Doutor Fernando Manuel dos Santos Perdigão

Prof. Doutor Mahmoud Tavakoli

Dissertação submetida para obtenção do grau de Mestre em Engenharia Eletrotécnica e de Computadores.

Coimbra, Setembro 2023

Agradecimentos

Ao longo destes cinco anos foram diversas as pessoas que me acompanharam e que de alguma forma foram imprescindíveis para a conclusão desta dissertação e, consequentemente, do meu mestrado. Como tal, gostaria de prestar os meus agradecimentos a todas as pessoas que contribuíram para esta caminhada e que a tornaram tão especial.

Primeiramente e acima de tudo, gostaria de agradecer à minha família, por todo o carinho, amor, dedicação e suporte prestados nestes anos. Ao meu pai por todos os incentivos, à minha mãe pelo alento e proteção, e à minha irmã pela cumplicidade e aconselhamento. Relembro com carinho e admiração todos os esforços que fizeram para que isto fosse possível. Sem vocês ao meu lado todos os obstáculos seriam mais difíceis de ultrapassar.

Seguidamente, expressar a minha maior gratidão ao meu orientador Dr. David Portugal, por toda a instrução, ajuda e apoio constante. Foi um pilar fundamental para que nunca ficasse desmotivado e seguisse sempre o caminho certo para que o desfecho final fosse o desejado. Um agradecimento também muito especial ao Eng. José Faria, por ter sido um enorme apoio e um suporte essencial, especialmente a nível técnico, oferecendo todo o seu vasto conhecimento e paciência em prol da minha aprendizagem. Serei eternamente grato e desejo o maior sucesso aos dois.

Gostaria de agradecer aos meus queridos amigos Eletrões, por terem feito o meu percurso académico tão gratificante e divertido. Deste grupo levo as melhores memórias e não tenho dúvidas que serão uma amizade para a vida. Destacar neste grupo o meu padrinho Bernardo Leite, por ter sido o meu fiel companheiro nesta jornada, por todos os ensinamentos, por todos os trabalhos compartilhados e por todos os momentos inesquecíveis. Um agradecimento também ao meu irmão Afonso Carvalho, por ter sido a primeira pessoa a dar-me a mão em Coimbra e por ter permanecido tão leal ao longo dos anos.

Finalmente, agradecer à minha melhor amiga Daniela, por ser o meu porto seguro, por toda a amizade e apoio, por nunca me ter deixado desistir, e por todas as conversas e momentos que me fizeram focar em alcançar os meus objetivos.

Resumo

Com a crescente necessidade de garantir os cuidados de saúde, o conforto e o bem-estar dos pacientes, temos assistido a avanços tecnológicos relevantes na área da saúde. Apesar das evidentes vantagens da digitalização da saúde, esta traz também desafios ao nível da segurança e da privacidade.

Esta dissertação encontra-se inserida no projeto *Wireless biOmonitoring stickers and smart bed architecture: toWards Untethered Patients (WoW)* e procura apresentar uma solução para o problema da segurança e privacidade de dados, através da implementação de transmissão segura de sinais vitais de pacientes, que são adquiridos por um nó de Internet das Coisas (IoT) embutido numa cama de hospital. O principal objetivo deste trabalho é assegurar as comunicações de dados vitais, garantindo que apenas as pessoas com a devida autorização podem aceder a estes. Para além disso, pretende-se garantir a robustez do sistema contra ataques de cibersegurança devido à sensibilidade dos dados pessoais envolvidos nesta transmissão.

Assim sendo, o trabalho centra-se em desenvolver e integrar mecanismos de segurança como encriptação, autenticação e emparelhamento físico via *Near Field Communication (NFC)* na comunicação sem fios através da tecnologia *Bluetooth Low Energy (BLE)*. Os mecanismos implementados são validados através de testes experimentais exaustivos realizados em laboratório num ambiente controlado.

Além disso, o trabalho desenvolvido nesta dissertação tem ainda como desfecho a realização de um estudo comparativo de desempenho entre a comunicação segura e não segura, pesando os prós e os contras de ambas as abordagens.

Palavras-Chave: Internet das Coisas; Biomonitorização; Segurança; Comunicação; *Bluetooth Low Energy*; Cuidados de Saúde; Sensores *Wearables*.

Abstract

With the increasing need to ensure the assistance, comfort, and well-being of patients, we have seen relevant technological advances in healthcare. Despite the evident benefits of healthcare digitization, it also brings security and privacy challenges.

This dissertation is part of the Wireless biOmonitoring stickers and smart bed architecture: toWards Untethered Patients (WoW) project and seeks to present a solution to the problem of data security and privacy, through the implementation of a secure transmission for patients' vital signs data collected via an Internet of Things (IoT) node embedded in a hospital bed. The main goal of this work is to provide secure communication of vital data and to ensure that only people with proper authorization can access them. In addition, the robustness of the system against cybersecurity attacks should be guaranteed, as this transmission involves sensitive personal data.

Therefore, the work focuses on the development and integration of security mechanisms such as encryption, authentication and physical pairing via Near Field Communication (NFC) in wireless communication using Bluetooth Low Energy (BLE) technology. The implemented mechanisms are validated through exhaustive experimental tests performed in a controlled laboratory environment.

Furthermore, the work carried out in this dissertation culminates in a comparative performance study between secure and insecure communication, weighing the advantages and disadvantages of both approaches.

Keywords: Internet of Things; Biomonitoring; Security; Communication; Bluetooth Low Energy; Healthcare; Wearable Sensors.

"The Internet of Things devoid of comprehensive security management is tantamount to the Internet of Threats."

— Stephane Nappo

Índice

Lista de Acrónimos

ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
ATT	Attribute Protocol
BLE	Bluetooth Low Energy
CCM	Counter with CBC-MAC
CSRK	Connection Signature Resolving Key
ECDH	Elliptic-Curve Diffie–Hellman
ECG	Eletrocardiograma
GAP	Generic Access Profile
GATT	Generic Attribute Profile
Gbps	Gigabits per second
GPRS	General Packet Radio Service
GSM	Global System Mobile
GUI	Graphical User Interface
IMU	Inertial Measurement Unit
IoT	Internet of Things
IRK	Identity Resolving Key
JW	Just Works
Kbps	Kilobits per second

LESC	LE Secure Connections
LPWAN	Low Power Wide Area Network
LTK	Long Term Key
MAC	Message Authentication Code
Mbps	Megabits per second
MIC	Message Integrity Check
MITM	Man-in-the-middle
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
OOB	Out of Band
P2P	Peer-to-Peer
PDU	Protocol Data Unit
RTOS	Real Time Operating System
SMP	Security Manager Protocol
STK	Short Term Key
TK	Temporary Key
TNEP	Tag NDEF Exchange Protocol
UUID	Universally Unique Identifier
WBAN	Wireless Body Area Networks
Wi-Fi	Wireless Fidelity
WoW	Wireless biOmonitoring stickers and smart bed architecture: toWards Untethered Patients
WPA2	Wi-Fi Protected Access 2

Lista de Figuras

Lista de Tabelas

1 Introdução

1.1 Contexto e Motivação

A biomonitorização consiste na verificação em tempo real das condições de saúde de um paciente através da leitura dos seus sinais vitais. Estes dados permitem aos profissionais de saúde avaliarem a situação do paciente bem como perceber a evolução do seu quadro clínico. Para pacientes idosos ou com doenças crónicas, é de extrema importância realizar uma monitorização contínua dos seus sinais vitais para que os profissionais de saúde consigam prever precocemente qualquer condição de perigo para o paciente, levando a que seja possível evitar tal condição [1].

Com vista à realização de uma biomonitorização contínua, hoje em dia ainda é necessário que os pacientes sejam hospitalizados e conectados através de fios a diversos aparelhos de medição de sinais vitais. Esta situação apresenta bastantes limitações, como, por exemplo, na mobilidade do paciente, pois este fica restringido à sua cama, e na inconveniência apresentada pelos fios dos aparelhos de medição conectados ao paciente, que pode levar a falsos alarmes caso ocorra algum problema na ligação entre o paciente e os aparelhos, sobrecarregando dessa forma os recursos humanos e financeiros dos sistemas de saúde [2].

Por estes motivos, surge a necessidade de evoluir tecnologicamente na área da saúde, promovendo a transição para uma saúde mais digital. Diversos países e organizações têm vindo a juntar esforços para avançar mais rapidamente com esta mudança através de programas de financiamento, como as iniciativas da Organização Mundial de Saúde [3] e da União Europeia [4]. Com a digitalização na área da saúde é possível alterar a forma como os cuidados são prestados, levando a tratamentos mais eficientes, promovendo a saúde humana [3].

Com estas evoluções tecnológicas é possível diminuir as limitações que a biomonitorização contínua com fios apresenta. A principal solução para este problema trata-se da utilização de um método que utilize comunicações sem fios. Um possível método consiste na implantação de adesivos eletrónicos no corpo do paciente de forma não intrusiva, que contêm os sensores

necessários para a aquisição de sinais vitais. Como este é um método sem fios, é necessária a utilização de uma tecnologia de comunicação *wireless* para a transmissão dos dados, como é o caso do *Bluetooth*, *Wireless Fidelity (Wi-Fi)* ou ZigBee. Embora estes avanços tecnológicos na área dos cuidados de saúde apresentem muitos benefícios, esta digitalização também levanta algumas preocupações, principalmente ao nível da segurança e da privacidade dos dados dos pacientes.

A *Internet of Things* (IoT) é um paradigma de comunicação extremamente poderoso que permite interligar elementos inteligentes através da Internet, fazendo com que estes possam trocar informações, dados e recursos [5]. Atualmente, algumas das aplicações IoT mais atrativas são os sistemas de saúde digital. Dada a elevada procura dos sistemas de saúde por inovações tecnológicas que permitam aliviar a sobrecarga nos sistemas, a IoT permite dar resposta a essa procura de uma forma eficiente [6].

Alguns dos principais requisitos de um sistema IoT incluem a sua segurança e privacidade [7], especialmente em cenários de saúde, pois os dados transmitidos são extremamente sensíveis e pessoais, sendo absolutamente necessário assegurar a proteção total da informação. Para garantir que as transmissões de dados não são comprometidas, os protocolos de comunicação sem fios utilizados devem conter mecanismos de segurança como encriptação e autenticação, que impeçam o acesso por parte de terceiros não autorizados e mal-intencionados aos dados transmitidos.

1.2 Objetivos

Esta dissertação insere-se no projeto WoW [8], que consiste no desenvolvimento de um método de biomonitorização sem fios de pacientes em camas de hospital utilizando adesivos eletrónicos colocados de forma não intrusiva na pele. Estes adesivos denominados de *biostickers*, contêm sensores capazes de medir os dados vitais dos pacientes e de transmitir estes dados através de comunicação sem fios com a tecnologia BLE para um módulo de aquisição de dados, designado *smart box*, que é responsável por adquirir os mesmos.

Trabalhos anteriores no âmbito do projeto [9, 10] mostraram que a arquitetura utilizada apresenta vulnerabilidades ao nível da segurança na comunicação entre os *biostickers* e a *smart box*. Atualmente, a transmissão de dados entre estes dois dispositivos não apresenta qualquer tipo de segurança, funcionando apenas num modo em que os dois dispositivos são conectados e os dados transmitidos sem encriptação, *i.e.*, em *plain text*.

Assim, o principal objetivo deste trabalho de dissertação é assegurar as comunicações e

acesso aos dados, garantindo que apenas as pessoas com a devida autorização podem aceder a estes. Para além disso, pretende-se assegurar a robustez do sistema contra ataques de cibersegurança devido à sensibilidade dos dados pessoais envolvidos nesta transmissão. Assim sendo, o trabalho centra-se em desenvolver e integrar mecanismos de segurança como encriptação, autenticação e emparelhamento físico via NFC na comunicação sem fios através da tecnologia BLE. Adicionalmente, o trabalho desenvolvido nesta dissertação tem ainda como desfecho final a realização de um estudo comparativo de desempenho entre a comunicação segura e não segura, pesando os prós e os contras de ambas as abordagens.

1.3 Estrutura da Dissertação

Esta dissertação está dividida em diferentes capítulos. Este primeiro capítulo apresenta o contexto e as motivações para este trabalho e os seus principais objetivos. No Capítulo 2 é apresentada uma análise crítica da literatura estudada, onde se revê o trabalho de pesquisa realizado sobre temas relacionados ao desta dissertação. Aqui incluem-se tecnologias de comunicações sem fios, aquisição e transmissão de dados sem fios e arquiteturas de sistemas para aplicações na área dos cuidados de saúde. Neste capítulo é ainda apresentada uma lista das contribuições deste trabalho para a pesquisa na área. No Capítulo 3 é apresentada a arquitetura concebida para implementação da comunicação segura, a descrição dos materiais envolvidos e a metodologia seguida. O Capítulo 4 aborda os testes de desempenho realizados e fornece os respetivos resultados e discussão. Para concluir a dissertação, no Capítulo 5 são apresentadas as principais conclusões acerca deste trabalho, apontando possíveis soluções de melhoria no sistema para trabalho futuro.

2 Trabalho Relacionado

Neste capítulo são apresentados os principais conceitos das comunicações sem fios atualmente existentes que melhor se enquadram no sistema em estudo. Para além de uma descrição das principais tecnologias, é realizada uma análise comparativa de modo a apresentar os benefícios e as desvantagens de cada uma das tecnologias. Com base neste conhecimento, são analisados trabalhos semelhantes na literatura, de forma a melhor compreender a aplicação deste tipo de comunicações, em especial na área da saúde, permitindo ter uma perceção do estado da arte atual e os principais desafios para o avanço tecnológico. Antes de terminar o capítulo são ainda apresentadas as principais lacunas encontradas na literatura revista e uma lista de contribuições que este trabalho se propõe a alcançar.

2.1 Background

A segurança e a privacidade na área dos cuidados de saúde desempenham um papel crucial para a proteção dos dados dos pacientes, isto porque um ataque a um dispositivo pode originar a divulgação de informação pessoal dos pacientes. Assim, a segurança e a privacidade na área da saúde têm como principal objetivo proteger as informações dos pacientes, como o seu nome, data de nascimento, morada ou dados biométricos. Os avanços tecnológicos e a digitalização na área da saúde, implicam uma crescente atenção à proteção destes dados, levantando diversas questões ligadas à segurança e à privacidade na transmissão dos dados [11]. Assim sendo, um aspeto fundamental que deve ser considerado quando se aborda segurança e privacidade em aplicações na área da saúde para sistemas sem fios é a tecnologia de comunicação *wireless* a ser utilizada, isto porque a escolha de uma tecnologia de comunicação sem fios que não inclua os mecanismos de segurança necessários para garantir a mesma, tornam o sistema inseguro para a transmissão de dados. Assim, torna-se evidente que a principal fonte de problemas de segurança em sistemas sem fios na área dos cuidados de saúde está na insegurança das comunicações. Por este motivo, surge a necessidade de utilizar uma

tecnologia de comunicação sem fios que empregue a segurança adequada ao sistema.

Uma tecnologia de comunicação sem fios permite que os dispositivos estabeleçam ligações sem cabos físicos por meio de diversos tipos de redes [2]. Existem diversos tipos de tecnologias de comunicação sem fios, tendo estas as mais diversas características. Cada tecnologia tem as suas vantagens e desvantagens e é com base nestas que os utilizadores decidem qual a melhor tecnologia de comunicação sem fios a utilizar dado o sistema/arquitetura que pretendem implementar. Com base no trabalho de pesquisa realizado, a decisão de qual tecnologia de comunicação utilizar incide principalmente sobre as seguintes características [10]:

- **Consumo de energia**: Se maximizar a vida útil da bateria dos dispositivos for um parâmetro importante no sistema a implementar, então a tecnologia utilizada deve ser o mais energeticamente eficiente possível.

- **Latência**: Se o sistema pretendido não for recetivo a atrasos na transmissão de dados, ou seja, lida com eventos críticos, então a tecnologia de comunicação sem fios escolhida deve apresentar uma baixa latência.

- **Alcance**: Caso os dispositivos a serem conectados estejam muito distantes um do outro, então a tecnologia a utilizar deve apresentar um elevado alcance, assegurando que o alcance é suficiente para comunicar entre dispositivos.

- **Fiabilidade**: Se for necessário garantir que todos os dados são entregues e transmitidos corretamente, então a tecnologia de comunicação deve ser o mais fiável possível, integrando mecanismos como deteção de erros ou retransmissão.

- **Segurança**: Para garantir que o sistema é o mais seguro possível, a tecnologia utilizada deve apresentar mecanismos de segurança como encriptação e autenticação, para garantir que apenas pessoas autorizadas acedem aos dados.

- **Largura de banda**: A tecnologia de comunicação sem fios escolhida deve apresentar uma largura de banda que seja suficiente para lidar com todas as comunicações dentro do intervalo de transmissão designado.

Uma das tecnologias de comunicação sem fios mais popular é o *Bluetooth*. Nesta secção será abordado o funcionamento desta tecnologia, bem como o funcionamento da tecnologia *Bluetooth Low Energy*, que é a tecnologia dentro do *Bluetooth* que melhor se enquadra nas características do sistema em estudo.

2.1.1 Bluetooth

O *Bluetooth* é uma tecnologia de comunicação sem fios de curto alcance utilizada para transmitir dados entre dispositivos. Esta tecnologia pertence ao padrão IEEE 802.15.1 e transmite numa frequência de banda na ordem dos 2.4 GHz com uma taxa de transmissão de dados entre 1 e 3 Megabits per second (Mbps) [12]. Ao nível da segurança, o *Bluetooth* utiliza o protocolo Advanced Encryption Standard (AES) de 128 bits - Counter with CBC-MAC (CCM) (AES-CCM) para implementar mecanismos de segurança como encriptação e autenticação nas comunicações.

O *Bluetooth* apresenta duas arquiteturas distintas: o *Bluetooth* clássico e o *Bluetooth Low Energy* (BLE). Como o próprio nome indica, a principal diferença entre estas tecnologias incide principalmente no consumo de energia, sendo o *Bluetooth Low Energy* a tecnologia que lida explicitamente com a utilização de um baixo consumo de energia, ao contrário do *Bluetooth* clássico. O *Bluetooth Low Energy* tem vindo a ganhar enorme destaque no domínio da IoT, pois este oferece um equilíbrio entre o consumo de energia, o alcance de transmissão e a taxa de transmissão de dados. Desta forma, o *Bluetooth Low Energy* é a tecnologia dentro do *Bluetooth* que melhor se enquadra no tipo de sistema pretendido.

2.1.2 Bluetooth Low Energy

O *Bluetooth Low Energy* (BLE) foi desenvolvido pelo *Bluetooth Special Interest Group* (Bluetooth SIG) e materializou-se pela primeira vez na versão 4.0 da especificação principal do *Bluetooth* [13]. Um dos principais objetivos para a criação desta nova tecnologia *Bluetooth* consistiu na necessidade de criar uma tecnologia que fosse altamente eficiente na utilização da energia, preservando assim a vida útil dos dispositivos conectados [14].

O BLE é uma tecnologia de baixo custo, baixa complexidade e baixo consumo de energia, especialmente designada para aplicações na área da IoT. Possui um alcance máximo de transmissão na ordem dos 100 metros, uma taxa de transmissão de dados entre os 125 Kilobits per second (Kbps) e os 2 Mbps, uma largura de banda entre os 2.400 GHz e os 2.4835 GHz, baixa latência para evitar atrasos significativos na transmissão dos dados e um baixo consumo de energia ($<$15 mA) [14, 2].

O BLE suporta diversas topologias de rede. Pode ser utilizada uma topologia em estrela (*star*), onde os dados são obtidos através de nós periféricos e posteriormente enviados para um nó central que os coleta e processa. Temos também a comunicação *Peer-to-Peer (P2P)*, que permite que um dispositivo transmita dados para um número ilimitado de recetores em

simultâneo. Por último, temos ainda a topologia de malha (*mesh*), que permite a criação de redes de dezenas de milhares de dispositivos, onde cada um é capaz de comunicar com qualquer outro dispositivo da rede [14].

2.1.3 Segurança no BLE

Ao nível da segurança, o *Bluetooth Low Energy* fornece recursos, capacidades e protocolos de segurança para proteger as comunicações [14]. O modelo de segurança do BLE inclui cinco características distintas [15]:

- **Emparelhamento:** Processo de geração e troca de chaves secretas entre dispositivos;
- ***Bonding*:** Processo de armazenamento em ambos os dispositivos das chaves secretas geradas para posteriores conexões entre dispositivos reconhecidos, saltando a etapa de emparelhamento;
- **Autenticação:** Processo de verificação do compartilhamento de chaves secretas entre dispositivos;
- **Encriptação:** Processo de encriptação dos dados transmitidos entre dispositivos. A tecnologia BLE utiliza o protocolo AES de 128 bits para encriptar os dados.
- **Integridade das Mensagens:** Processo de assinatura de dados (*data signing*) e verificação das assinaturas no dispositivo recetor, permitindo validar a identificação do remetente. No BLE é utilizado o Message Authentication Code (MAC), ou também designado Message Integrity Check (MIC), para autenticar a origem das mensagens.

O BLE apresenta duas opções de emparelhamento entre dispositivos: LE Legacy Pairing e LE Secure Connections (LESC). O LE Legacy Pairing é um método de emparelhamento que utiliza criptografia simétrica em que são geradas duas chaves: uma Temporary Key (TK) e uma Short Term Key (STK). A geração da chave temporária (TK) depende do método de geração de chaves escolhido e é gerada cada vez que ocorre o processo de emparelhamento. A chave de curto prazo (STK) é gerada a partir da TK trocada entre os dispositivos. A STK é também gerada cada vez que ocorre o processo de emparelhamento e é utilizada para encriptar toda a ligação.

O LE Secure Connections é o método de emparelhamento mais recente e foi introduzido na versão 4.2 do *Bluetooth*. O LESC é um método de emparelhamento que utiliza criptografia assimétrica e foi criado com o intuito de ser um método de emparelhamento signi-

ficativamente mais seguro que o LE Legacy Pairing. Neste método, os dispositivos utilizam criptografia Elliptic-Curve Diffie–Hellman (ECDH) para gerarem individualmente um par de chaves pública/privada. Os dispositivos trocam apenas as chaves públicas e, a partir daí, geram uma chave secreta compartilhada designada de Long Term Key (LTK). Esta chave é gerada e armazenada em cada um dos dispositivos vinculados e usada em conexões subsequentes entre os dois dispositivos. A principal vantagem no uso da criptografia ECDH consiste no facto desta evitar que terceiros descubram a chave secreta compartilhada, pois mesmo que capturem ambas as chaves públicas muito dificilmente conseguem descodificar as chaves privadas, e sem o acesso a estas não conseguem desencriptar a comunicação [15].

Embora a criptografia assimétrica tenda a ser mais lenta, uma vez que exige maior poder computacional relativamente à criptografia simétrica, a criptografia ECDH apresenta um excelente desempenho computacional, mostrando uma elevada rapidez no processo de geração de chaves [16, 17]. Assim, pelo relevante nível de segurança imposto pela criptografia assimétrica e desempenho computacional da criptografia ECDH, o método de emparelhamento LE Secure Connections mostra-se significativamente mais robusto do que o método LE Legacy Pairing.

Para além destes métodos de emparelhamento, a segurança na tecnologia BLE apresenta ainda diferentes modos e níveis. Estes termos fazem referência a uma combinação de atributos e requisitos de segurança [18]. O primeiro modo reforça a segurança por meio de encriptação, enquanto o segundo modo reforça a segurança através de assinatura de dados (*data signing*). A assinatura de dados consiste na autenticação do remetente, verificando a identidade do mesmo e garantindo que os dados não foram alterados durante a transmissão. A assinatura de dados é utilizada para transmitir dados autenticados por meio de uma conexão não encriptada, priorizando a rapidez das conexões e das transmissões de dados [19]. Na Tabela 2.1 apresentam-se os níveis e modos de segurança do BLE.

	Modo 1	**Modo 2**
Níveis	1. Sem segurança (sem autenticação e sem encriptação) 2. Emparelhamento não autenticado com encriptação 3. Emparelhamento autenticado com encriptação 4. Emparelhamento LE Secure Connections autenticado com encriptação	1. Emparelhamento não autenticado com assinatura de dados 2. Emparelhamento autenticado com assinatura de dados

Tabela 2.1: Tabela com os modos de segurança da tecnologia BLE. Adaptado de [18, 9].

Para além dos métodos de emparelhamento existem ainda diferentes métodos de geração de chaves que podem ser aplicados dependendo das características da aplicação pretendida. Os métodos são os seguintes [18, 9]:

- **Just Works (JW)**: Este método não envolve qualquer interação com o utilizador e apenas estabelece diretamente uma conexão. Este método foi desenvolvido para cenários em que os dispositivos não apresentam qualquer tipo de *input* nem ecrã para introduzir ou apresentar senhas [20]. Assim sendo, este mostra-se um método bastante inseguro. Este fornece segurança contra ataques passivos de espionagem (*passive eavesdropping attack*) [21], que ocorrem quando um espião monitoriza a comunicação entre dois dispositivos, mas não interfere no canal de comunicação. No entanto, não fornece segurança contra ataques Man-in-the-middle (MITM) [21], que é uma forma de ataque em que os dados trocados entre dois dispositivos são de alguma forma intercetados, registados e, possivelmente, alterados pelo atacante sem que as vítimas se apercebam.

- **Passkey Entry**: Este método foi desenvolvido especialmente para cenários em que um dos dispositivos tem um teclado, mas nenhum ecrã, enquanto o outro dispositivo apresenta um ecrã [21]. No entanto, pode ser utilizado perante outras configurações consoante as diferentes capacidades de entrada e saída por parte dos dispositivos. Este método apresenta duas variantes distintas dependendo do método de emparelhamento utilizado. Caso seja utilizado o LE Legacy Pairing, o dispositivo com ecrã exibe um número aleatório de seis dígitos e o utilizador deve inserir através do teclado no outro dispositivo o mesmo número. Caso seja utilizado o LE Secure Connections, existem duas interações possíveis: realizar o mesmo processo que utilizando o LE Legacy Pairing, ou caso nenhum dos dispositivos tenha ecrã, mas ambos tenham teclado, o utilizador pode inserir em ambos os dispositivos a serem conectados a mesma senha de seis dígitos para os emparelhar [18]. A principal desvantagem deste método é que exige que os dispositivos tenham algum tipo de entrada, como um teclado ou um ecrã tátil. Este método fornece proteção contra ataques MITM [22].

- **Out of Band (OOB)**: Este método utiliza um meio externo para descobrir os dispositivos e trocar informações de emparelhamento, como as chaves de encriptação que são usadas no BLE [21]. Um canal comummente utilizado no emparelhamento OOB é o *Near Field Communication* (NFC). O NFC apresenta-se como um canal seguro, pois é uma tecnologia com um alcance extremamente curto, o que faz com que para que exista uma conexão, os dispositivos tenham que estar próximos um do outro, assegurando

que a comunicação é realizada entre os dispositivos corretos. Este método é também resistente a ataques MITM, o que garante que a segurança não é comprometida [20].

- **Numeric Comparison**: Este método é utilizado em cenários onde ambos os dispositivos apresentam ecrã [20]. Neste método existe um número aleatório de seis dígitos a ser apresentando em ambos os dispositivos a serem conectados. Para dar-se a conexão, o utilizador deverá comparar se os dois números são iguais e com base nessa avaliação deverá pressionar, por exemplo, um botão em caso afirmativo ou outro botão em caso negativo, ou uma simples entrada binária como '*yes*' ou '*no*' mediante a situação [21]. Este método apenas funciona com o emparelhamento LE Secure Connections e também garante proteção contra ataques MITM [18].

2.2 Tecnologias e Protocolos de Comunicação sem fios

Para além da tecnologia *Bluetooth*, existem outras tecnologias de comunicação sem fios também utilizadas em sistemas IoT que apresentam características distintas. Estas apresentam diferentes vantagens e desvantagens. Por conseguinte, para além de serem apresentadas as tecnologias Wi-Fi e ZigBee, é realizada uma comparação destas com o *Bluetooth* e o *Bluetooth Low Energy*, de modo a percebermos o peso dos benefícios relativamente às desvantagens apresentadas para cada uma das tecnologias.

2.2.1 Wi-Fi

O Wi-Fi é uma tecnologia de comunicação sem fios desenvolvida pela Wi-Fi Alliance, que pertence ao grupo de padrões IEEE 802.11. Esta tecnologia de comunicação distingue-se das outras tecnologias sem fios, principalmente, pelas elevadas frequências em que transmite. Este protocolo transmite em frequências de 2.4 GHz e 5 GHz, o que faz com que possa transportar mais dados em relação a outras tecnologias que transmitem em frequências inferiores [23]. Em termos de alcance de transmissão, este protocolo tem um alcance máximos de 100 metros e pode atingir uma taxa de transmissão de dados de até 6.75 Gigabits per second (Gbps) [2].

Ao nível das topologias de rede, esta tecnologia suporta topologias em estrela e P2P. Porém, é uma tecnologia de comunicação sem fios que apresenta um elevado consumo de energia, não sendo, portanto, o protocolo mais indicado para sistemas que tenham em conta a eficiência energética. Ao nível da segurança, o Wi-Fi utiliza o protocolo Wi-Fi Protected

Access 2 (WPA2) que usa o algoritmo de encriptação AES [24].

2.2.2 ZigBee

O ZigBee é um protocolo de comunicação sem fios desenvolvido pela ZigBee Alliance baseado no padrão de rádio IEEE 802.15.4. Este foi desenvolvido para ser uma tecnologia mais simples e menos dispendiosa, e é extremamente utilizado na área da IoT para diversas aplicações, especialmente em sistemas de casas inteligentes. O ZigBee é um protocolo de baixo consumo de energia, o que permite um longo tempo útil de vida da bateria dos dispositivos [2].

Esta tecnologia apresenta uma baixa taxa de transmissão dados, na ordem dos 250 Kbps, sendo extremamente eficiente a nível energético. É uma tecnologia com alcance máximo na ordem dos 300 metros e que funciona na banda dos 868-915 MHz e 2.4 GHz para uma topologia *mesh* [25]. Numa topologia *mesh* não existe um ponto central de conexão. Em vez disso, cada nó está conectado a pelo menos um outro nó e geralmente a mais do que um. Cada nó é capaz de enviar e receber mensagens de outros nós. Assim, os nós atuam como retransmissores, passando a informação para o seu destino final. Ao suportar esta topologia, o ZigBee consegue ter um maior alcance dado que os pacotes são enviados através dos vários nós utilizando um mecanismo *multi-hop* [26]. Para além desta topologia, o ZigBee suporta ainda as topologias *tree* e *star*.

Ao nível da segurança, o ZigBee fornece encriptação, autenticação e confidencialidade na transmissão de dados ao utilizar o algoritmo de encriptação AES-CCM. Além disso, esta tecnologia inclui ainda mecanismos de verificação da integridade das mensagens, evitando a alteração dos dados durante a sua transmissão [26].

2.2.3 Comparação entre Tecnologias

Na Tabela 2.2 apresenta-se uma comparação de diversas características técnicas de cada uma das quatro tecnologias de comunicação sem fios apresentadas anteriormente. Na Fig. 2.1 são apresentadas as pilhas dos protocolos de cada uma das tecnologias de comunicação sem fios abordadas.

Tecnologias de comunicação	Bluetooth	BLE	Wi-Fi	ZigBee
Padrão	IEEE 802.15.1	IEEE 802.15.1	IEEE 802.11 a/c/b/d/g/n	IEEE 802.15.4
Alcance de transmissão	<100 m	<100 m	<100 m	<300 m
Frequência de transmissão	2.4 GHz	2.4 GHz	2.4 - 5 GHz	868 - 915 MHz, 2.4 GHz
Taxa de transmissão de dados	1 - 3 Mbps	125 kbps - 2 Mbps	1 Mbps - 6.75 Gbps	250 kbps
Encriptação	AES-128 block cipher	AES-128 block cipher	AES block cipher	AES block cipher
Autenticação	AES-CCM	AES-CCM	WPA2	AES-CCM
Topologia	Piconet, P2P, Broadcast, Mesh	Piconet, P2P, Broadcast, Mesh	Star, P2P	Tree, P2P, Star, Mesh
Consumo de energia	Alto (<30 mA)	Baixo (<15 mA)	Muito alto	Baixo (<16 mA)

Tabela 2.2: Tabela comparativa das diferentes tecnologias de comunicação sem fios. Adaptado de [2].

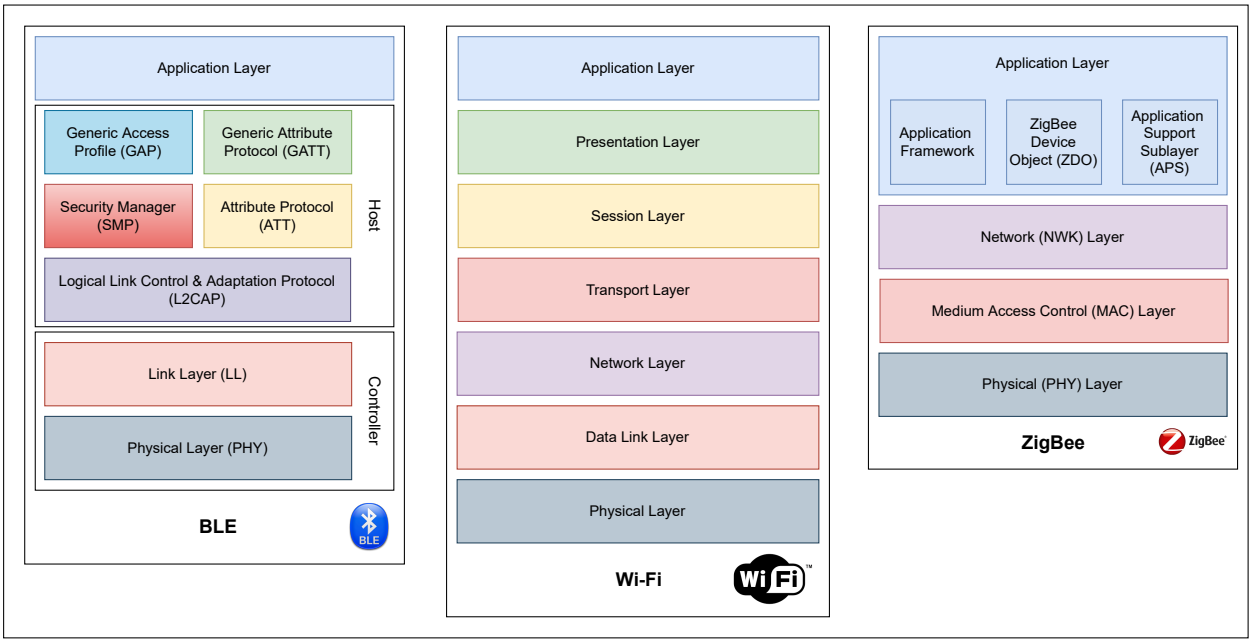

Figura 2.1: Pilhas dos protocolos das diferentes tecnologias de comunicação sem fios. Adaptado de [2].

Através da tabela comparativa apresentada anteriormente é possível concluir que o *Bluetooth Low Energy* mostra-se um candidato adequado no que toca a tecnologias para desenvolver comunicações seguras sem fios em arquiteturas IoT, especialmente relacionadas com a saúde, pois apresenta diversos mecanismos de segurança, tem um limite de transmissão de dados apropriado, baixa latência e reduzido consumo de energia. Assim, com esta tecnologia é possível alcançar um sistema de transmissão e aquisição de dados sem fios eficiente, seguro e de baixo consumo energético.

2.3 Aquisição e Transmissão de Dados via Bluetooth

Esta secção introduz trabalhos relacionados com transmissão e aquisição de dados através de comunicações *Bluetooth*, quer em sistemas ligados aos cuidados de saúde, quer em outro tipo de sistemas. Além disso, é realizada uma pesquisa sobre a segurança utilizada nessas comunicações de modo a perceber o estado da arte atual relativamente ao nível de segurança empregue nestas comunicações. Nesta secção são também apresentados alguns produtos comerciais ligados à área da saúde que utilizam a tecnologia de comunicação sem fios *Bluetooth*. Por fim, conduz-se uma análise comparativa de trabalhos para identificar as principais lacunas encontradas na literatura, permitindo perceber as contribuições que este trabalho pode oferecer com base nessas fragilidades.

2.3.1 Aplicações Gerais

Em [27] é apresentado o projeto de um sistema portátil para aquisição e transmissão de dados atmosféricos a partir de sensores. Este sistema permite medir e analisar diferentes dados recolhidos como temperatura, humidade, pressão ou gases poluentes no ar. Os dados são recolhidos e enviados para dispositivos remotos através de uma conexão *Bluetooth* ou Global System Mobile (GSM)/General Packet Radio Service (GPRS). A solução foi projetada para ser utilizada em sistemas remotos de casas inteligentes e estações de monitorização de ar. O sistema é composto por um *modem* GSM/GPRS com um módulo *Bluetooth* embutido, um cartão micro SIM, um LCD, um alarme e um microcontrolador que faz interface com os sensores utilizados. Relativamente à comunicação, a conexão é assegurada através de um módulo M66F como *modem* GSM/GPRS que suporta interface *Bluetooth*, sendo totalmente compatível com a especificação *Bluetooth* 3.0. O consumo de energia aqui apresentado é bastante baixo, sendo, segundo os autores, de 1.3 mA. Os dados recolhidos através dos sen-

sores são então transmitidos via *Bluetooth* para um servidor remoto com uma base de dados onde os mesmos são armazenados. Conclui-se que o sistema de aquisição de dados proposto mostra-se útil para aplicações IoT dado que segue requisitos como o baixo consumo de energia e as pequenas dimensões do sistema. No entanto, embora os dados aqui transmitidos não sejam tão sensíveis como em casos de cuidados de saúde, não existe qualquer referência por parte dos autores relativamente à implementação de mecanismos de segurança na transmissão.

Os autores de [28] propõem um sistema de aquisição e monitorização de dados em ambiente doméstico baseado na tecnologia BLE. Este sistema tem como principal objetivo recolher dados como a temperatura, humidade ou deteção de movimento, que forneçam informações a uma central de controlo doméstica que permita realizar monitorização remota de dispositivos. A solução é composta por um módulo *Bluetooth* mestre, oito nós *Bluetooth slaves* e um computador que permite o controlo do sistema através de uma Graphical User Interface (GUI). Os módulos BLE utilizados neste trabalho integram funcionalidades como microcontrolador e Analog-to-Digital Converter (ADC) num único módulo. Estes apresentam características como um alcance de transmissão entre os 30 e os 150 metros, dependendo do ambiente. A aquisição de dados é baseada na leitura de entradas ADC. Quando os módulos *Bluetooth* terminam o processo de medição, os dados recolhidos são transmitidos para o módulo mestre que encaminha os mesmos para o computador. Ao nível da segurança, nas comunicações entre os nós foram implementados vários métodos de codificação, como a codificação Manchester. Os autores referem que os próximos passos envolvem a criação de um servidor vinculado à interface do utilizador e o desenvolvimento de uma aplicação para dispositivos móveis para conectar-se ao servidor, onde o utilizador com uma chave de segurança pode aceder aos dados e controlar o sistema.

Em [29] é apresentado um sistema portátil de aquisição de dados microclimáticos agrícolas. O sistema proposto apresenta um desempenho estável, baixo custo e reduzido consumo energético. A solução consiste em três módulos: um terminal de aquisição de dados, uma aplicação de telemóvel Android e uma central de controlo de dados. O terminal de aquisição contém sensores capazes de recolher dados climatéricos como a temperatura e a humidade do ar e do solo, o pH do solo e a pressão atmosférica. Os dados recolhidos são depois enviados para a aplicação Android dos telemóveis via *Bluetooth*. Nesta aplicação ocorre o armazenamento dos dados, análise e processamento dos mesmos, e por fim a exibição dos dados ao utilizador. Para além destas funcionalidades, os dados são ainda enviados para a central de controlo, através de comunicação GPRS, onde os mesmos são monitorizados. O módulo

de aquisição é composto por um microcontrolador STM32F103ZET6, diversos sensores para leitura de dados climatéricos e um módulo de comunicação *Bluetooth*. Para a transmissão dos dados, o sistema utiliza uma comunicação *Bluetooth* através do módulo removível *Bluetooth* HC-05. Sendo um módulo portátil de fácil remoção, quando é necessária a comunicação o utilizador conecta o módulo, e quando não é necessária a transmissão de dados o módulo pode ficar desconectado, poupando dessa forma energia. Relativamente à segurança, os autores não referem qualquer implementação de mecanismos de segurança como encriptação dos dados ou verificação da integridade dos mesmos. É apenas mencionado que os dois dispositivos são emparelhados, sem especificar o nível de segurança deste emparelhamento, e posteriormente os dados transmitidos através da tecnologia *Bluetooth*.

No trabalho desenvolvido em [30] é apresentado um contador elétrico baseado num sistema de aquisição de dados *Bluetooth* tendo em vista a complexidade de cabos e o elevado potencial de erros na aquisição de dados. Desta forma, foi projetado um sistema de aquisição baseado no processador ARM LPC2142, combinado com a tecnologia de comunicação sem fios *Bluetooth* através do módulo Rok101008. Nesta solução realiza-se uma conversão ADC antes de ocorrer a transmissão dos dados. O sinal de entrada que é enviado pelo amplificador do sensor é um sinal analógico e este sinal é enviado para o TLC2543 para ser realizada a conversão ADC. Em seguida, os dados convertidos são enviados para o microprocessador ARM LPC2142. Por último, os dados digitais são transmitidos para o computador através do módulo *Bluetooth*. Assim, o sistema de aquisição de dados do contador elétrico torna-se simples e com elevada mobilidade e praticabilidade. Em termos de segurança, neste trabalho também não são referidos quaisquer implementações de mecanismos de segurança na comunicação *Bluetooth*.

2.3.2 Bluetooth em Aplicações de Cuidados de Saúde

Nesta secção são apresentados trabalhos seminais que utilizam comunicações *Bluetooth* em aplicações ligadas a cuidados de saúde.

De particular relevância para esta dissertação, em [31] é apresentado um estudo sobre a utilização da tecnologia *Bluetooth Low Energy* em sistemas de cuidados de saúde baseados em adesivos eletrónicos. Neste trabalho, os autores referem que a introdução de comunicações sem fios em sistemas de adesivos eletrónicos tornaram estes sistemas mais convenientes para os utilizadores relativamente aos sistemas com fios, isto porque os sistemas com comunicações sem fios permitem uma aplicação mais discreta e confortável para o utilizador. Desta

forma, o uso de tecnologias sem fios como o BLE promove estas características para além de apresentar um baixo consumo de energia, permitindo que os dispositivos comuniquem por largos períodos de tempo. De uma forma geral, embora o *Bluetooth Low Energy* apresente uma taxa de transmissão de dados inferior ao *Bluetooth* clássico, os autores concluem que a utilização da tecnologia BLE em sistemas de cuidados de saúde baseados em adesivos eletrónicos mostra-se crucial para comprimir o volume dos dispositivos e prolongar a vida útil da bateria. Na Fig. 2.2 é possível obter uma visão geral do sistema proposto pelos autores deste trabalho.

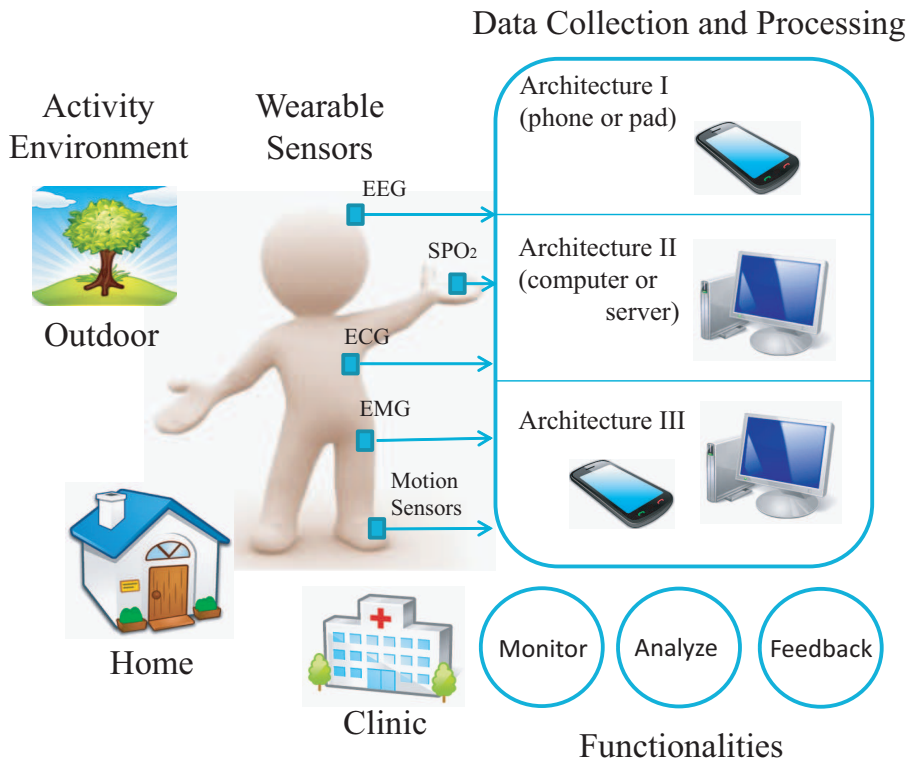

Figura 2.2: Arquitetura do sistema IoT baseado em adesivos eletrónicos apresentado em [31].

No trabalho desenvolvido em [6] é apresentado um adesivo eletrónico proposto para aplicações remotas de assistência médica de longo prazo conectadas à IoT. Estes adesivos eletrónicos são considerados compactos, leves e de baixo consumo energético, o que permite que sejam facilmente conectados ao corpo humano para monitorização de sinais vitais. Estes são compostos por três principais componentes: uma placa central para a aquisição, processamento e transmissão dos sinais vitais; uma placa de alimentação para fornecimento de energia e carregamento de baterias; e três diferentes sensores que permitem medir parâmetros como

Eletrocardiograma (ECG), fotopletismografia[1] (PPG), frequência cardíaca e temperatura corporal. Nestes adesivos é ainda incorporado um módulo *Bluetooth Low Energy* (BLE) de pequenas dimensões, designado Simblee, que permite transmitir sem fios os dados medidos para um IoT *gateway*, que pode ser móvel (*smartphones*) ou fixo (computadores). Tal como referido neste trabalho, nesta transmissão é realizada uma encriptação dos dados, tanto do lado dos adesivos como do *gateway*, de forma a garantir a privacidade e a segurança dos dados durante a transmissão. Para esta encriptação é utilizado o protocolo AES-128. Este é um protocolo que apresenta uma baixa latência e não requer muita memória nem elevados recursos computacionais, pelo que se torna adequado para este tipo de adesivos eletrónicos com recursos limitados. Na Fig. 2.3 é possível obter uma visão geral do sistema proposto pelos autores deste trabalho.

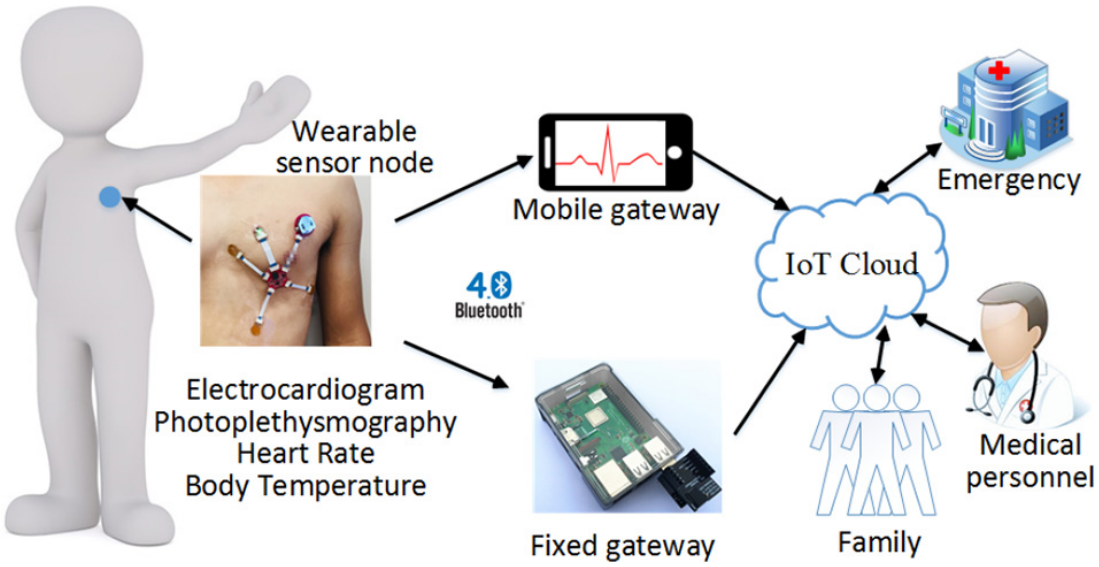

Figura 2.3: Esquema do sistema IoT para aplicação de cuidados de saúde proposto em [6].

Em [5], os autores apresentam um sistema IoT híbrido visando melhorar a segurança nos ambientes de trabalho e reduzir os riscos para a saúde na indústria da construção. A arquitetura IoT proposta incorpora duas principais redes: Wireless Body Area Networks (WBAN) para recolha de dados e Low Power Wide Area Network (LPWAN) para conexão com a Internet. As condições ambientais e os sinais vitais são medidos pelos adesivos eletrónicos implantados na rede WBAN. Os dados são transmitidos através da tecnologia sem fios BLE dentro da WBAN, que são recolhidos e transmitidos para um *gateway* utilizando a tecnologia LoRa dentro da LPWAN. O *gateway* tem como principais objetivos o pré-processamento

[1] A fotopletismografia é uma técnica ótica utilizada na deteção de alterações volumétricas no sangue.

dos sinais dos sensores, a exibição dos dados e disparar alertas caso ocorra alguma emergência. Por último, este sistema incorpora ainda um servidor em nuvem IoT, que é projetado e implementado para armazenamento de dados e outras funcionalidades. Na Fig. 2.4 é apresentada a arquitetura do sistema proposto pelos autores, onde estão representados os três principais subsistemas: os nós dos adesivos eletrónicos, o *gateway* IoT e a *cloud* IoT.

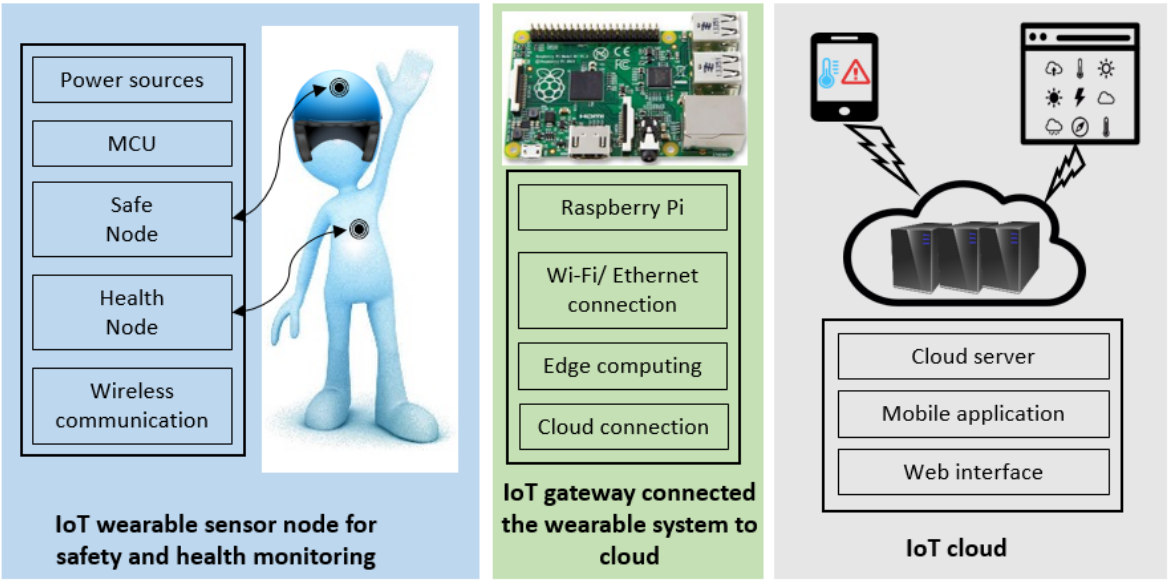

Figura 2.4: Arquitetura do sistema IoT híbrido para monitorização ambiental e de saúde apresentado em [5].

Existem dois nós de adesivos eletrónicos: o *Safe Node*, que é responsável por monitorizar o ambiente, e o *Health Node*, cujo objetivo é medir os sinais vitais dos utilizadores. O *Health Node* é composto por sensores que permitem medir grandezas como a frequência cardíaca e a temperatura corporal, e incorpora ainda um módulo BLE que permite a comunicação WBAN. O *Safe Node* contém sensores que permite medir grandezas climatéricas como a temperatura e a humidade relativa. A tecnologia BLE utilizada neste nó é responsável por receber os dados dos sensores do *Health Node* dentro da WBAN. Embora o BLE apresente uma elevada taxa de transmissão de dados e um baixo consumo de energia, é limitado no alcance de transmissão. Assim, para suprimir esta limitação, foi incorporada a tecnologia LoRa que permite um maior alcance, apesar de aumentar o consumo energético do sistema. Em termos de segurança, apenas é utilizada encriptação na transmissão de dados através da tecnologia LoRa, onde é utilizado o *speck block cipher*. Relativamente à comunicação através da tecnologia BLE não é especificado qualquer tipo de mecanismo de segurança implementado.

Doukas et al. [32] propõem uma arquitetura de um sistema IoT que utiliza adesivos eletrónicos para recolher dados vitais de pacientes em tempo real, recorrendo a uma *cloud* para lidar com todas as necessidades de processamento e armazenamento dos dados. Neste trabalho os autores desenvolveram um protótipo designado de "CloudSensorSock". Este dispositivo é composto por uma placa Arduino equipada com sensores de movimento, sensores vitais e sensores de qualidade de ar (CO_2), módulo *Bluetooth*, módulo Wi-Fi e uma bateria. Este dispositivo comunica com uma aplicação móvel Android através da tecnologia BLE, que atua como um *gateway* para o servidor da *cloud*. Todas as comunicações são consideradas seguras, pois recorrem a mecanismos de segurança como autenticação e encriptação de dados. Nestas comunicações, os sensores são autenticados com um ID exclusivo e os dados são encriptados utilizando o algoritmo de criptografia simétrica Advanced Encryption Standard (AES). Os utilizadores e aplicações externas podem ser autenticados utilizando mecanismos de segurança mais sofisticados como as assinaturas digitais (*digital signatures*). Na Fig. 2.5 é apresentada a arquitetura do sistema IoT proposto pelos autores deste trabalho.

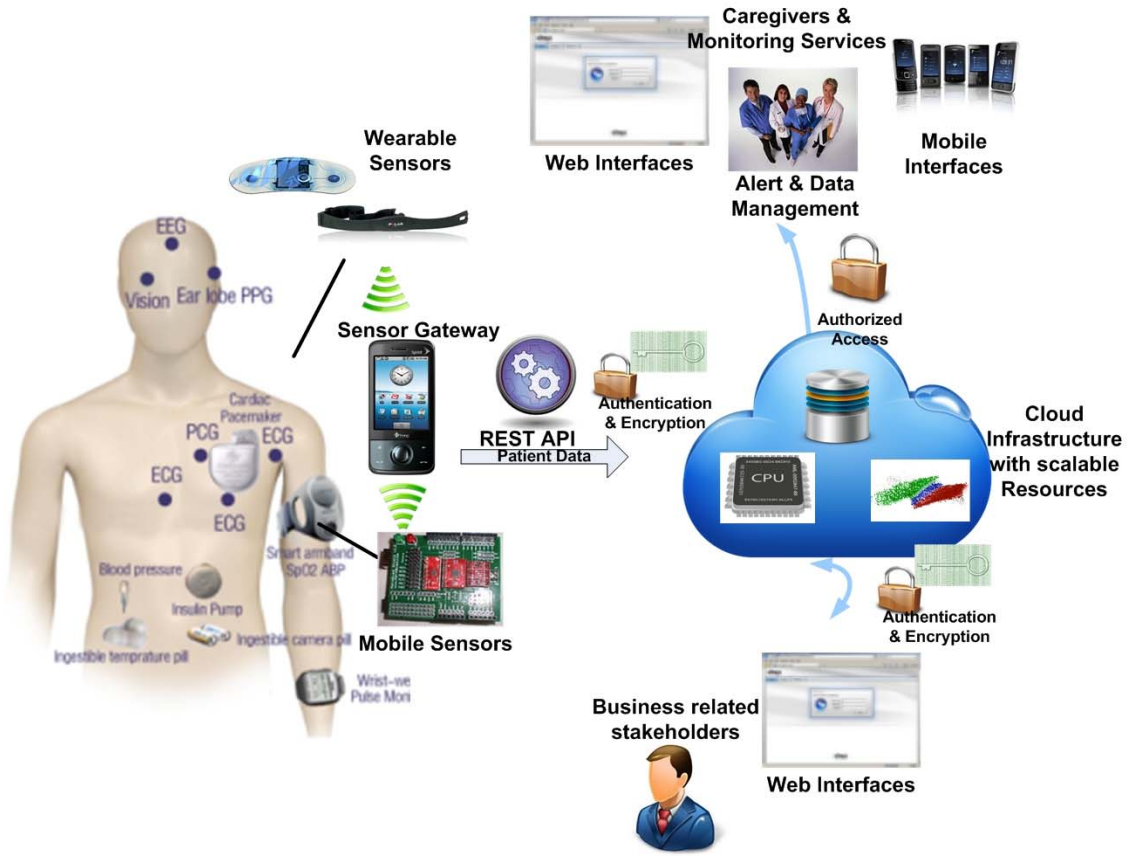

Figura 2.5: Arquitetura IoT proposta em [32] para sistema de cuidados de saúde.

2.3.3 Produtos Comerciais na Área da Saúde que utilizam a Tecnologia Bluetooth

Existem diversos produtos comerciais para cuidados de saúde que utilizam a tecnologia BLE, uma vez que várias empresas exploram ativamente a evolução tecnológica na área da saúde nos últimos anos. De seguida, apresentam-se três produtos comerciais relevantes de diferentes empresas.

Começando pelo BPM Core da empresa Withings [33], este consiste num monitor de pressão arterial inteligente que tem como principal objetivo a deteção de problemas cardíacos silenciosos. Este é considerado um dispositivo 3 em 1, pois permite com apenas uma execução examinar três diferentes métricas: a pressão arterial sistólica e diastólica, procurando prever a hipertensão; a frequência cardíaca através de um eletrocardiograma (ECG), permitindo detetar qualquer tipo de arritmia cardíaca; e uma deteção de valvulopatias com base na leitura de um preciso estetoscópio digital embutido no aparelho. Este produto utiliza a tecnologia de comunicação BLE para sincronização com uma aplicação denominada Withings Health Mate, que permite ao utilizador aceder aos seus dados no *smartphone* e ainda compartilhar os mesmos com o seu médico, evitando assim ter de se deslocar ao hospital, realizando uma monitorização domiciliar da sua pressão arterial. Ao nível da comunicação BLE, não são mencionados quaisquer mecanismos de segurança. A principal desvantagem deste produto prende-se no custo do mesmo, em torno de 300€. Este deve-se principalmente às funcionalidades extras apresentadas pelo dispositivo para além da monitorização básica da pressão arterial.

Outro produto comercial é o Polar H10 da empresa Polar [34], que foi desenvolvido para medir e monitorizar a frequência cardíaca durante a prática de atividades físicas, oferecendo informações úteis para atletas de alto rendimento e pessoas interessadas em controlar a sua saúde cardiovascular. Este produto utiliza um sensor composto por elétrodos que é capaz de realizar leituras precisas da frequência cardíaca dos utilizadores. O sensor é colocado dentro de uma alça para garantir o máximo conforto ao utilizador, e dentro de uma firme fivela para assegurar o máximo contacto com a pele, bloqueando qualquer interferência que o movimento implique, medindo de forma precisa a frequência cardíaca. Ao nível da conectividade, o Polar H10 utiliza a tecnologia *Bluetooth* para transmitir os dados lidos pelo sensor a diversos tipos de dispositivos, como *smartphones* ou *smartwatches*, e ainda conectar a uma enorme diversidade de aplicações de desporto, como a Polar Beat, Strava ou Nike Run Club. No que diz respeito à segurança nesta comunicação, a empresa Polar afirma que utiliza

medidas de segurança técnicas e organizacionais adequadas, como encriptação, protegendo a confidencialidade e a integridade dos dados trocados entre os dispositivos, impedindo o acesso não autorizado e o uso indevido dos dados pessoais dos utilizadores.

O modelo 3230 da empresa Nonin [35] é um oxímetro de pulso leve, pequeno e portátil. Este produto é indicado para a medição e monitorização da saturação de oxigénio no sangue (SpO_2) e da frequência de pulsação de pacientes. Este oxímetro permite a gestão da condição de pacientes, fornecendo medições rápidas, precisas, em tempo real e não invasivas de oxigénio, a fim de satisfazer as necessidades clínicas dos pacientes. Este é um aparelho que possui conectividade *Bluetooth* segura para a troca de informações vitais entre o oxímetro de pulso e outros dispositivos compatíveis, como *smartphones*, *tablets* ou sistemas de monitorização médica. Assim, os profissionais de saúde podem monitorizar estes dados remotamente e tomar decisões sobre cuidados a ter com base nas medições realizadas pelos pacientes no seu domicílio. A tecnologia *Bluetooth* utilizada neste produto comercial é a versão 4.0 de baixo consumo energético (BLE). Nesta comunicação são impostos mecanismos de segurança como encriptação e autenticação, sendo utilizadas chaves de encriptação de 128 bits AES. Com a utilização desta tecnologia de comunicação sem fios de baixo consumo de energia, este produto mostra-se eficiente a nível energético, poupando a vida útil da bateria do dispositivo, e seguro, pois utiliza encriptação e autenticação nas comunicações.

2.3.4 Fragilidades Tipicamente Encontradas na Literatura

Como é possível concluir a partir da revisão da literatura apresentada anteriormente, um dos principais fatores não abordados nestes trabalhos é o nível de segurança imposto nas comunicações. Na maioria dos trabalhos revistos, os autores não fazem qualquer referência a mecanismos de segurança implementados, fazendo com que o leitor não tenha nenhuma perceção do nível de segurança do sistema proposto. Nos poucos trabalhos em que é abordado de alguma forma o tema da segurança, não o é realizado de forma profunda, sendo que os autores apenas referem que existe algum mecanismo de segurança implementando, não mencionando quais os protocolos utilizados ou o procedimento da implementação desses mesmos mecanismos. Na Tabela 2.3 é apresentada uma análise comparativa entre os diferentes trabalhos abordados anteriormente.

Assim, como a segurança e a privacidade são dois dos principais requisitos destes sistemas IoT, esta dissertação procura abordar primordialmente a segurança nestas comunicações, procurando suprimir estas lacunas encontradas na literatura.

Trabalhos	Ano	Aplicação	Tipo de dados adquiridos	Tecnologias de comunicação sem fios	Características de Segurança
Xuange et al. [30]	2010	Contador elétrico baseado num sistema de aquisição de dados	Energia consumida	Bluetooth	Desconhecido
Doukas et al. [32]	2012	Sistema IoT de cuidados de saúde baseados em adesivos eletrónicos	Temperatura Corporal, Frequência Cardíaca, Sensores de movimento, Sensores CO_2	BLE, Wi-Fi, GPRS/3G	AES
Zhang et al. [31]	2014	Sistema IoT de cuidados de saúde baseado em adesivos eletrónicos	Sinais de movimento, Eletroencefalograma (EEG), Eletrocardiograma (ECG), Eletromiografia (EMG), Saturação de Oxigénio	BLE	Desconhecido
Chen et al. [28]	2015	Sistema de aquisição e monitorização de dados em ambientes domésticos	Temperatura, Humidade, Sinais de movimento	BLE	Codificação Manchester
Gao et al. [29]	2015	Sistema portátil de aquisição de dados microclimáticos agrícolas	Temperatura do ar e solo, pH do solo, Humidade do ar e solo, Pressão Atmosférica	Bluetooth	Desconhecido
Yordanov et al. [27]	2017	Sistema portátil para aquisição e transmissão de dados atmosféricos medidos por sensores	Temperatura, Humidade, Pressão Atmosférica, Gases poluentes no ar	Bluetooth, GSM/GPRS	Desconhecido
Wu et al. [5]	2019	Sistema IoT híbrido para monitorização da segurança e saúde no trabalho	Frequência Cardíaca, Temperatura Corporal, Temperatura e Humidade do ar	BLE, LoRa	Speck Cipher
Wu et al. [6]	2020	Sistema IoT de cuidados de saúde baseado em adesivos eletrónicos	Eletrocardiograma (ECG), Fotopletismografia (PPG), Frequência Cardíaca, Temperatura Corporal	BLE	AES-128

Tabela 2.3: Comparação entre os diferentes trabalhos estudados.

2.4 Declaração das Contribuições

Motivado pelos desafios do projeto WoW, no qual esta dissertação encontra-se inserida, este trabalho procura garantir a segurança e a integridade dos sinais vitais transmitidos através da comunicação BLE com vista à biomonitorização sem fios de pacientes rumo à internação domiciliar.

Com isto em mente, na sequência da revisão da literatura apresentada anteriormente e do levantamento das suas maiores fragilidades, no âmbito desta dissertação são propostas as seguintes contribuições:

- Materializar a arquitetura de transmissão BLE segura sem fios de dados vitais (ver

Capítulo 3), consolidando a transmissão e aquisição dos dados.

- Implementar mecanismos de segurança como encriptação e autenticação na comunicação BLE sem fios, aumentando a robustez do sistema contra ciberataques.
- Implementar emparelhamento físico com NFC, aplicando o método de emparelhamento mais seguro da tecnologia BLE, ou seja, emparelhamento LE Secure Connections com OOB (Modo 1 Nível 4).
- Validar experimentalmente os mecanismos de segurança implementados.
- Conduzir um estudo comparativo de desempenho entre a comunicação segura e a comunicação não segura, através da realização de diversos testes experimentais com diferentes configurações de segurança.

2.5 Sumário

Neste capítulo foram analisados diversos trabalhos da literatura relacionados com a transmissão e aquisição de dados, tendo em vista primordialmente sistemas na área da saúde, procurando constatar os principais benefícios e desafios da digitalização desta área, especialmente com foco na segurança e na privacidade dos dados envolvidos. Este trabalho de pesquisa serviu também como orientação para o desenvolvimento da nossa implementação neste trabalho.

No próximo capítulo é apresentada a arquitetura proposta para a transmissão e aquisição de dados via BLE, bem como todos os componentes envolvidos na mesma. De seguida é descrita a implementação dos mecanismos de segurança empregues neste sistema.

3 Metodologia

Neste capítulo é apresentada a metodologia seguida no desenvolvimento do trabalho desta dissertação, incluindo todas as ferramentas e métodos utilizados na implementação. Aqui é também apresentada a arquitetura do sistema desenvolvida para a implementação da transmissão BLE segura dos dados entre os dispositivos.

3.1 Arquitetura do Sistema

Esta dissertação foca-se na transmissão e aquisição de sinais vitais de pacientes através de uma comunicação BLE segura. Com o intuito de realizar a transmissão e aquisição dos dados são necessários dois dispositivos que suportem o emparelhamento e transmissão através da tecnologia de comunicação sem fios BLE. Para assegurar a transmissão dos dados entre os dispositivos são utilizados protocolos desta tecnologia de comunicação que são responsáveis pela gestão da conexão e da troca de dados. Para atender às necessidades de segurança do sistema, é utilizado outro protocolo da tecnologia BLE que lida objetivamente com o emparelhamento e a segurança da comunicação BLE estabelecida. Para validação das implementações desenvolvidas neste trabalho é utilizado um terceiro dispositivo que permite a visualização dos pacotes transmitidos durante a comunicação.

Na Fig. 3.1 ilustra-se a arquitetura proposta para a implementação da transmissão e aquisição segura dos dados. Como podemos verificar na figura estão presentes os dois dispositivos envolvidos na comunicação, o dispositivo emissor (nRF52 DK) e o dispositivo recetor (módulo de aquisição). Aqui estão também presentes os protocolos da tecnologia BLE utilizados tanto para o desenvolvimento da transmissão e aquisição de dados como dos mecanismos de segurança. Nesta arquitetura é ainda possível observar o terceiro dispositivo com a função de escuta dos pacotes BLE transmitidos.

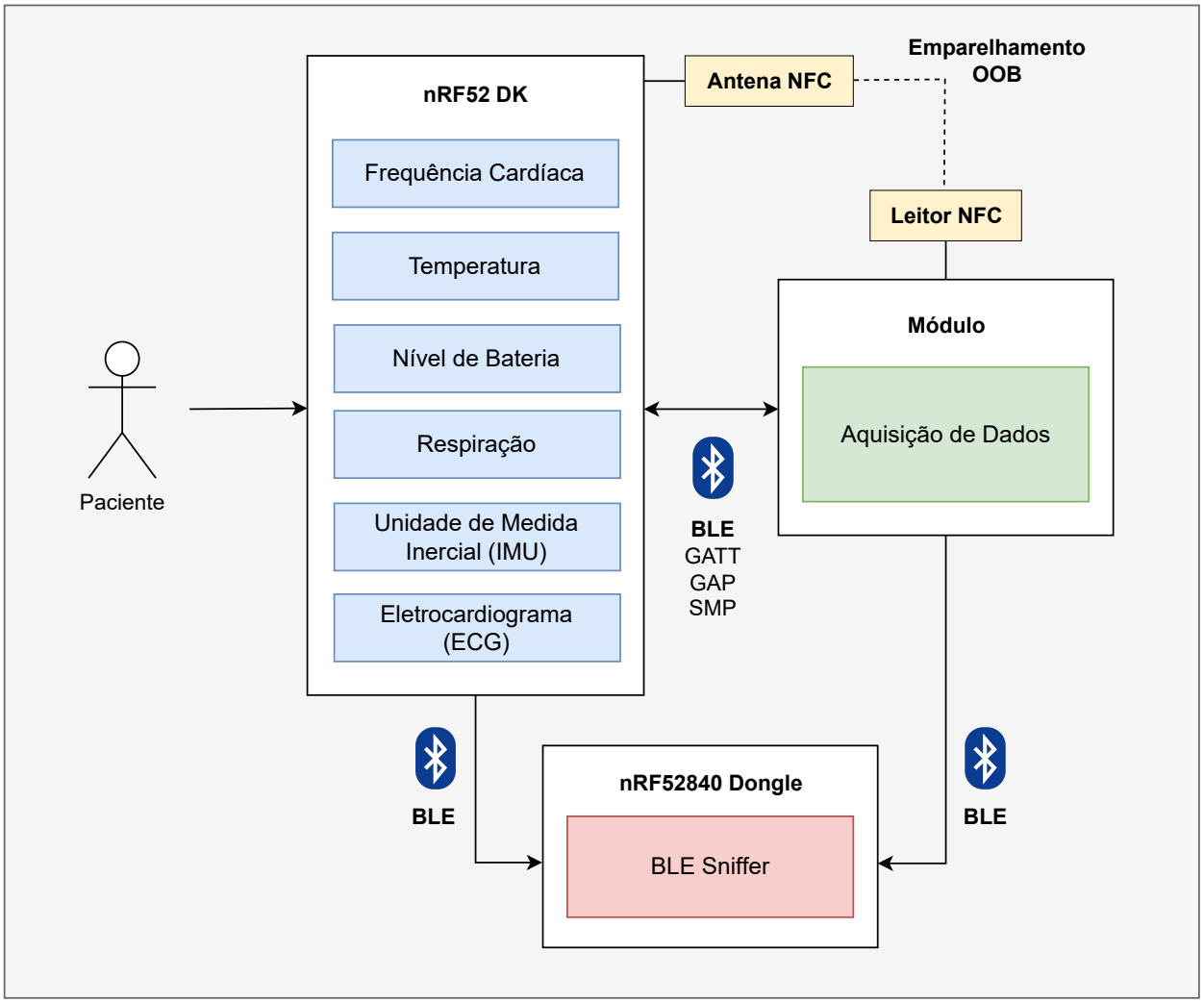

Figura 3.1: Arquitetura de transmissão BLE segura proposta para o desenvolvimento desta dissertação. No contexto deste trabalho, o módulo de aquisição de dados pode variar entre um *smartphone*, Raspberry Pi ou nRF52 DK.

3.2 Componentes do Sistema

Com base na arquitetura de transmissão BLE apresentada na Fig. 3.1, para o desenvolvimento deste trabalho são utilizados primordialmente dois componentes: kit de desenvolvimento nRF52 DK[2] da Nordic Semiconductor[3], onde é desenvolvido o *firmware* para a comunicação BLE entre os componentes, e nRF52840 Dongle[4], também da Nordic Semiconductor, para ser utilizado como BLE *sniffer* (módulo de escuta).

Nas secções seguintes são apresentados cada um destes componentes, incluindo as suas

[2]nRF52 DK, `https://www.nordicsemi.com/Products/Development-hardware/nrf52-dk`

[3]Nordic Semiconductor, `https://www.nordicsemi.com`

[4]nRF52840 Dongle, `https://www.nordicsemi.com/Products/Development-hardware/nrf52840-dongle`

principais vantagens e características, culminando numa justificação pela decisão da utilização destes componentes em específico.

3.2.1 Kit de Desenvolvimento nRF52 DK

Para o desenvolvimento do *firmware* relativo à transmissão de dados foi escolhido o kit de desenvolvimento nRF52 DK, pois este é uma plataforma versátil e poderosa para o desenvolvimento de aplicações que utilizem Bluetooth Low Energy (BLE). Esta é também a placa utilizada nos *biostickers* (adesivos eletrónicos) do projeto WoW. Este kit apresenta diversas características, entre as quais se destacam:

- **Processador de alto desempenho**: O processador ARM Cortex M4 fornece um elevado desempenho e um baixo consumo de energia ao sistema desenvolvido com este *hardware*;
- **Suporte à conectividade BLE**: Este kit está desenhado para o desenvolvimento de aplicações sem fios BLE, como os dispositivos vestíveis utilizados no projeto WoW;
- **Baixo consumo energético**: O kit apresenta um baixo consumo de energia, sendo apropriado para aplicações com dispositivos alimentados por bateria (como os dispositivos vestíveis);
- **Ampla gama de interfaces**: Este kit inclui diversas interfaces como USB, SPI, I2C, UART e GPIO, facilitando a conexão com sensores e outros dispositivos como pretendido neste trabalho.

Como visto em cima, a nRF52 DK apresenta-se como uma plataforma ideal para aplicações BLE devido à sua aptidão para desenvolver soluções restritas ao nível do consumo energético e da conectividade sem fios. Na Fig. 3.2 é possível visualizar a placa nRF52 DK e a sua antena NFC.

O sistema operativo selecionado inicialmente para o desenvolvimento deste trabalho foi o MbedOS[5]. Este foi escolhido dado que se encontrava em utilização anteriormente na comunicação BLE entre os dispositivos **de forma não segura**. Assim, com o intuito de facilitar a integração do trabalho desenvolvido no restante projeto, foi escolhido o mesmo sistema operativo. No entanto, após uma análise cuidada e exaustiva das camadas de segurança pretendidas, foi possível concluir que as versões mais recentes do sistema operativo MbedOS

[5]MbedOS, `https://os.mbed.com/mbed-os/`

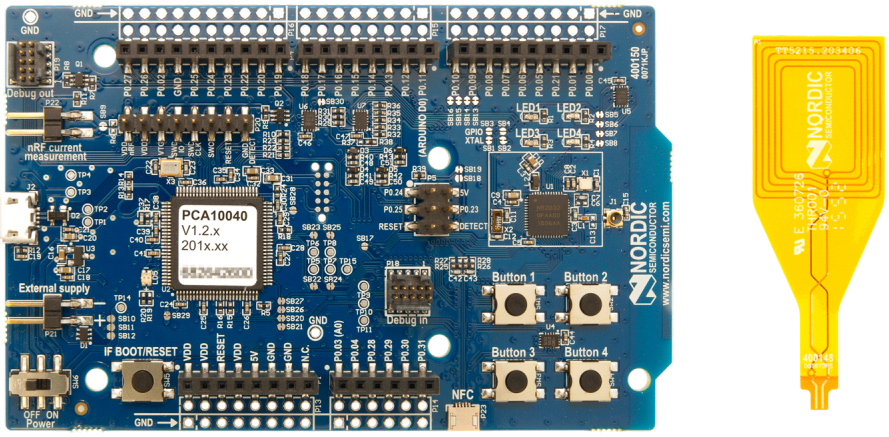

Figura 3.2: Kit de desenvolvimento nRF52 DK (à esquerda) e antena NFC (à direita).

não suportam o método de emparelhamento LE Secure Connections da tecnologia BLE[6] que é alvo neste trabalho.

Com vista à resolução deste problema, após investigação adicional, as possíveis soluções encontradas foram a utilização de uma versão anterior do sistema operativo MbedOS que suportasse emparelhamento LE Secure Connections ou a alteração para um sistema operativo mais recente. Considerando a falta de suporte e antiguidade da versão 5.12 do MbedOS lançada em 2019, foi tomada a decisão de alterar o sistema operativo utilizado. Assim sendo, o sistema operativo escolhido para o desenvolvimento do *firmware* pretendido foi o Zephyr[7]. O principal fator pela qual o Zephyr foi o sistema operativo selecionado prende-se com o facto deste ser o único e mais recente sistema operativo ativamente suportado pela empresa Nordic Semiconductor, que fabrica os kits de desenvolvimento utilizados neste trabalho.

O Zephyr é um *Real Time Operating System (RTOS)* seguro, escalonável e de código aberto, projetado para dispositivos embebidos com recursos limitados [36]. Algumas das principais características do sistema operativo Zephyr são as seguintes:

- **Escalável**: O Zephyr foi projetado para suportar uma ampla gama de dispositivos e arquiteturas de processador, desde microcontroladores com recursos limitados até dispositivos mais robustos;
- **Segurança**: Este sistema operativo inclui uma variedade de recursos de segurança, tais como criptografia e autenticação, facilitando a criação de sistemas seguros e de elevada confiabilidade;

[6]No Apêndice A deste trabalho apresenta-se o código do sistema operativo que suporta esta conclusão.
[7]Zephyr, `https://www.zephyrproject.org/`

- **Conectividade**: O Zephyr inclui suporte para uma variedade de tecnologias de comunicação sem fios, incluindo BLE, Wi-Fi e LoRaWAN, facilitando a conexão entre dispositivos e/ou com a *cloud*;
- **Tempo Real**: O Zephyr inclui um RTOS leve e eficiente que é capaz de responder a eventos e tarefas em tempo real, facilitando a criação de sistemas responsivos e determinísticos.

Na Tabela 3.1 apresenta-se uma comparação das características e recursos dos sistemas operativos de IoT Zephyr e Mbed OS.

Sistema Operativo	**Mbed OS**	**Zephyr**
Ano da 1ª Versão	2009	2016
Arquitetura	Monolítico	Microkernel
Escalonador	Preemptivo	Preemptivo, Não-preemptivo, Baseado em prioridade
Modelo de Programação	Multithreading	Multithreading
Linguagem de Programação	C C++	C
Arquiteturas de Processador	ARM	ARM, Intel x86, ARC, RISC-V
RAM	∼5 kB	∼2 kB a ∼8 kB
ROM	∼15 kB	∼50 kB
Suporte LESC	Não	Sim

Tabela 3.1: Comparação entre sistemas operativos Zephyr e Mbed OS. Adaptado de [37].

Analisando a tabela comparativa anterior, é possível concluir que o sistema operativo Zephyr apresenta uma arquitetura microkernel, o que fornece uma maior flexibilidade ao sistema [38]. Apresenta também uma enorme diversidade ao nível do escalonamento, suportando um modelo de programação *multithreading* com um escalonador preemptivo, não-preemptivo ou baseado em prioridades [36]. No que diz respeito às linguagens de programação, o MbedOS suporta as linguagens C e C++, enquanto o Zephyr é mais restrito e

apenas suporta a linguagem C. Relativamente à memória, é possível concluir que o Zephyr apresenta maior capacidade tanto ao nível da Random Access Memory (RAM) como da Read Only Memory (ROM) relativamente ao Mbed OS, o que permite desenvolver aplicações mais sofisticadas com conectividade segura e protocolos mais avançados [37]. Uma das grandes vantagens do sistema operativo Zephyr recai sobre o facto deste suportar diversas arquiteturas de processadores como ARM, Intel x86, ARC ou RISC-V, enquanto o Mbed OS foi projetado apenas para arquiteturas ARM [36, 37].

No cômputo geral, o Zephyr é um sistema operativo que fornece aos desenvolvedores uma plataforma flexível e segura para a criação de aplicações com foco em conectividade, segurança e desempenho em tempo real.

3.2.2 nRF52840 Dongle

Com o intuito de testar a segurança da comunicação BLE, é utilizado um BLE *sniffer* para escutar os pacotes BLE trocados entre os dispositivos. O BLE *sniffer* adotado foi o nRF *Sniffer*[8], sendo este desenvolvido pela mesma empresa que o *hardware* utilizado neste trabalho (Nordic Semiconductor). O *software* nRF *Sniffer* para BLE consiste num *firmware* programado num kit de desenvolvimento (DK) ou dongle e num *plugin* de captura para o *software* Wireshark[9] que regista e analisa os dados detetados.

A placa escolhida para esta função foi a nRF52840 Dongle. Esta Dongle é uma plataforma de desenvolvimento pequena e de baixo custo baseada na nRF52840 System-on-Chip (SoC). Esta foi a plataforma escolhida dado que é também desenvolvida pela Nordic Semiconductor e apresenta as seguintes três principais características:

- **Conectividade BLE**: A Dongle nRF52840 oferece suporte à conectividade BLE, tornando-a ideal para a escuta de pacotes desta tecnologia de comunicação sem fios;
- **Baixo consumo de energia**: A Dongle foi projetada para consumir pouca energia, tornando-a ideal para o desenvolvimento de dispositivos cuja bateria deve ser poupada;
- **Pequena dimensão**: A Dongle nRF52840 é pequena e compacta, facilitando a criação de protótipos e testes de aplicações sem ocupar muito espaço físico.

[8] nRF Sniffer, `https://www.nordicsemi.com/Products/Development-tools/nrf-sniffer-for-bluetooth-le`

[9] Wireshark, `https://www.wireshark.org/`

Assim sendo, a Dongle nRF52840 fornece aos desenvolvedores uma plataforma versátil e de baixo custo para o desenvolvimento de aplicações BLE, procurando ocupar o mínimo espaço possível nesses protótipos, sendo bastante útil para pequenos testes como a funcionalidade de BLE *sniffer*. Na Fig. 3.3 é possível visualizar a nRF52840 Dongle.

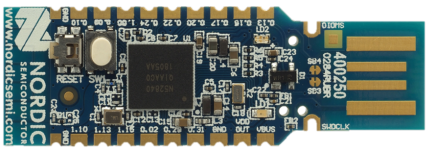

Figura 3.3: nRF52840 Dongle.

3.3 Comunicação BLE

Para assegurar a transmissão e aquisição dos dados vitais dos pacientes é essencial configurar a comunicação entre os componentes do sistema descritos anteriormente. Assim, como concluído no Capítulo 2, com base na análise da literatura, nesta dissertação será utilizada a tecnologia de comunicação sem fios *Bluetooth Low Energy* (BLE). Nesta secção será então abordada a implementação da comunicação entre os dispositivos envolvidos utilizando a tecnologia BLE.

Para o desenvolvimento da transmissão e aquisição de dados foi utilizado o protocolo Generic ATTribute Profile (GATT) da pilha da tecnologia de comunicação sem fios BLE, que é possível visualizar na Fig. 2.1. Este é o protocolo responsável por definir a forma como os dados são transmitidos entre dispositivos BLE. Assim, como qualquer outro protocolo ou perfil na especificação do *Bluetooth*, o GATT começa por definir as funções que os dispositivos que interagem podem adotar. Ao definir estas funções, o protocolo GATT facilita o desenvolvimento de comunicações BLE eficientes e padronizadas. Os papéis que os dispositivos podem adotar são então os seguintes [22]:

- **Servidor GATT**: Responsável por armazenar dados e responder a solicitações de clientes GATT. Caso a solicitação seja de leitura, o servidor é responsável por disponibilizar os dados solicitados ao cliente, caso a solicitação seja de escrita, o servidor recebe os dados do cliente e é responsável por os gravar. O servidor pode ainda enviar notificações ou indicações ao cliente para indicar uma modificação nos dados.

- **Cliente GATT**: Responsável por enviar solicitações ao servidor GATT. O cliente

envia solicitações de leitura ou escrita ao servidor e recebe notificações ou indicações do servidor.

O protocolo GATT utiliza o Attribute Protocol (ATT) como protocolo de transporte para trocar dados entre dispositivos através de uma conexão BLE. O ATT é o protocolo de baixo nível que define a representação dos dados que são transferidos entre dispositivos BLE através de estruturas de dados denominadas atributos. Na Fig. 3.4 é possível observar a estrutura de um atributo. Por definição, os atributos são compostos por quatro diferentes campos [15, 22]:

- **Tipo**: Corresponde a um Universally Unique Identifier (UUID) e identifica o tipo de dados que são armazenados no valor do atributo. Por exemplo, o UUID "0x2A1C" corresponde a um valor de um atributo de medição de temperatura adotado pela especificação do *Bluetooth*.
- **Identificador (*Handle*)**: Funciona como um endereço e identifica exclusivamente o atributo dentro do servidor GATT, permitindo que os clientes o utilizem para consultar um atributo específico na tabela de atributos do servidor. Este identificador varia entre "0x0001" e "0xFFFF".
- **Permissões**: As permissões definem o tipo de interações que são possíveis ter com esse atributo. Estas determinam se um atributo pode ser **lido**, **escrito**, **notificado** ou **indicado**. Nestas permissões podem ainda ser adicionados requisitos de segurança, como encriptação ou autenticação, para aceder aos atributos.
- **Valor**: Valor armazenado no atributo.

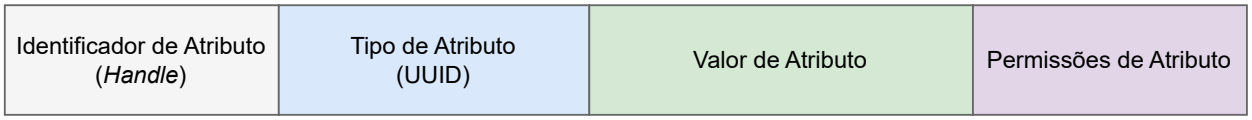

Figura 3.4: Representação de um atributo na tabela de atributos do servidor. Adaptado de [15].

Com base nos atributos armazenados na tabela de atributos, o protocolo GATT define tipos de dados de alto nível que produzem uma hierarquização na estruturação dos dados expostos pelo servidor GATT. Os tipos de dados existentes são os seguintes [15]:

- **Serviços**: Os serviços GATT agrupam um ou mais atributos, alguns dos quais características, conceitualmente relacionados numa secção comum, que permitem satisfazer uma funcionalidade específica no servidor GATT.

- **Características**: As características fazem parte de um serviço e representam itens individuais de dados que possuem um tipo, um valor associado e um conjunto de propriedades que indicam como esses dados podem ser utilizados. Adicionalmente, uma característica pode ainda conter descritores associados.

- **Descritores**: Os descritores de características do GATT são utilizados principalmente para fornecer ao cliente informações adicionais sobre a característica em questão, como, por exemplo, uma descrição textual sobre a mesma.

Na Fig. 3.5 é possível visualizar a estrutura de um servidor GATT para um serviço de medição de frequência cardíaca, onde está presente um serviço e duas diferentes características, onde a primeira apresenta adicionalmente um descritor.

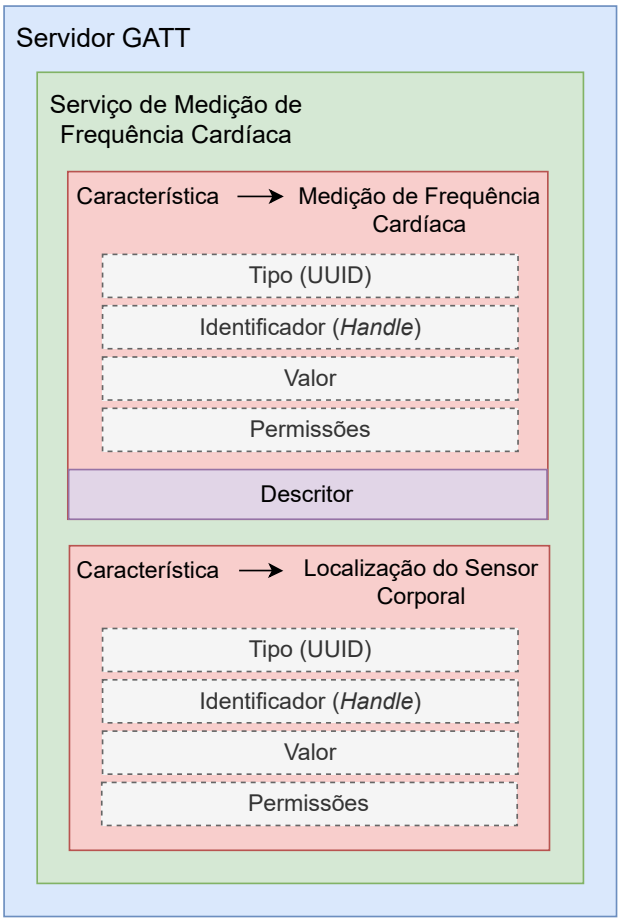

Figura 3.5: Estrutura de servidor GATT para serviço de medição de frequência cardíaca. Adaptado de [13].

Como o foco desta dissertação é a transmissão e aquisição de sinais vitais de pacientes, na implementação deste trabalho foi necessário desenvolver um servidor GATT personalizado, onde se armazenam os dados vitais dos pacientes medidos através de sensores conectados ao kit de desenvolvimento, e um cliente GATT, cujo objetivo prende-se na conexão ao servidor GATT e posterior realização da aquisição dos dados vitais dos pacientes transmitidos através desta comunicação.

No desenvolvimento do servidor foi definido apenas um serviço GATT que contém sete diferentes características. Estas correspondem ao nível da bateria em percentagem do dispositivo, temperatura corporal, frequência cardíaca, respiração, eletrocardiograma (ECG) e Unidade de Medida Inercial ou Inertial Measurement Unit (IMU). A cada sinal corresponde uma característica, com exceção da respiração, que apresenta duas características para o mesmo sinal. Isto deve-se à existência de dois sensores para leitura da respiração em diferentes pontos do corpo, um na zona da caixa torácica e outro na zona da barriga/umbigo, sendo dessa forma definida uma característica para cada um dos valores medidos com os diferentes sensores.

A estas características foram adicionados descritores e permissões de leitura e notificação para interação por parte do cliente GATT que se conecta ao servidor. As permissões de notificação foram definidas, pois estas permitem poupar tempo, largura de banda e energia, uma vez que uma leitura num momento em que os dados não foram ainda alterados provoca um consumo energético e um gasto de largura de banda e tempo desnecessário para efetuar a transmissão. Com estas permissões, o cliente consegue fazer leituras individuais do valor de cada uma das características ou ativar as notificações, fazendo com que o servidor notifique o cliente sempre que o valor da característica sofre uma alteração.

Para o desenvolvimento do cliente GATT foi utilizada a biblioteca GATT Discovery Manager[10], que lida com a descoberta de serviços em servidores GATT e simplifica a tarefa. Esta descoberta é necessária para que o cliente descubra todos os serviços e características do servidor e possa interagir com as mesmas. Após a descoberta de todas as características do servidor GATT desenvolvido, o cliente subscreve as características sobre as quais pretende receber notificações e a partir desse momento fica recetivo à aquisição dos valores transmitidos através dessas características.

As características definidas no servidor GATT apresentam ainda diferentes taxas de atualização dos seus valores através de leituras dos sensores em determinados períodos de

[10]GATT Discovery Manager, `https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/nrf/libraries/bluetooth_services/gatt_dm.html`

tempo definidos, pelo que o cliente será notificado com uma nova mensagem do novo valor da característica por parte do servidor sempre que este intervalo de tempo seja alcançado e o cliente tenha ativado devidamente as notificações. Na Tabela 3.2 é possível observar um breve sumário das principais informações relativas a cada característica do servidor GATT implementado.

Característica	**Característica UUID**	**Tipo de dados**	**Permissões**	**Taxa de atualização (ms)**	**Intervalo de valores**
Frequência Cardíaca	0x2A37	Inteiro de 16 Bits	Leitura Notificação	5000	[40, 160]
Temperatura Corporal	0x2A1C	Byte para definição de escala, Float no formato IEEE 11073	Leitura Notificação	60000	[30, 40]
Nível de Bateria	0x2A19	Inteiro de 32 Bits	Leitura Notificação	10000	[0, 100]
Respiração 1	0xA002	Inteiro de 16 Bits	Leitura Notificação	100	[-32,768; 32,767]
Respiração 2	0xA008	Inteiro de 16 Bits	Leitura Notificação	100	[-32,768, 32,767]
ECG	0xA003	Array de 32 Bytes	Leitura Notificação	250	[0, 10]
IMU	0xA004	Array de 6 Floats (Acelerómetro e Giroscópio de 3 eixos cada)	Leitura Notificação	50	[0, 10]

Tabela 3.2: Sumário do servidor GATT personalizado desenvolvido neste trabalho.

3.4 Segurança na Comunicação

Para implementar os mecanismos de segurança na comunicação entre os dispositivos foram utilizados os protocolos Generic Access Profile (GAP) e Security Manager Protocol (SMP) da tecnologia BLE (ver Fig. 2.1).

O Generic Access Profile (GAP) é o protocolo responsável por definir como os dispositivos BLE interagem entre si, isto é, como se descobrem, como se conectam, como transmitem dados, como gerem as suas conexões e como executam muitas outras operações fundamentais de uma forma padrão e universalmente compreendida. O GAP define ainda o formato e o conteúdo dos pacotes de anúncio (*advertising packets*), que podem conter informações como

o nome do dispositivo, serviços oferecidos e parâmetros de conexão. O protocolo GAP define quatro funções que um dispositivo pode desempenhar numa rede BLE, permitindo uma maneira flexível e eficiente de comunicação entre dispositivos BLE:

- **Broadcaster**: Este dispositivo envia pacotes de anúncio em intervalos regulares para publicitar a sua presença e tornar-se detetável por outros dispositivos BLE.
- **Observador**: Este dispositivo procura pacotes de anúncio de outros dispositivos BLE sem estabelecer uma conexão.
- **Periférico (ou *slave*)**: Este dispositivo fornece serviços e dados para outros dispositivos BLE e aceita conexões de dispositivos centrais.
- **Central (ou *master*)**: Este dispositivo inicia conexões com dispositivos periféricos e gere a conexão uma vez estabelecida.

Na comunicação resultante do trabalho desenvolvido nesta dissertação é esperado que seja iniciada uma conexão BLE entre dois dispositivos. Posto isto, os papéis do protocolo GAP que aceitam o estabelecimento de conexões entre dispositivos são os dispositivos periféricos e centrais. Assim sendo, um dos dispositivos irá atuar como periférico, sendo este o dispositivo que contém o servidor GATT e ligação aos sensores e que é responsável por fornecer os serviços e dados ao outro dispositivo, que irá adotar a função central, que contém o cliente GATT e que ficará responsável por iniciar a conexão com o dispositivo periférico e adquirir os dados do servidor.

Para além da gestão da conexão BLE, o protocolo GAP define também modos e procedimentos de segurança que especificam como os pares definem o nível de segurança exigido para transmissão de dados e, posteriormente, como esse nível de segurança é aplicado. O Security Manager Protocol (SMP) é o protocolo utilizado para implementar comunicações seguras entre dois dispositivos através da tecnologia BLE. Este é o protocolo responsável por estabelecer, gerir e manter uma conexão segura entre dois dispositivos. O SMP define os protocolos e algoritmos para a geração e troca de chaves de segurança entre os dispositivos, que permitem que os pares comuniquem com segurança por meio de uma ligação encriptada. Os mecanismos de segurança são aplicados durante a fase de emparelhamento dos dispositivos, onde ocorrem as trocas de chaves de segurança entre os mesmos. Com a implementação destes mecanismos, o SMP fornece à comunicação BLE proteção contra ciberataques, como ataques *eavesdropping* ou MITM, garantindo a confidencialidade e a integridade dos dados transmitidos através da conexão BLE.

Neste trabalho, devido ao elevado nível de segurança necessário a impor na comunicação BLE, o método de emparelhamento selecionado a utilizar foi o LE Secure Connections com geração de chaves OOB. Este é o método de emparelhamento mais seguro da tecnologia de comunicação BLE, enquanto a escolha sobre o OOB provém do facto deste ser o método de geração de chaves mais seguro e os nossos dispositivos não apresentarem quaisquer capacidades de entrada, como um teclado, ou de saída, como um ecrã, impossibilitando o uso de outros métodos seguros de geração de chave. Independentemente dos recursos de entrada e saída dos dispositivos, o método OOB pode ser sempre utilizado desde que existam os componentes necessários para uma comunicação fora de banda (como antenas NFC). Assim, com base nesta informação e na Tabela 3.3, para o método de geração de chave escolhido apenas existem duas possibilidades possíveis: JW ou OOB. Como o Just Works é um método de geração de chaves não autenticado e neste trabalho procuramos utilizar o modo de segurança BLE 1 com Nível 4 (ver Tabela 2.1), é obrigatória a utilização de um método autenticado. Assim sendo, a opção mais viável e a escolha natural para o método de geração de chaves recai sobre o método OOB, com a utilização de um canal NFC para realizar a troca de dados de emparelhamento.

		Dispositivo Central				
		Apenas Ecrã	**Ecrã Sim/Não**	**Apenas Teclado**	**Sem Entrada e Sem Saída**	**Teclado e Ecrã**
Dispositivo Periférico	**Apenas Ecrã**	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry
	Ecrã Sim/Não	Just Works	Just Works (LE Legacy Pairing) ou Numeric Comparison (LE Secure Connections)	Passkey Entry	Just Works	Passkey Entry (LE Legacy Pairing) ou Numeric Comparison (LE Secure Connections)
	Apenas Teclado	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
	Sem Entrada e Sem Saída	Just Works	Just Works	Just Works	Just Works	Just Works
	Teclado e Ecrã	Passkey Entry	Passkey Entry (LE Legacy Pairing) ou Numeric Comparison (LE Secure Connections)	Passkey Entry	Just Works	Passkey Entry (LE Legacy Pairing) ou Numeric Comparison (LE Secure Connections)

Tabela 3.3: Mapeamento de recursos de entrada e de saída para escolha do método de geração de chave utilizado. Adaptado de [39].

3.4.1 Emparelhamento LE Secure Connections com OOB

Como explicado na secção anterior, o método de emparelhamento em estudo neste trabalho é o LE Secure Connections com OOB. Nesta secção será discutido o funcionamento deste método de emparelhamento, abordando todas as fases envolvidas neste processo. Na Fig. 3.6 é possível verificar o esquema geral do emparelhamento LE Secure Connections, evidenciado em três fases distintas, destacadas com diferentes cores.

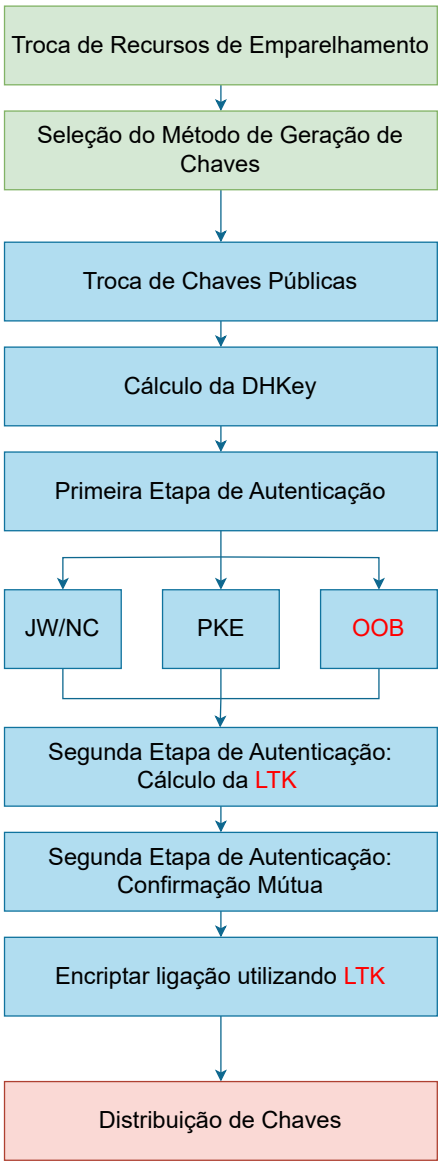

Figura 3.6: Esquema do emparelhamento LE Secure Connections. Adaptado de [18].

1ª Fase - Troca de Recursos de Emparelhamento

A primeira fase do emparelhamento LE Secure Connections consiste numa troca de recursos de emparelhamento entre os dispositivos conectados. Esta fase é utilizada para trocar

os recursos de entrada e de saída de ambos os dispositivos, a disponibilidade de dados de autenticação OOB, requisitos de autenticação, requisitos de tamanho de chave e definição de chaves específicas para distribuição. É com base nestes dados que é determinado qual o método de geração de chaves a ser utilizado na 2ª fase do emparelhamento.

Esta troca de recursos de emparelhamento funciona da seguinte forma: o dispositivo central inicia a troca de recursos realizando a solicitação de emparelhamento e enviando os seus dados. Do outro lado, o outro dispositivo recebe essa solicitação e caso esteja disponível para emparelhar envia a sua resposta ao dispositivo central. Na Fig. 3.7 é possível verificar a definição do pacote de solicitação/resposta de emparelhamento.

Field	Code (1 Byte)	IO Cap (1 Byte)	OOB Data Flag (1 Byte)	AuthReq (1 Byte)					Maximum Encryption Key Size (1 Byte)	Initiator Key Distribution (1 Byte)	Responder Key Distribution (1 Byte)
Sub-Define				BF	MITM	SC	KP	Reserved			
Bits	8	8	8	2	1	1	1	3	8	8	8

Figura 3.7: Solicitação/Resposta de Emparelhamento.

Para que o método de emparelhamento utilizado seja o LE Secure Connections, o campo relativo ao método de emparelhamento LE Secure Connections de ambos os pacotes de solicitação/resposta de emparelhamento (*flag* 'SC') deve estar a 1. Caso contrário, indica que um dos dispositivos ou ambos não suportam LE Secure Connections e dessa forma o método de emparelhamento utilizado será o LE Legacy Pairing, reduzindo drasticamente o nível de segurança da comunicação.

No caso do método de emparelhamento LE Secure Connections, para que o método de geração de chaves selecionado seja o OOB, pelo menos um dos dispositivos deve conter dados de autenticação OOB, e estes devem ser indicados no campo 'OOB *Data Flag*' do pacote.

2ª Fase - Geração da Chave de Longo Prazo (LTK)

A segunda fase do emparelhamento LE Secure Connections envolve diversas tarefas como a troca de chaves públicas, o cálculo da chave Diffie-Hellman (DHKey), duas etapas de autenticação e por fim a encriptação da ligação.

A primeira tarefa consiste na troca das correspondestes chaves públicas entre dispositivos. Primeiramente, o dispositivo central envia a sua chave pública ao outro dispositivo, e em seguida ocorre a troca inversa.

A segunda tarefa corresponde ao cálculo de chaves Diffie-Hellman (DHKey), uma para cada um dos dispositivos (3.1 e 3.2). O cálculo destas chaves é realizado em função da chave privada do dispositivo correspondente e da chave pública do outro dispositivo, trocada na etapa anterior, utilizando o algoritmo de criptografia de curva elíptica de 256 bits (P256).

$$DHKey_A = P256(ChavePrivada_A, ChavePublica_B) \tag{3.1}$$

$$DHKey_B = P256(ChavePrivada_B, ChavePublica_A) \tag{3.2}$$

Em seguida ocorrem as tarefas de autenticação. A primeira etapa de autenticação permite ao utilizador confirmar que o dispositivo com o qual está a tentar emparelhar é realmente o dispositivo com o qual deseja realizar o emparelhamento. Esta primeira etapa varia consoante o método de geração de chave escolhido. No emparelhamento com o método OOB, a primeira etapa de autenticação divide-se em duas partes: uma primeira parte *Out Of Band*, onde é utilizado outro canal que não o *Bluetooth* (no nosso caso será o NFC) para trocar dados, e uma segunda parte *In Band*, na qual os dados são trocados via *Bluetooth*. Nas Figs. 3.8 e 3.9, é possível visualizar as comunicações *Out Of Band* e *In Band*, respetivamente, entre os dispositivos.

A parte *Out Of Band* começa pela geração de números aleatórios, `Ra` e `Rb`, por parte de cada um dos dispositivos. Em seguida, são calculados valores de confirmação, `Ca` e `Cb`, também por parte de cada um dos dispositivos. Estes valores de confirmação são calculados em função da chave pública e do número aleatório, `Ra` ou `Rb`, do próprio dispositivo. Por fim, são trocados os dados de autenticação OOB entre os dois dispositivos. Os dados de autenticação OOB correspondem ao endereço do dispositivo, ao número aleatório gerado e ao valor de confirmação calculado [18].

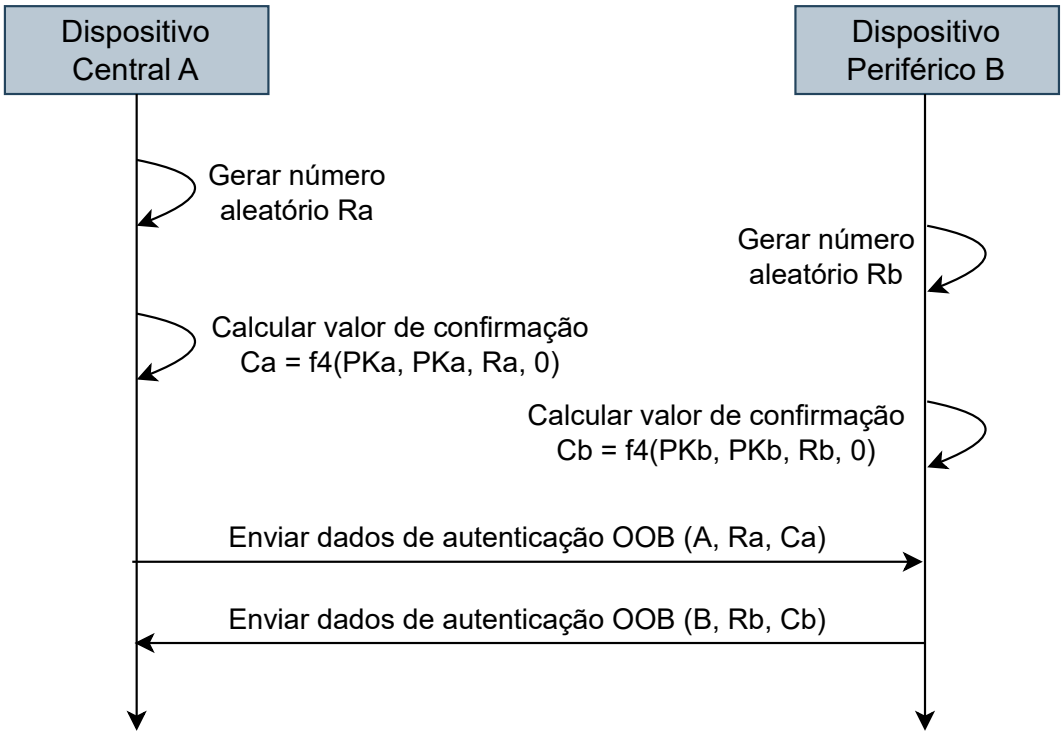

Figura 3.8: Primeira Etapa de Autenticação: Parte 1 - *Out Of Band*. Adaptado de [18].

A segunda parte corresponde à etapa *In Band*. Aqui são recalculados os valores de confirmação, `Ca` e `Cb`, só que desta vez são os dispositivos contrários que calculam esses valores. Estes valores são recalculados utilizando as chaves públicas trocadas anteriormente *In Band* e os números aleatórios recebidos *Out Of Band*. Após recalcular esses valores, os mesmos são comparados com os valores calculados inicialmente e anteriormente transferidos *Out Of Band*. Caso algum dos valores não seja o mesmo, o emparelhamento é abortado [18]. Antes de terminar, cada um dos dispositivos gera um número aleatório que apenas pode ser utilizado uma vez (*nonce*), `Na` e `Nb`, e envia o seu valor ao outro dispositivo. Estes valores procuram garantir a segurança evitando ataques de repetição (*replay attacks*) e devem ser gerados sempre que é iniciado um novo emparelhamento [13]. Um ataque de repetição consiste na interceção dos pacotes transmitidos entre dispositivos por parte de um invasor. Posteriormente, esse invasor retransmite ou reproduz esses pacotes na tentativa de enganar um dos dispositivos, fazendo-o acreditar que se encontra inserido numa transmissão segura [18].

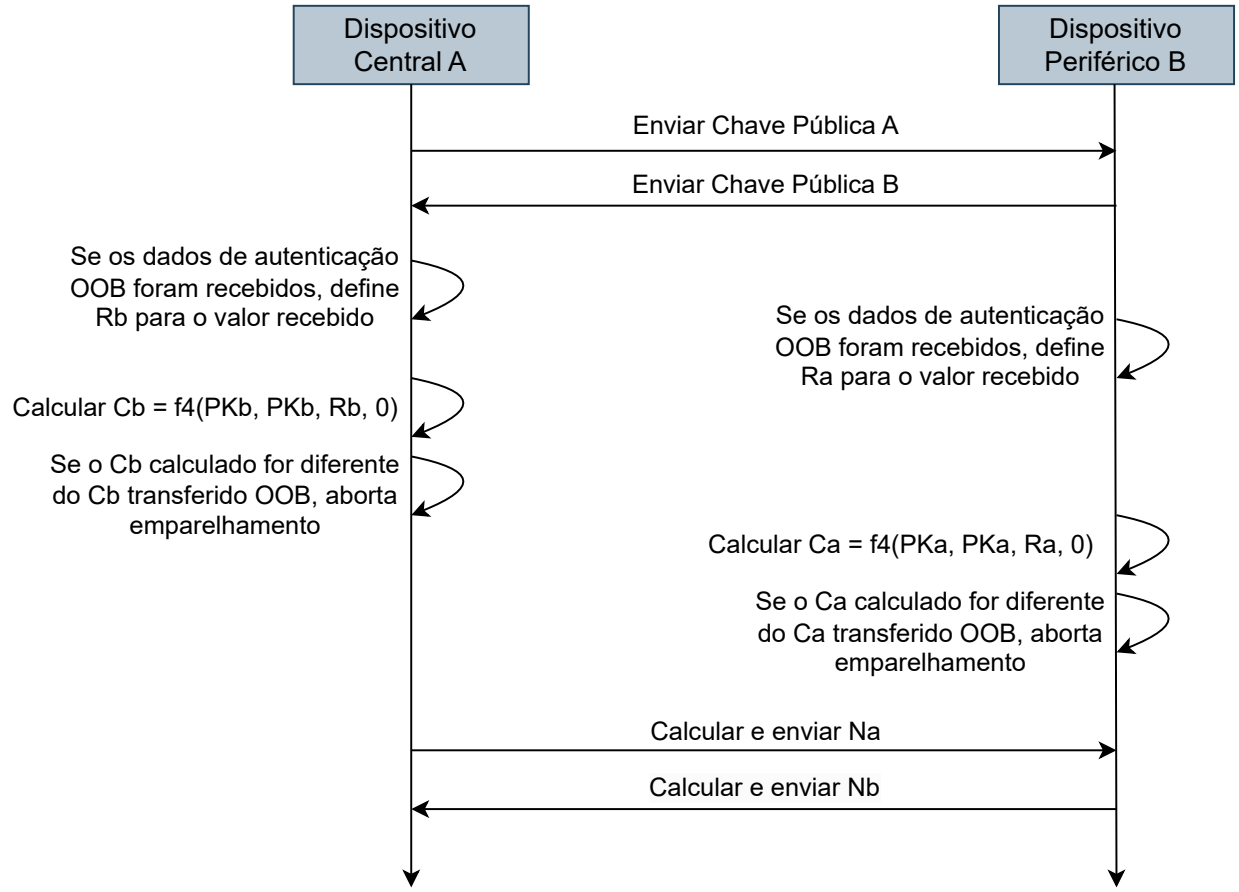

Figura 3.9: Primeira Etapa de Autenticação: Parte 2 - *In Band*. Adaptado de [18].

Após a primeira etapa de autenticação terminar, ocorre a segunda etapa de autenticação. Nesta segunda etapa são realizadas verificações adicionais para garantir que as trocas de dados realizadas nas etapas anteriores foram devidamente concluídas por ambos os dispositivos. Nesta etapa existem então quatro tarefas: cálculo da chave de longo prazo (LTK) e da chave MacKey através de uma função de geração de chaves do LESC, cálculo dos valores de verificação, `Ea` e `Eb`, através de uma função de geração de valores de verificação do LESC, para troca e comparação entre dispositivos e início da encriptação da ligação utilizando a LTK para criar uma chave de sessão [13, 18]. Na Fig. 3.10 é possível observar as tarefas relativas à segunda etapa de autenticação do método de emparelhamento LE Secure Connections com OOB.

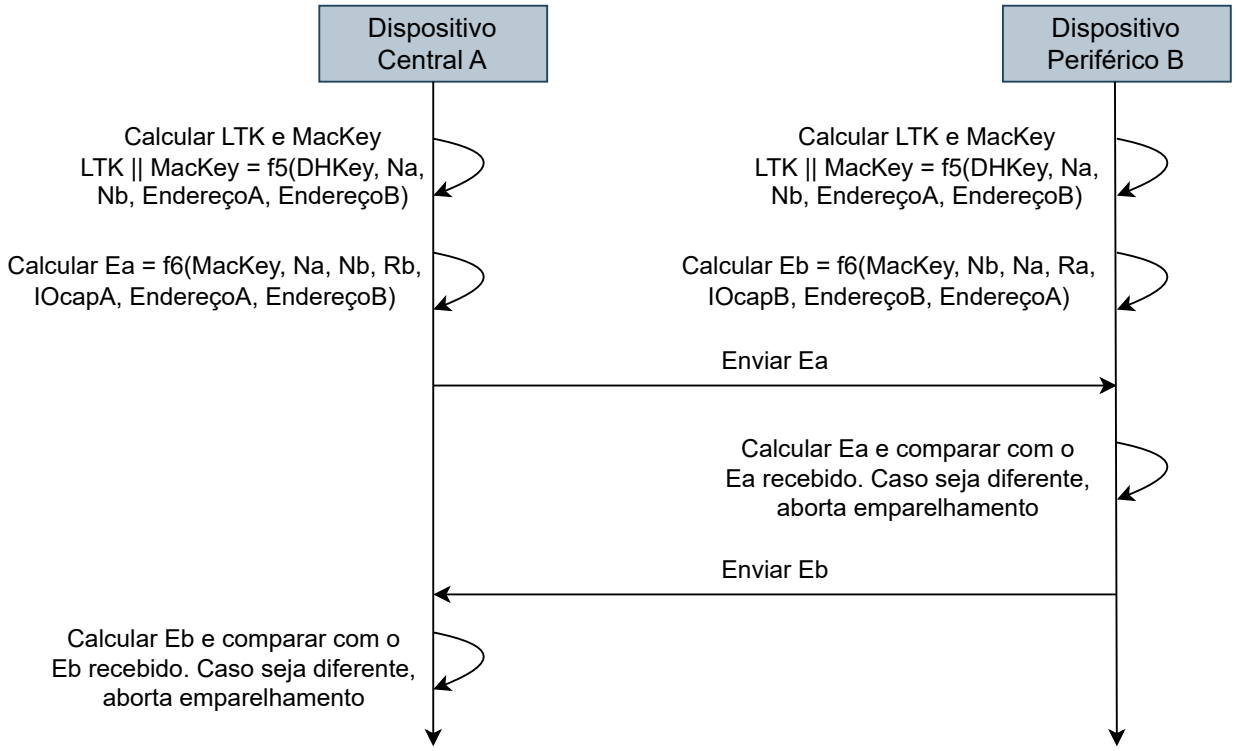

Figura 3.10: Segunda Etapa de Autenticação. Adaptado de [13].

3ª Fase - Distribuição de Chaves

A terceira e última fase do emparelhamento LE Secure Connections envolve a encriptação da ligação entre os dispositivos utilizando uma chave de sessão derivada da chave de longo prazo (LTK) e a distribuição das chaves Identity Resolving Key (IRK) e Connection Signature Resolving Key (CSRK), caso tenham sido selecionadas durante a 1ª fase [18]. A IRK é utilizada para gerar endereços privados que devem ser resolvíveis pelos outros dispositivos de forma a manter a privacidade. A CSRK é usada para assinar os dados e verificar essas assinaturas, garantindo que os dados são provenientes de fonte segura.

3.4.2 Emparelhamento LE Secure Connections com JW

O método de emparelhamento LE Secure Connections com Just Works é significativamente mais resistente a ataques de espionagem que o mesmo método de geração de chaves utilizado com o emparelhamento LE Legacy Pairing, isto porque o método LESC utiliza criptografia ECDH.

Este emparelhamento, relativamente ao emparelhamento com OOB descrito anteriormente, apenas apresenta diferenças na primeira etapa de autenticação do emparelhamento LESC (ver Fig. 3.6). Nesta fase do emparelhamento, após os dispositivos trocarem as suas

chaves públicas, cada um deles gera um *nonce*, `Na` e `Nb`, que é essencialmente um valor de semente aleatório para proteção contra ataques de repetição. Em seguida, o dispositivo periférico utiliza esse valor e as chaves públicas trocadas para gerar um valor de confirmação `Cb` e envia-o juntamente com o seu *nonce* para o dispositivo central. Ao mesmo tempo, o dispositivo central envia o seu *nonce* `Na` para o dispositivo periférico. Após isso, o dispositivo central calcula o valor de confirmação com as chaves públicas e o *nonce* `Nb` enviado anteriormente pelo dispositivo periférico. Se os valores de confirmação corresponderem, a conexão continua. Caso contrário, o emparelhamento é abortado [13]. Na Fig. 3.11 é possível observar as tarefas relativas à primeira etapa de autenticação do método de emparelhamento LE Secure Connections com JW.

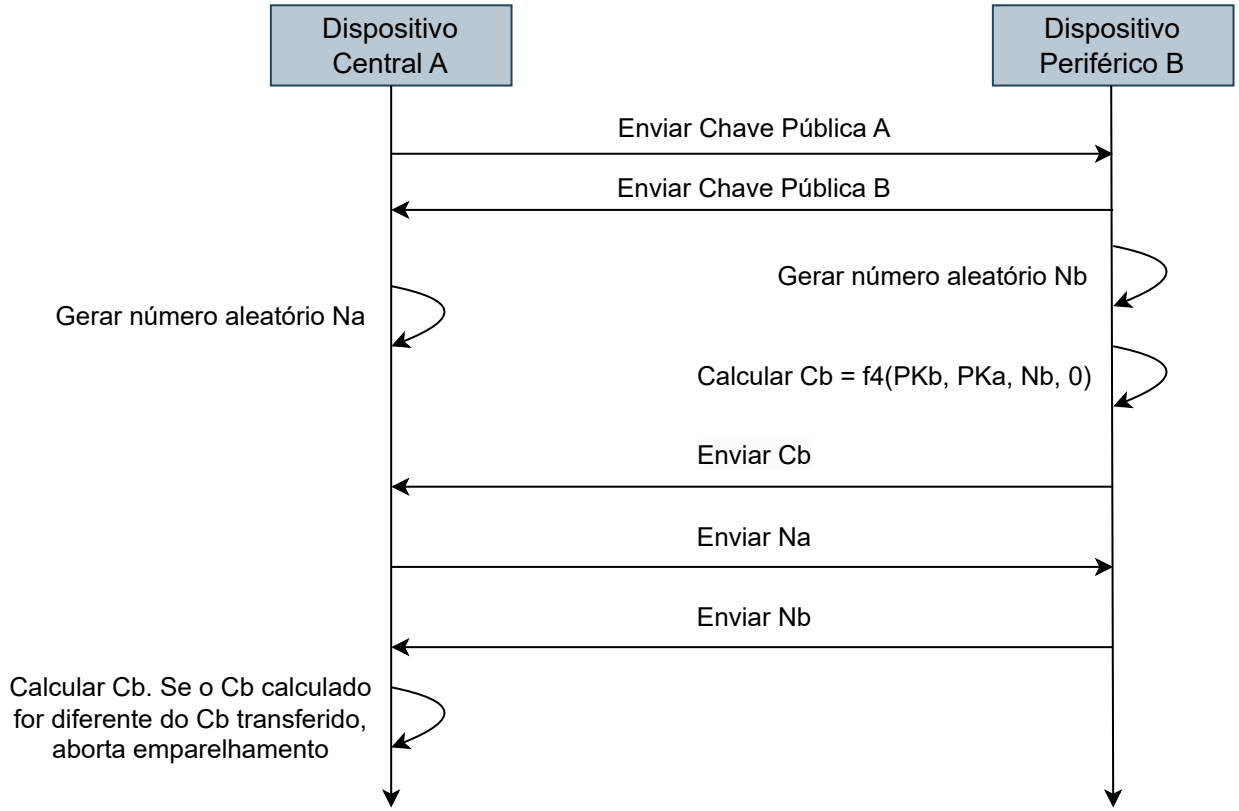

Figura 3.11: Primeira etapa de autenticação para o emparelhamento LE Secure Connections com Just Works. Adaptado de [13].

Desta forma, este emparelhamento mostra-se significativamente mais seguro que a mesma abordagem com o método de emparelhamento LE Legacy Pairing. No entanto, esta não é a abordagem ideal a introduzir no sistema do projeto, pois este é um método de geração de chaves que não fornece autenticação e, por esse motivo, continua suscetível a ataques MITM [18]. Assim, conclui-se que o método de emparelhamento mais adequado e que maior segurança fornece ao sistema é o método LESC com OOB, descrito na Secção 3.4.1.

3.4.3 Troca de Dados via NFC

Com o intuito de reforçar a segurança na comunicação, foi adotada a tecnologia NFC no emparelhamento OOB com o objetivo de utilizar um canal de comunicação seguro através do qual seja possível partilhar dados de autenticação que são usados na comunicação BLE entre os dispositivos. O NFC é uma tecnologia de alcance extremamente curto, na ordem dos 10 centímetros de alcance máximo, com taxa máxima de transmissão de dados de 0.4 Mbps, opera na banda de frequência de 13.56 MHz e apresenta baixo consumo energético e baixo custo [40]. No NFC existem três diferentes modos de funcionamento [2, 41]:

1. **Modo leitor/gravador**, em que os dispositivos NFC ativos podem ler e modificar informações armazenadas em *tags* NFC passivas;

2. **Modo de emulação de cartão**, em que dispositivos NFC, como *smartphones* com leitor incorporado, podem operar como cartões sem contacto (*contactless cards*);

3. **Modo ponto a ponto**, em que dispositivos habilitados com a tecnologia NFC podem comunicar diretamente um com o outro e trocar informações de forma bidirecional.

Ao nível da segurança, o NFC representa um canal seguro, visto que apresenta um alcance extremamente curto, o que faz com que para que exista uma conexão, os dispositivos tenham que estar a uma distância muito próxima, assegurando que a comunicação é realizada entre os dispositivos corretos. Consequentemente, o NFC apresenta proteção inerente contra ataques MITM [42].

Para o armazenamento e troca de dados em *tags* e dispositivos NFC utiliza-se o formato padrão NFC Data Exchange Format (NDEF)[11]. Este formato possibilita a comunicação entre dispositivos habilitados com a tecnologia NFC (como *smartphones* ou tablets), bem como entre estes dispositivos e *tags* NFC. O NDEF foi desenvolvido com o intuito de fornecer um formato padrão e flexível que permite armazenar diferentes tipos de dados como textos, URLs ou pequenos arquivos binários. O NDEF apresenta na sua estrutura dois formatos: mensagens e registos (*records*). O principal formato são as mensagens NDEF, que consistem em um ou mais registos NDEF de diferentes tipos. Cada registo possui um cabeçalho que inclui informações sobre o tipo de dados que ele contém, o tamanho dos dados e qualquer informação adicional que possa ser relevante. As mensagens podem ser lidas e escritas

[11]NFC Data Exchange Format (NDEF), `https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/nrf/libraries/nfc/ndef/index.html`

por qualquer dispositivo habilitado com a tecnologia NFC que suporte o padrão NDEF, tornando-o uma maneira conveniente de trocar informações entre dispositivos.

No caso deste trabalho foi utilizado um dispositivo leitor NFC ST25R3911B Nucleo Expansion Board (X-NUCLEO-NFC05A1)[12] que é responsável por ler os dados de outro dispositivo NFC (antena NFC do kit de desenvolvimento nRF52 DK), utilizando o modo de funcionamento leitor/gravador. A Fig. 3.12 ilustra a comunicação NFC utilizada neste trabalho. Para realizar a troca de dados entre o dispositivo leitor e a *tag* através de uma conexão NFC foi utilizado um protocolo que opera na camada de aplicação da pilha da tecnologia NFC, que é possível observar na Fig. 3.13. O protocolo designado para esse efeito foi o Tag NDEF Exchange Protocol (TNEP)[13]. Os dados trocados neste protocolo são mensagens no formato NDEF e estas podem ser trocadas entre os dispositivos de forma bidirecional. O TNEP permite os dispositivos negociarem e estabelecerem uma conexão NFC, trocarem mensagens NDEF e interromperem a conexão quando a troca de dados estiver concluída.

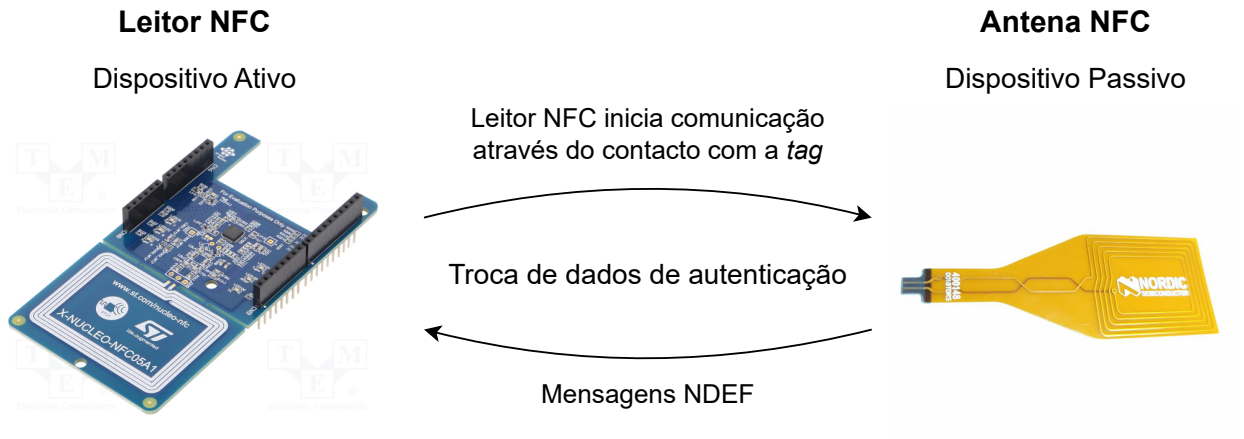

Figura 3.12: Comunicação NFC para troca de dados de autenticação entre dispositivos.

[12]NFC Reader X-NUCLEO-NFC05A1, `https://www.st.com/en/ecosystems/x-nucleo-nfc05a1.html`

[13]Tag NDEF Exchange Protocol (TNEP), `https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/nrf/libraries/nfc/tnep/index.html#tag-ndef-exchange-protocol-tnep`

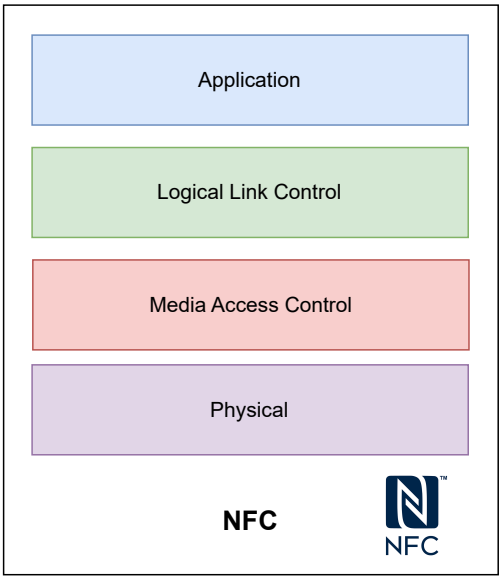

Figura 3.13: Pilha da tecnologia de comunicação NFC. Adaptado de [2].

3.5 Sumário

O fluxograma da Fig. 3.14 representa o algoritmo desenvolvido para a comunicação BLE segura neste trabalho. Neste diagrama são especificados todos os processos desta comunicação, desde a inicialização do protocolo BLE, passando pelas etapas de emparelhamento e conexão, até alcançar a fase final da transmissão dos dados por meio de notificações.

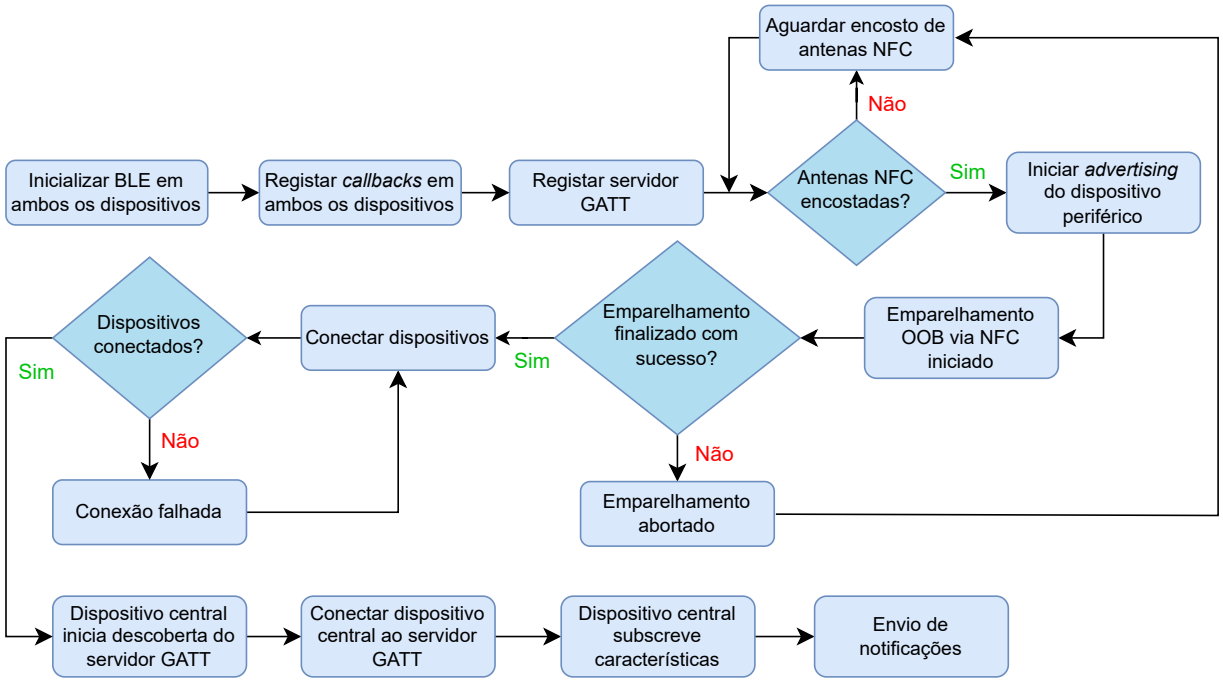

Figura 3.14: Fluxograma de comunicação BLE implementada entre dispositivos.

Neste capítulo foi apresentada a arquitetura do sistema implementado neste trabalho, bem como todos os diferentes componentes do sistema, incluindo protocolos, ferramentas e métodos utilizados.

O próximo capítulo foca-se na validação experimental do trabalho implementado nesta dissertação e são analisados os resultados provenientes dos testes comparativos de desempenho realizados entre comunicação segura e não segura.

4 Validação Experimental

Com o intuito de validar o desempenho do sistema desenvolvido e realizar uma avaliação comparativa entre o sistema sem segurança em utilização no projeto WoW e o sistema implementado, foram realizados em laboratório diversos testes de análise de desempenho. Neste capítulo são apresentadas as diversas configurações experimentais a serem avaliadas neste trabalho, as diferentes métricas de avaliação e as ferramentas utilizadas para a obtenção dos resultados. Com base nos resultados obtidos é realizada uma análise e lançada a discussão sobre o trabalho desenvolvido.

4.1 Design Experimental

O principal objetivo dos testes experimentais consistiu na validação dos mecanismos de segurança implementados no sistema e na análise comparativa entre a transmissão segura e a transmissão não segura. Para estes testes foram criados diferentes *setups* de testes baseados na arquitetura do sistema (ver Fig. 3.1). Estes *setups* são compostos por um módulo de aquisição de dados, que poderá ser um kit de desenvolvimento nRF52 DK, um *smartphone* ou uma Raspberry Pi 4B. Este dispositivo atua como dispositivo central, ao qual foi adicionado um leitor NFC para realizar emparelhamento OOB. No caso do *smartphone* não foi necessário adicionar um leitor NFC, uma vez que foi utilizado o modelo Xiaomi Redmi Note 7, que contém um leitor embutido no mesmo. Este dispositivo irá comunicar com outro kit de desenvolvimento nRF52 DK que atua como dispositivo periférico e que contém uma antena NFC passível de ser lida para realizar emparelhamento OOB. Para a verificação dos pacotes BLE transmitidos entre estes dois componentes foi utilizada a nRF52840 Dongle como BLE *sniffer* e o programa de análise de tráfego Wireshark.

Neste trabalho foram definidas cinco diferentes configurações para avaliação. Estas configurações foram ponderadamente escolhidas para permitir realizar uma análise comparativa entre os diferentes níveis de segurança implementados (emparelhamento LESC com OOB e

também com JW) com diferentes módulos de aquisição, proporcionando análise de desempenho, bem como conclusões sobre o comportamento do sistema relativamente a diferentes dispositivos. Os dispositivos escolhidos para os testes foram a Raspberry Pi, por ser o módulo de aquisição de dados integrado no projeto WoW, e o *smartphone*, por ser um dispositivo de fácil acesso e que contém um leitor NFC embutido.

A nRF52 DK foi selecionada para substituir a Raspberry Pi no emparelhamento LESC com OOB, isto porque a implementação do método OOB na Raspberry Pi envolve significativas modificações na aquisição de dados do projeto WoW. Atualmente no projeto é utilizada a biblioteca Bleak[14] que lida com a comunicação DBus, que, por sua vez, é utilizada pela API oficial para interagir prontamente com a *stack* do *Bluetooth* em Linux (também designada BlueZ[15]) . No entanto, a biblioteca Bleak não suporta todos os métodos de emparelhamento, pelo que para implementar o emparelhamento OOB toda a interação com a *stack* do *Bluetooth* teria que ser refeita na Raspberry Pi utilizando diretamente o DBus. Esta abordagem implicaria um elevado consumo de tempo, que neste trabalho é limitado, pelo que teve que ser escolhida outra configuração, na qual foi selecionada a nRF52 DK por ser o mesmo kit de desenvolvimento do *firmware* dos *biostickers*. Assim, as configurações de teste estão descritas na Tabela 4.1.

Configuração	**Acrónimo**	**Descrição**
1	NoSec-RPi	Sistema atual do projeto WoW com Raspberry Pi sem mecanismos de segurança implementados
2	LE-JW-S	Sistema com emparelhamento LE Secure Connections com método JW com *smartphone*
3	LE-JW-RPi	Sistema com emparelhamento LE Secure Connections com método JW com Raspberry Pi
4	LE-OOB-S	Sistema com emparelhamento LE Secure Connections com método OOB com *smartphone*
5	LE-OOB-nRF	Sistema com emparelhamento LE Secure Connections com método OOB com nRF52 DK

Tabela 4.1: Configurações dos testes experimentais.

[14]Bleak, `https://github.com/hbldh/bleak`

[15]BlueZ, `http://www.bluez.org/`

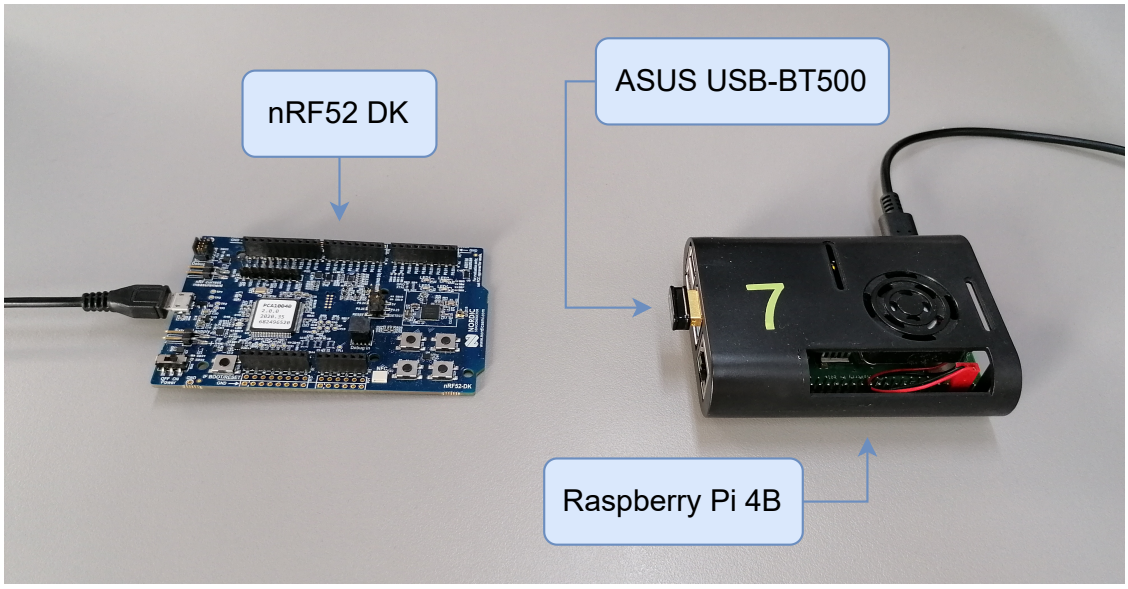

Figura 4.1: Esquema do *setup* experimental para emparelhamento com Raspberry Pi (Configurações NoSec-RPi e LE-JW-RPi).

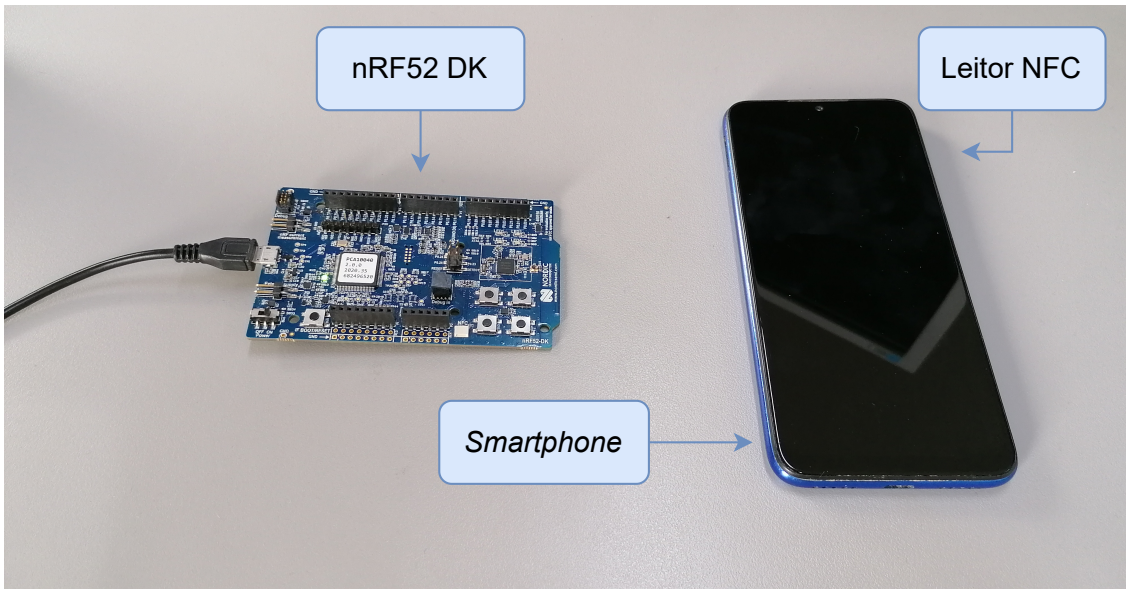

Figura 4.2: Esquema do *setup* experimental para emparelhamento com *smartphone* (Configurações LE-JW-S e LE-OOB-S).

Para garantir a consistência dos testes, estes foram criteriosamente dimensionados com repetições de 10 execuções para cada configuração. Em cada execução ocorre a troca de 5000 mensagens, onde são transmitidos os diferentes sinais vitais simulados, presentes nas características do servidor GATT personalizado apresentado anteriormente na Tabela 3.2. A distância entre os dispositivos foi constante para todos os testes, tendo sido de 10 centímetros. Com vista à análise e avaliação do desempenho dos sistemas desenvolvidos, foram avaliadas

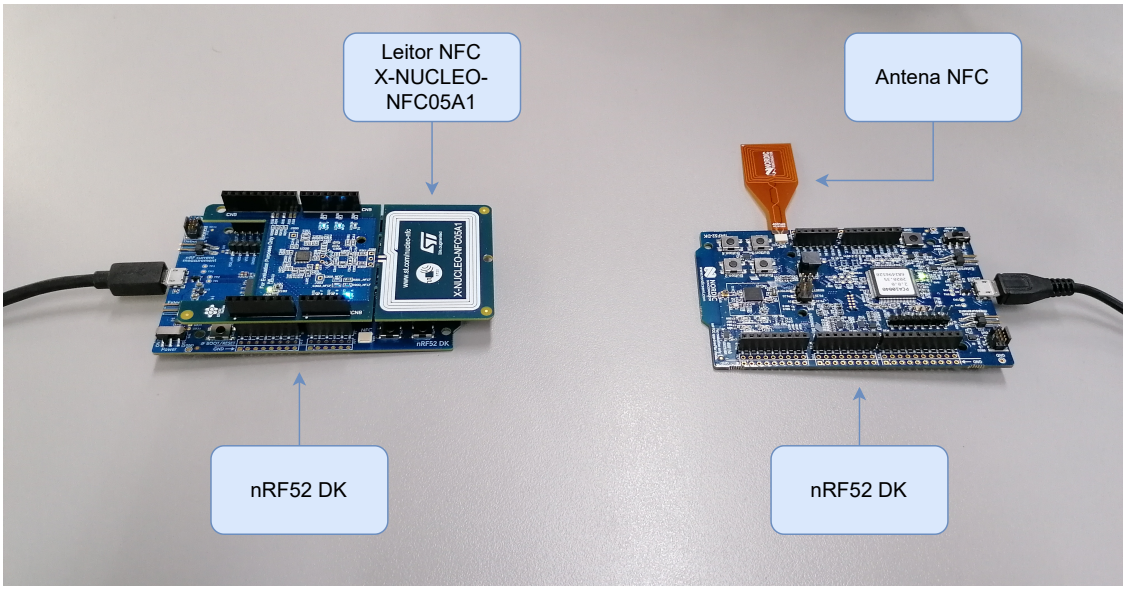

Figura 4.3: Esquema do *setup* experimental para emparelhamento com nRF52 DK (Configuração LE-OOB-nRF).

as seguintes métricas de desempenho:

- **Taxa de Aquisição (Hz)**: Representa a frequência de receção dos pacotes BLE transmitidos, permitindo retirar conclusões sobre atrasos na transmissão dos pacotes;
- **Perda de Pacotes (%)**: Caracteriza o número total de pacotes BLE perdidos durante a transmissão e que por esse motivo não alcançam o destinatário, o que possibilita compreender se o sistema apresenta a fiabilidade necessária;
- **Tempo Total de Teste (s)**: Representa a duração total do emparelhamento e troca das 5000 mensagens e permite analisar se os mecanismos de segurança impõem um aumento significativo nesse tempo;
- **Tamanho do *Payload* (bytes)**: Caracteriza o tamanho dos pacotes BLE trocados e proporciona retirar conclusões sobre o *overhead* imposto nas comunicações com segurança relativamente a comunicações não seguras.

Para extrair os resultados das comunicações BLE, foram desenvolvidos *scripts* em linguagem Python[16] que permitem analisar os *logs* obtidos por meio de gravações das comunicações no programa Wireshark. Este foi o método selecionado para o processamento dos resultados, uma vez que automatiza o processo e minimiza a interação humana no processamento. Com vista ao processamento dos *logs* do Wireshark foi utilizada a biblioteca

[16]Python, `https://www.python.org/`

Pyshark[17] que proporciona a análise dos pacotes BLE através de filtros do Wireshark. Assim, com esta biblioteca é possível ler um ficheiro com os dados da captura das comunicações (*log*) e filtrar os pacotes BLE, permitindo retirar dados para posterior análise.

Deste modo, o *script* desenvolvido começa por extrair os dados mais relevantes dos *logs*, como os *timestamps*, o UUID e o valor da característica envolvida no pacote ou o tamanho do mesmo. Após a recolha destes dados são calculadas as métricas de avaliação apresentadas anteriormente.

4.2 Resultados e Discussão

O primeiro mecanismo de segurança a ser implementado neste trabalho consistiu na encriptação e autenticação dos pacotes transmitidos durante a comunicação BLE. Na Fig. 4.4 é possível inspecionar um pacote BLE capturado pelo nRF *Sniffer* utilizando o programa Wireshark durante a comunicação do sistema com segurança desenvolvido neste trabalho que transmite o nível da bateria do dispositivo em percentagem. Esta figura comprova que o pacote transmitido encontra-se encriptado, dado que a *flag 'Encrypted'* encontra-se ativa, e autenticado, uma vez que a *flag* 'MIC' encontra-se também ativa, validando o remetente. Este pacote apenas foi possível de desencriptar, uma vez que o SMP foi colocado em modo *debug*, resultando na utilização de pares de chaves pública/privada pré-definidas pela especificação do *Bluetooth* no Vol. 3, Parte H, 2.3.5.6.1 [13]. Desta forma, o *sniffer* obtém acesso aos dados, pois tem conhecimento prévio sobre estas chaves. Um intermediário na comunicação que não tenha acesso às chaves de encriptação não conseguirá desencriptar os pacotes, garantindo a segurança da informação transmitida.

O segundo mecanismo de segurança a validar neste trabalho é o emparelhamento físico com a tecnologia NFC. Para tal foi implementado o emparelhamento LE Secure Connections com OOB. Na Fig. 4.5 é possível observar todos os pacotes BLE do protocolo SMP trocados entre os dois dispositivos durante a comunicação, que representam todo o processo do emparelhamento LE Secure Connections com OOB descrito anteriormente na Secção 3.4.1. Na Fig. 4.6 é possível verificar detalhadamente um pacote BLE do protocolo SMP capturado pelo nRF *Sniffer* durante a comunicação do sistema com segurança, que corresponde à solicitação de emparelhamento por parte do dispositivo central (ver Fig. 3.7). Nesta figura é possível observar que a *flag* correspondente ao método de emparelhamento LE Secure Connections encontra-se ativa, estão presentes dados OOB e a *flag* correspondente à proteção

[17]Pyshark, `https://github.com/KimiNewt/pyshark`

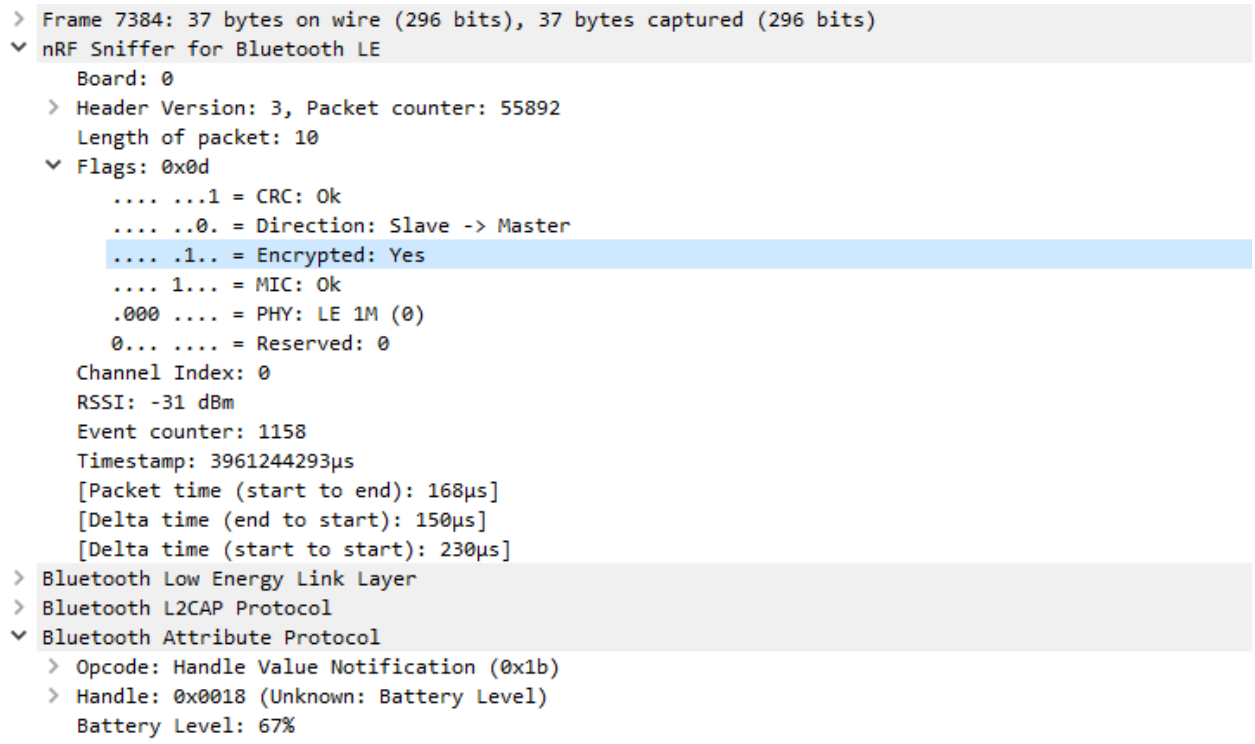

Figura 4.4: Pacote BLE encriptado capturado pelo nRF *Sniffer* utilizando o *software* Wireshark, com informação de nível de bateria.

contra ataques MITM também se encontra ativa. Desta forma, o método de emparelhamento utilizado entre os dispositivos nesta comunicação será o LE Secure Connections com OOB como ambicionado. Com este método de emparelhamento a comunicação torna-se significativamente mais segura, dado que o emparelhamento é forçado através do contacto físico entre a antena e o leitor NFC, assegurando que a comunicação pretendida é entre os dois dispositivos.

No.	Time	Source	Destination	Protocol	Length	Info
1704	3.498…	Slave_0x45c1c…	Master_0x45c1…	SMP	32	Rcvd Security Request: AuthReq: Bonding, SecureConnection
1833	4.586…	Master_0x45c1…	Slave_0x45c1c…	SMP	37	Sent Pairing Request: AuthReq: Bonding, MITM, SecureConnection, Reserved | Initia…
1836	4.636…	Slave_0x45c1c…	Master_0x45c1…	SMP	37	Rcvd Pairing Response: AuthReq: Bonding, SecureConnection | Initiator Key(s): IRK…
1841	4.688…	Master_0x45c1…	Slave_0x45c1c…	SMP	41	Sent Pairing Public Key
1848	4.738…	Slave_0x45c1c…	Master_0x45c1…	SMP	41	Rcvd Pairing Public Key
1850	4.738…	Slave_0x45c1c…	Master_0x45c1…	SMP	47	Rcvd Pairing Confirm
1851	4.786…	Master_0x45c1…	Slave_0x45c1c…	SMP	47	Sent Pairing Random
1854	4.836…	Slave_0x45c1c…	Master_0x45c1…	SMP	47	Rcvd Pairing Random
1897	5.936…	Master_0x45c1…	Slave_0x45c1c…	SMP	47	Sent Pairing DHKey Check
1900	5.986…	Slave_0x45c1c…	Master_0x45c1…	SMP	47	Rcvd Pairing DHKey Check
1913	6.336…	Master_0x45c1…	Slave_0x45c1c…	SMP	47	Sent Identity Information
1915	6.337…	Master_0x45c1…	Slave_0x45c1c…	SMP	38	Sent Identity Address Information
1916	6.386…	Master_0x45c1…	Slave_0x45c1c…	SMP	38	Sent Identity Address Information

Figura 4.5: Pacotes BLE de emparelhamento trocados entre os dispositivos.

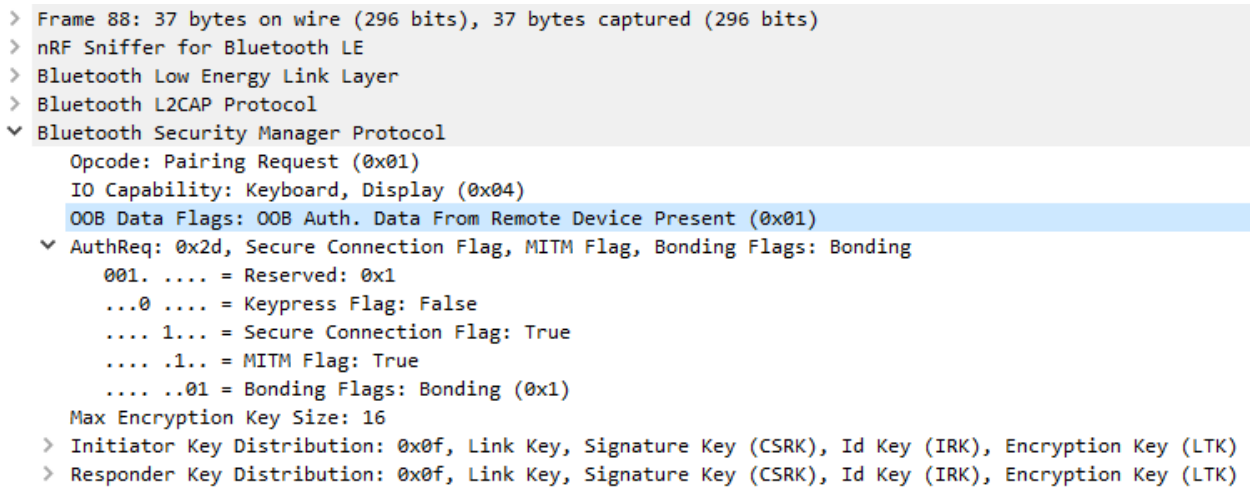

Figura 4.6: Pacote BLE de pedido de emparelhamento capturado pelo nRF *Sniffer* utilizando o *software* Wireshark.

Após validação dos mecanismos de segurança implementados no sistema, parte-se agora para uma análise detalhada aos testes experimentais realizados em laboratório com vista à comparação do desempenho entre a transmissão de dados segura e não segura.

Começando pela Fig. 4.7, nesta é possível observar um gráfico com diagramas de caixa, que permitem representar os dados e a sua variação, onde são apresentados os valores para a perda de pacotes das diversas configurações de testes. De uma forma geral, é possível concluir que todas as configurações apresentam uma baixa percentagem de perda de pacotes, o que indica que as configurações mostram-se fiáveis ao assegurar a chegada dos pacotes transmitidos por parte do servidor. Nas quatro primeiras configurações foram alcançados valores significativamente baixos de perda de pacotes, com valores médios de 0.7%, 0.7%, 0.4% e 0.1%, respetivamente. Apenas a configuração LE-OOB-nRF apresenta uma perda superior às restantes configurações, sendo ainda assim uma perda média na ordem dos 2.4%, não sendo este considerado um valor extremamente elevado. No entanto, utilizando os mesmos mecanismos de segurança com o *smartphone* (LE-OOB-S), essa perda não é verificada, pelo que é possível de constatar que a utilização do kit de desenvolvimento nRF52 DK como módulo de aquisição de dados pode ter alguma influência neste resultado. Este acontecimento pode dever-se ao facto da placa nRF52 DK recetora apresentar limitações no acompanhamento da elevada taxa de transmissão de dados da nRF52 DK transmissora, levando ao sobrecarregamento de *buffers* na aquisição e consequente perda de pacotes. Em termos de variação, esta última configuração é também aquela que apresenta uma maior variação dos seus valores, embora valores discrepantes (*i.e.*, *outliers*) apenas sejam verificados na configuração NoSec-RPi. Assim, é possível inferir através deste gráfico que não houve um incremento

significativo na perda de pacotes com o aumento do nível de segurança do sistema.

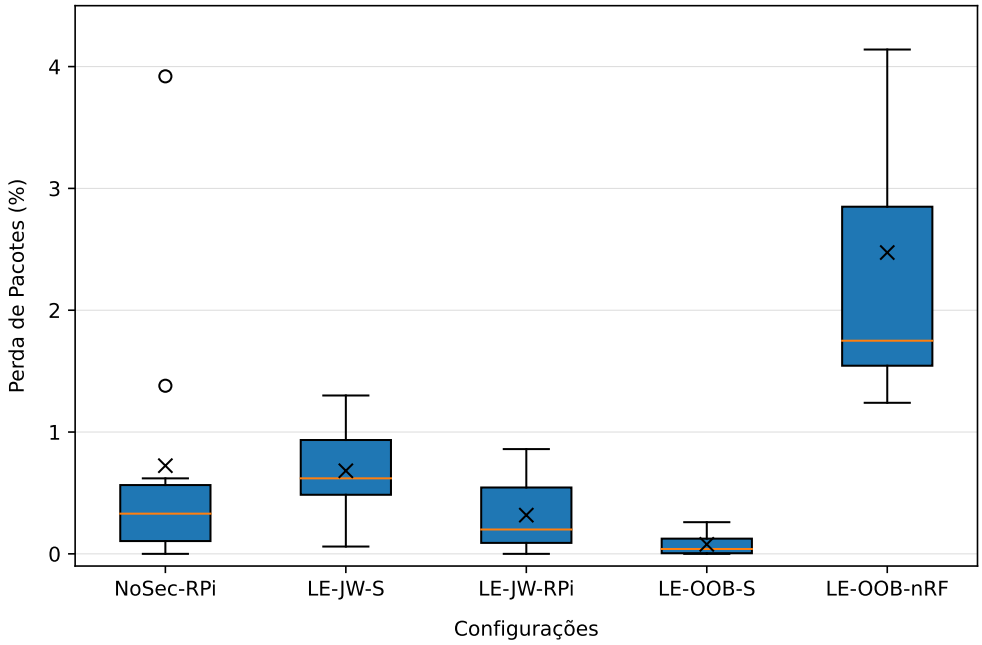

Figura 4.7: Perda de pacotes obtida nas diferentes configurações de testes. A média é indicada com o símbolo "×".

Na Fig. 4.8 é apresentado novamente um gráfico com diagramas de caixa, sendo que neste a métrica avaliada é o tempo total de teste em segundos por configuração. Através desta figura é possível concluir que a introdução de mecanismos de segurança no sistema não fez variar significativamente a duração total da transmissão. Nas configurações LE-JW-RPi e LE-OOB-nRF (configurações seguras) apenas houve um incremento de 2 s no tempo total de teste em relação à configuração não segura (NoSec-RPi). As principais alterações no tempo total de teste foram observadas nas configurações em que foi utilizado o *smartphone* (LE-JW-S e LE-OOB-S), embora a diferença para as restantes configurações não seja significativa, apenas na ordem dos 10/15 segundos (entre 2 a 3 ms a mais por pacote). Em termos de variação, estas foram também as configurações que apresentaram um ligeiro desvio e um valor discrepante, enquanto as outras configurações não apresentaram praticamente nenhuma variação na duração total do teste, mostrando-se muito estáveis no tempo necessário para a transmissão das 5000 mensagens. Este resultado pode ser surpreendente, pois seria de esperar um *overhead* maior da camada de segurança que não é verificado. A justificação para este resultado é apresentada posteriormente quando analisado o *payload* dos pacotes BLE transmitidos.

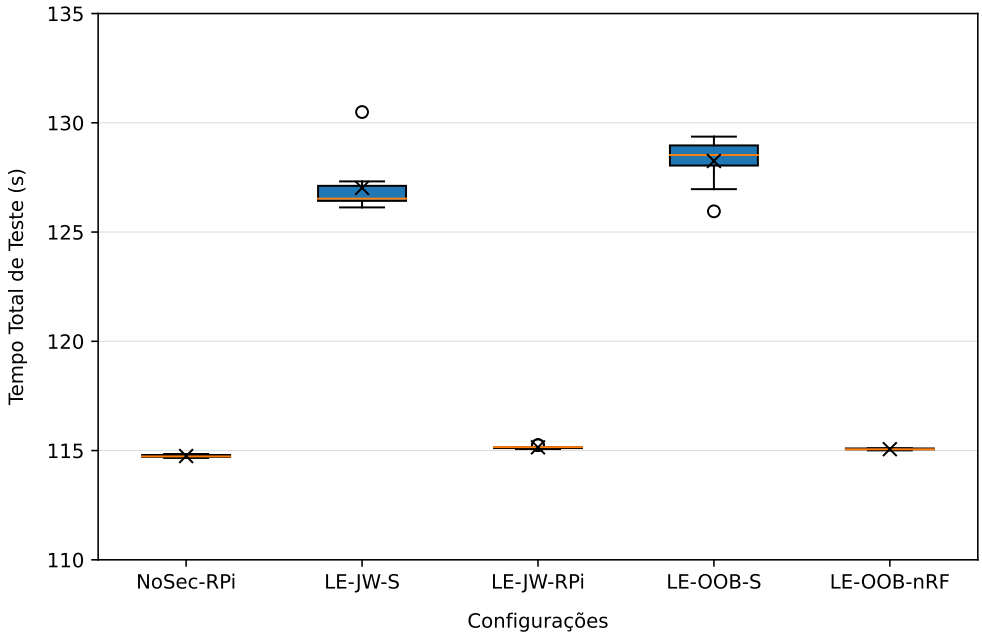

Figura 4.8: Tempo total dos testes em função das diferentes configurações. A média é indicada com o símbolo "×".

A Fig. 4.9 apresenta a taxa de aquisição em Hz obtida em função de cada característica do servidor para as diferentes configurações de teste. Neste gráfico está também presente o valor expectável da taxa de aquisição para cada uma das características, cujo valor foi apresentado anteriormente na Tabela 3.2. Neste gráfico é possível observar que as configurações que tiveram um menor desempenho em termos de aquisição foram as configurações LE-JW-S e LE-OOB-S, ambas as configurações que utilizam o *smartphone*, revelando que o *smartphone* apresenta limitações, não sendo, por isso, o dispositivo indicado para realizar a aquisição dos dados. Relativamente às características, como expectável, as características que apresentaram uma taxa de aquisição mais discrepante foram aquelas cuja taxa tem um valor mais elevado (IMU, Respiração 1, Respiração 2 e ECG). Este comportamento deve-se ao tempo de envio entre pacotes ser muito curto, o que faz com que muitos pacotes tenham que ser transmitidos num curto intervalo de tempo, fazendo com que existam problemas de *queues* e alguns pacotes tenham que ser retransmitidos, levando a que a taxa de aquisição seja diminuída. Como é possível visualizar no gráfico, para as características com menor taxa de aquisição (Frequência Cardíaca, Temperatura e Nível de Bateria), a variação entre a taxa de aquisição esperada e obtida é quase nula (desvio máximo de 0.023 Hz para a Frequência Cardíaca, 0.001 Hz para a Temperatura e 0.012 Hz para o Nível de Bateria). Assim, estes resultados foram bastante conclusivos, permitindo validar que, pelo menos, as configurações que não envolvem o *smartphone*, mostram-se muito competentes no cumprimento da

frequência de aquisição dos dados, não causando atrasos significativos na transmissão dos pacotes. Com este gráfico é também possível concluir que a introdução dos mecanismos de segurança não revelaram uma influência no desempenho do sistema relativamente à taxa de aquisição dos dados transmitidos.

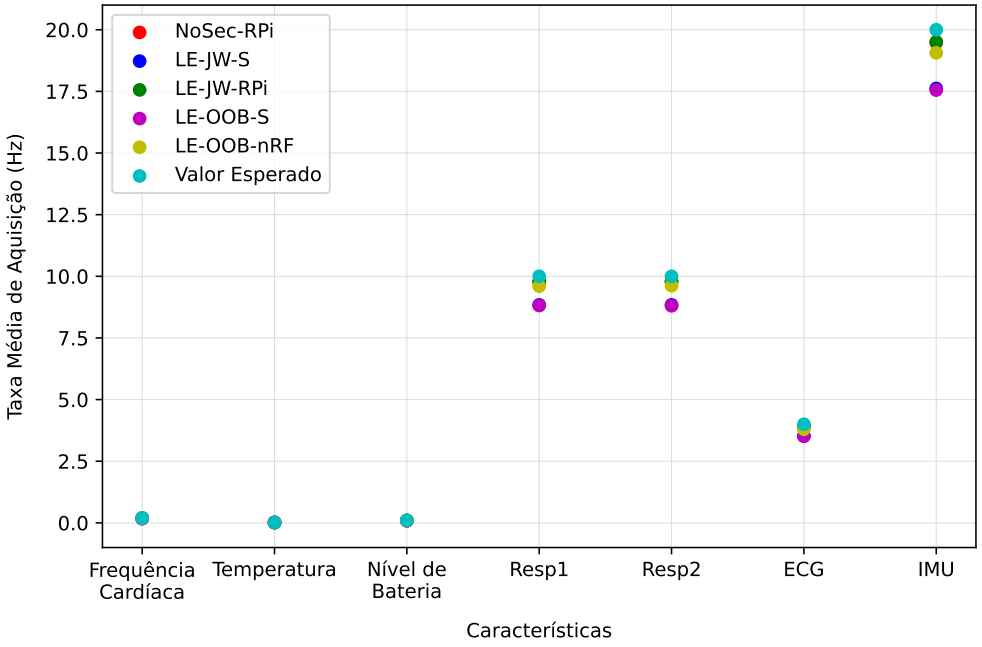

Figura 4.9: Taxa média de aquisição alcançada em cada configuração por característica do servidor.

Na Fig. 4.10 é apresentado um gráfico que representa o tamanho do *payload* em bytes dos pacotes BLE transmitidos nas diversas configurações em função das características do servidor. Nesta figura observa-se que o tamanho do *payload* dos pacotes transmitidos não sofreu variações com a introdução dos mecanismos de segurança (o tamanho dos *payloads* mantiveram-se constantes com 9 bytes para a Frequência Cardíaca, 12 bytes para a Temperatura, 11 bytes para o Nível da Bateria, 15 bytes para a Respiração 1 e 2, 13 bytes para o ECG e 8 bytes para a IMU). O motivo deve-se ao facto do Protocol Data Unit (PDU) dos pacotes BLE não conter qualquer campo referente à segurança do pacote, como é possível verificar na Fig. 4.11. O PDU é a unidade fundamental de troca de dados entre dispositivos, isto é, após conexão, os dados são transmitidos entre os dispositivos através de PDUs, que carregam os dados transmitidos e muitas outras informações sobre o pacote, como endereços ou *opcodes*. Assim, é possível concluir que os mecanismos de segurança não impõem nenhum *overhead* no tamanho dos *payloads* dos pacotes transmitidos. Isto permite também justificar a surpreendente conclusão observada anteriormente no tempo total de teste, pois como os pacotes não apresentam variação no tamanho do *payload*, o tempo total de teste não

será também significativamente incrementado, sendo a ligeira variação observada motivada apenas pela duração do emparelhamento.

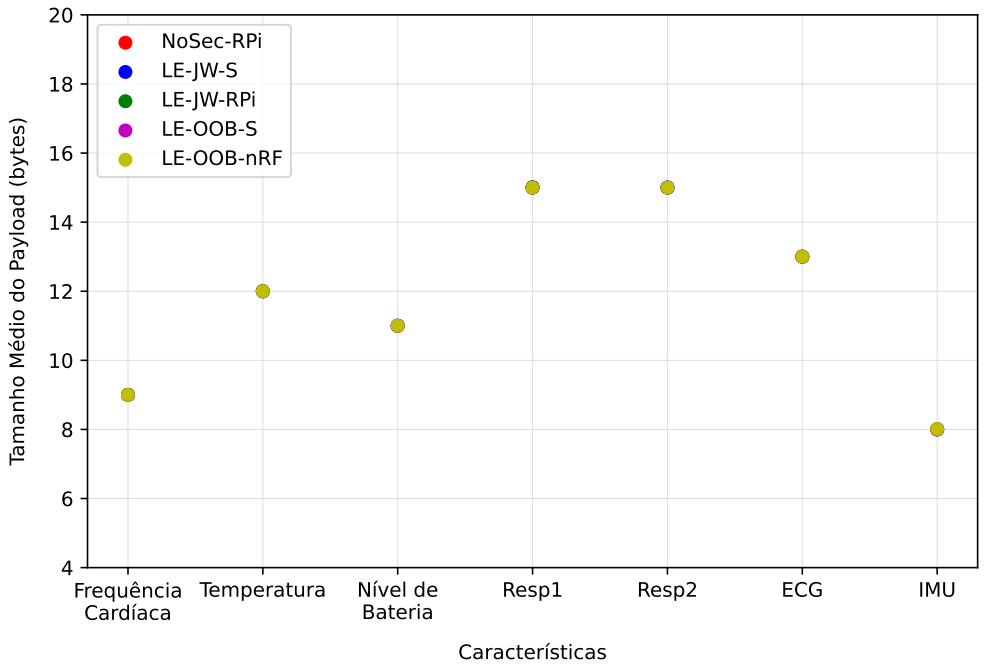

Figura 4.10: Tamanho médio do *payload* dos pacotes transmitidos obtido em cada configuração em função das diferentes características do servidor.

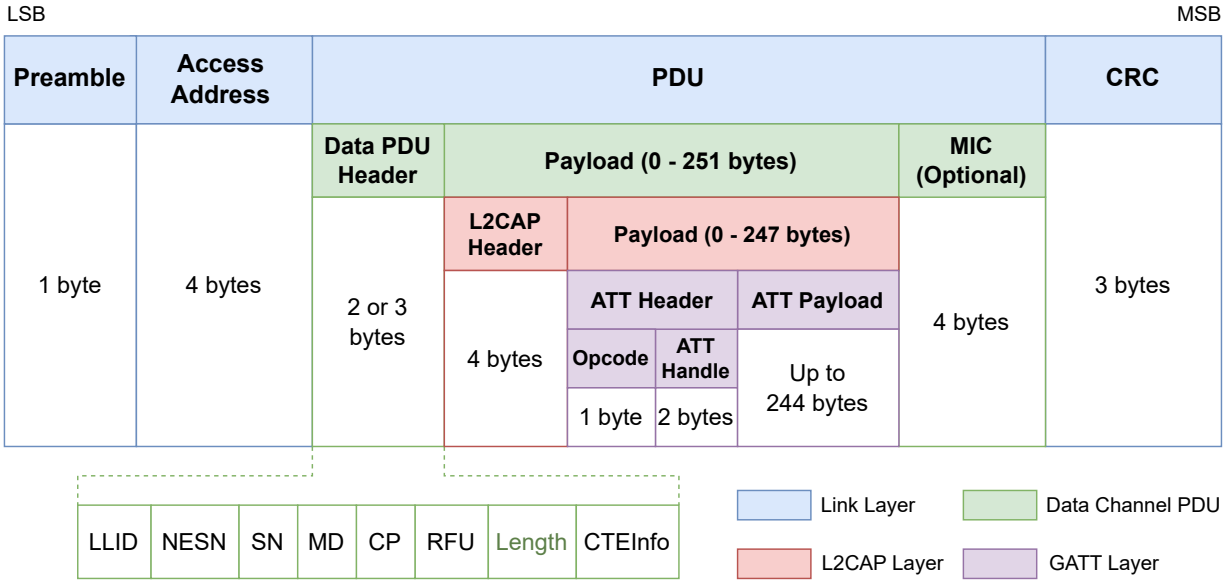

Figura 4.11: Formato de um pacote BLE. Adaptado de [10, 13]. O campo 'Length' no Data PDU Header indica o tamanho do *payload* do pacote BLE mais o tamanho do MIC, caso este seja utilizado.

4.3 Sumário

Neste capítulo validou-se o trabalho desenvolvido ao longo desta dissertação e analisou-se detalhadamente os resultados alcançados. Esta análise permitiu concluir que os sistemas seguros implementados mantêm baixa perda de pacotes e elevada taxa de aquisição relativamente ao sistema não seguro, demonstrando o comportamento pretendido na transmissão e aquisição segura dos dados. Desta forma, ficou comprovado que a introdução dos mecanismos de segurança não implica um *overhead* significativo na comunicação, nem diminui substancialmente o desempenho do sistema.

Verificou-se que a segurança apresenta um impacto positivo na comunicação, não exigindo muitos mais recursos do sistema para a transmissão e aquisição segura dos dados, e permitindo assegurar as comunicações e privacidade dos dados. Assim, é possível averiguar que foi corretamente realizada uma consolidação da segurança do sistema, que, por sua vez, aumenta a robustez da comunicação e diminui a probabilidade de os dados serem acessados por pessoas não autorizadas. Para visualização e melhor perceção do trabalho desenvolvido nesta dissertação, foi criado um vídeo demonstrativo do trabalho[18].

No próximo e último capítulo são apresentadas as principais conclusões e é realizada uma revisão crítica acerca do trabalho desenvolvido tendo em conta as contribuições propostas inicialmente, finalizando com possíveis direções para trabalho futuro.

[18]Vídeo demonstrativo do trabalho realizado na dissertação, `https://www.youtube.com/watch?v=ghw_MwN6M5Y`

5 Conclusão

Com vista à robustez de sistemas digitais de cuidados de saúde contra ciberataques, foi proposto e implementado neste trabalho um sistema de transmissão de sinais vitais seguro.

Inicialmente foi realizado um estudo de literatura em trabalhos relacionados com o tema, com foco especial em aplicações ligadas aos cuidados de saúde que utilizassem a tecnologia de comunicação sem fios *Bluetooth*. Com esta revisão da literatura foi possível ter uma perceção do estado da arte atual e com isso em mente identificar os problemas, criar soluções para os resolver, definir metas e objetivos e declarar as contribuições deste trabalho.

Relativamente à implementação, o planeamento definido inicialmente sofreu algumas alterações e o mesmo teve de ser ajustado, principalmente pelo facto do sistema operativo utilizado nos dispositivos do projeto WoW não suportar o método de emparelhamento pretendido para implementar comunicação BLE segura neste trabalho. Contudo, a migração de sistema operativo foi também uma das principais oportunidades, pois o Zephyr mostrou-se um sistema operativo de elevado desempenho e com um ótimo suporte. Com isto, este trabalho serviu como fator persuasivo para a equipa de desenvolvimento dos *biostickers* (adesivos eletrónicos) do projeto WoW atualizar o sistema operativo utilizado e assim capitalizar o *firmware* desenvolvido neste trabalho. Para a aplicação em ambiente real fica apenas em aberto o desenvolvimento dos *drivers* necessários para a utilização dos sensores com o Zephyr (fora do escopo deste trabalho).

Conclui-se por isso que o trabalho desenvolvido nesta dissertação foi de encontro à proposta realizada inicialmente, contribuindo positivamente para a literatura em segurança de sistemas de transmissão e aquisição de dados BLE ligados à área da saúde. Todas as tarefas propostas neste trabalho foram alcançadas com sucesso, permitindo não só melhorar o sistema atualmente utilizado no projeto WoW, bem como retirar diversas conclusões da análise realizada entre os diferentes níveis de segurança passíveis de implementação no sistema.

5.1 Principais Resultados

De uma forma geral, os resultados alcançados neste trabalho mostraram que os sistemas desenvolvidos apresentam uma segurança muito superior ao sistema sem segurança atualmente utilizado no projeto WoW, uma vez que incluem mecanismos de segurança como encriptação, autenticação e emparelhamento físico. Este era o principal objetivo deste trabalho, dado que a segurança é um requisito tão importante num sistema sensível como em cuidados de saúde, que envolvem dados pessoais com elevada necessidade de proteção.

Com este trabalho foi também possível verificar que a introdução dos mecanismos de segurança não prejudicou a transmissão dos sinais vitais, nem adicionou um consumo excessivo no tempo de transmissão ou outro qualquer tipo de *overhead* no sistema. Embora a segurança dos dados seja a prioridade do sistema, pois estes não podem ser expostos de forma alguma a pessoas não autorizadas, foi também importante concluir com este trabalho que a introdução de mecanismos de segurança apenas apresenta vantagens para o sistema, sendo assim obrigatória a sua utilização para um bom funcionamento e cumprimento das exigências de proteção de dados, privacidade e segurança.

5.2 Trabalho Futuro

Existem possíveis melhorias que poderiam aperfeiçoar ainda mais o sistema ao nível da robustez e da segurança. A primeira solução passaria pela implementação do emparelhamento LE Secure Connections com método OOB via NFC com a Raspberry Pi, que está integrada no projeto WoW como módulo de aquisição de dados. Como descrito anteriormente na Secção 4.1, não foi possível implementar este emparelhamento na Raspberry Pi, embora este tenha sido utilizado com o *smartphone* e nRF52 DK. Como foi possível concluir com este trabalho, este método mostrou-se, como expectável, o método de emparelhamento mais seguro da tecnologia BLE e não impõe consumos extras relativos à comunicação não segura, sendo portanto o método mais indicado a utilizar no projeto.

Uma segunda direção de trabalho passaria pela investigação da possibilidade e utilidade de um modo de segurança BLE misto, ou seja, com Modo 1 e Modo 2 de segurança BLE (ver Tabela 2.1), introduzindo no sistema assinatura de dados (*data signing*). A introdução deste mecanismo de segurança permitiria autenticar o remetente dos dados enviados e garantir que os mesmos não foram adulterados durante a transmissão, mesmo com a ligação não encriptada, aumentando ainda mais a segurança do sistema como pretendido.

6 Bibliografia

[1] Jozef Mihalov, Viera Stopjakova, Roman Zalusky, and Libor Majer. Multi-platform wireless measurement system for continuous biomonitoring. In *2013 23rd International Conference Radioelektronika (RADIOELEKTRONIKA)*, pages 191–196. IEEE, 2013.

[2] Fernanda Famá, José N. Faria, and David Portugal. An iot-based interoperable architecture for wireless biomonitoring of patients with sensor patches. *Internet of Things*, 19:100547, 2022.

[3] World Health Organization. *Global strategy on digital health 2020-2025*. World Health Organization, 2021.

[4] European Union. Eu4health. `https://ec.europa.eu/health/`, 2021.

[5] Fan Wu, Taiyang Wu, and Mehmet Rasit Yuce. An internet-of-things (iot) network system for connected safety and health monitoring applications. *Sensors*, 19(1), 2019.

[6] Taiyang Wu, Fan Wu, Chunkai Qiu, Jean-Michel Redouté, and Mehmet Rasit Yuce. A rigid-flex wearable health monitoring sensor patch for iot-connected healthcare applications. *IEEE Internet of Things Journal*, 7(8):6932–6945, 2020.

[7] Prosanta Gope and Tzonelih Hwang. Bsn-care: A secure iot-based modern healthcare system using body sensor network. *IEEE Sensors Journal*, 16(5):1368–1376, 2016.

[8] Glintt. Wow website project. `http://inovglintt.com/financiamento/wow/`.

[9] Marco Domingues. *Interoperable and Secure IoT Architecture for Digital Healthcare: Wireless Monitoring of Untethered Patients in Smart Beds*. M.sc. dissertation, University of Coimbra, 2022.

[10] José Faria. *Wireless IoT Smart Bed System*. M.sc. dissertation, University of Coimbra, 2022.

[11] Metty Paul, Leandros Maglaras, Mohamed Amine Ferrag, and Iman Almomani. Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, 2023.

[12] Yuehong YIN, Yan Zeng, Xing Chen, and Yuanjie Fan. The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*, 1:3–13, 2016.

[13] Bluetooth SIG. Bluetooth core specification version 5.3. `https://www.bluetooth.com/specifications/specs/core-specification-5-3/`, 2021.

[14] Bluetooth SIG. The bluetooth low energy primer. `https://www.bluetooth.com/blog/introducing-the-bluetooth-low-energy-primer/`, 2023.

[15] M. Afaneh. *Intro to Bluetooth Low Energy: The Easiest Way to Learn BLE*. Amazon Digital Services LLC - KDP Print US, 2018.

[16] Rosy Swami and Prodipto Das. A new secure data retrieval system based on ecdh and hierarchical clustering with pearson correlation. *Innovations in Systems and Software Engineering*, pages 1–11, 2022.

[17] Ravi Kishore Kodali and Ashwitha Naikoti. Ecdh based security model for iot using esp8266. In *2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, pages 629–633. IEEE, 2016.

[18] Bluetooth SIG. The bluetooth le security study guide. `https://www.bluetooth.com/bluetooth-resources/le-security-study-guide/`, 2023.

[19] Shaibal Chakrabarty and Daniel W. Engels. Black networks for bluetooth low energy. In *2016 IEEE International Conference on Consumer Electronics (ICCE)*, pages 11–14, 2016.

[20] M.U. Aftab. *Building Bluetooth Low Energy Systems*. Packt Publishing, 2017.

[21] N. Gupta. *Inside Bluetooth Low Energy*. Artech House Remote Sensing Library. Artech House, 2013.

[22] K. Townsend, R. Davidson, and C. Cufí. *Getting Started with Bluetooth Low Energy*. O'Reilly, 2014.

[23] Leverege. Introduction to iot: What is wi-fi. `https://www.leverege.com/iot-ebook/iot-wifi`.

[24] H Valchanov, J Edikyan, and V Aleksieva. A study of wi-fi security in city environment. *IOP Conference Series: Materials Science and Engineering*, 618(1):012031, oct 2019.

[25] André F. Silva and Mahmoud Tavakoli. Domiciliary hospitalization through wearable biomonitoring patches: Recent advances, technical challenges, and the relation to covid-19. *Sensors*, 20(23):6835, Nov 2020.

[26] Salam Khanji, Farkhund Iqbal, and Patrick Hung. Zigbee security vulnerabilities: Exploration and evaluating. In *2019 10th International Conference on Information and Communication Systems (ICICS)*, pages 52–57, 2019.

[27] Rumen Yordanov, Rosen Miletiev, Petar Kapanakov, and Emil Lontchev. Design of a portable system for sensor data acquisition and transmission. In *2017 XXVI International Scientific Conference Electronics (ET)*, pages 1–3, 2017.

[28] Aihou Chen, Aurora Gil-de Castro, Emilio J. Palacios-García, José M. Flores-Arias, and Francisco J. Bellido-Outeiriño. In-home data acquisition and control system based on ble. In *2015 International Symposium on Consumer Electronics (ISCE)*, pages 1–2, 2015.

[29] Chao Gao and Kaixue Yao. The design and implementation of portable agricultural microclimate data acquisition system based on android platform. In *2015 8th International Symposium on Computational Intelligence and Design (ISCID)*, volume 1, pages 210–213, 2015.

[30] Peng Xuange and Xiao Ying. An embedded electric meter based on bluetooth data acquisition system. In *2010 Second International Workshop on Education Technology and Computer Science*, volume 1, pages 667–670, 2010.

[31] Ting Zhang, Jiang Lu, Fei Hu, and Qi Hao. Bluetooth low energy for wearable sensor-based healthcare systems. In *2014 IEEE Healthcare Innovation Conference (HIC)*, pages 251–254, 2014.

[32] Charalampos Doukas and Ilias Maglogiannis. Bringing iot and cloud computing towards pervasive healthcare. In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 922–926, 2012.

[33] Withings. Bpm core. `https://www.withings.com/pt/en/bpm-core`.

[34] Polar H10 | Polar Global. Polar h10. https://www.polar.com/en/sensors/h10-heart-rate-sensor.

[35] Nonin. Model 3230 bluetooth low energy. https://www.nonin.com/products/3230/.

[36] Fawwad Hassan Jaskani, Saba Manzoor, Muhammad Talha Amin, Muhammad Asif, and Muntaha Irfan. An investigation on several operating systems for internet of things. *EAI Endorsed Transactions on Creative Technologies*, 6:160386, 07 2018.

[37] Yousaf Bin Zikria, Sung Won Kim, Oliver Hahm, Muhammad Khalil Afzal, and Mohammed Y. Aalsalem. Internet of things (iot) operating systems management: Opportunities, challenges, and solution. *Sensors*, 19(8):1793, Apr 2019.

[38] Sumera Rounaq and Muhammad Iqbal. Vision, challenges and future perspectives of low constrained devices iot operating systems: A systematic mapping review. *European Journal of Engineering and Technology Research*, 5(12):107–115, 2020.

[39] Chandranshu Gupta and Gaurav Varshney. An improved authentication scheme for ble devices with no i/o capabilities. *Computer Communications*, 200:42–53, 2023.

[40] Vedat Coskun, Busra Ozdenizci Kose, and Kerem Ok. A survey on near field communication (nfc) technology. *Wireless Personal Communications*, 71, 08 2013.

[41] Gerald Madlmayr, Josef Langer, Christian Kantner, and Josef Scharinger. Nfc devices: Security and privacy. In *2008 Third International Conference on Availability, Reliability and Security*, pages 642–647, 2008.

[42] Anusha Rahul, Gokul Krishnan, Unni H, and Sethuraman Rao. Near field communication (nfc) technology: A survey. *International Journal on Cybernetics & Informatics*, 4:133–144, 04 2015.

Apêndice A

MbedOS BLE Feature

No código abaixo apresentado é possível observar as linhas de código a partir das quais é possível concluir que as versões mais recentes do sistema operativo MbedOS não suportam emparelhamento LE Secure Connections.

```
1  // Feature support
2
3  // FIXME: Enable when new function available in the pal.
4  #if 0
5
6  ble_error_t PalSecurityManager::set_secure_connections_support(
7      bool enabled, bool secure_connections_only
8  )
9  {
10     // secure connection support is enabled automatically at the stack
       level.
11     if (secure_connections_only) {
12         pSmpCfg->auth |= SMP_AUTH_SC_FLAG;
13     } else {
14         pSmpCfg->auth &= ~SMP_AUTH_SC_FLAG;
15     }
16     return BLE_ERROR_NONE;
17 }
18 #endif
19
20 ble_error_t PalSecurityManager::get_secure_connections_support(
21     bool &enabled
22 )
23 {
```

```
24 #if BLE_FEATURE_SECURE_CONNECTIONS
25     // FIXME: should depend of the controller
26     enabled = false;
27     return BLE_ERROR_NONE;
28 #else
29     enabled = false;
30     return BLE_ERROR_NONE;
31 #endif
32 }
```