Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Análise de Protocolos de Comunicação entre Dispositivos de Baixa Energia e Automóveis para Keyless Entry

Murilo Simionato Arnemann

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Orientador
Prof. Dr. Marcelo Antonio Marotta

Brasília
2023

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Análise de Protocolos de Comunicação entre Dispositivos de Baixa Energia e Automóveis para Keyless Entry

Murilo Simionato Arnemann

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Prof. Dr. Marcelo Antonio Marotta (Orientador)
CIC/UnB

Prof.a Dr.a Carla Cavalcante Koike
CIC/UnB

Prof. Dr. João José Costa Gondim
CIC/UnB

Prof. Dr. João Luiz Azevedo de Carvalho
Coordenadora do Curso de Engenharia da Computação

Brasília, 10 de Dezembro de 2023

Dedicatória

Para meus pais, meu irmão e meus avós que sempre me apoiaram em todos os meus esforços acadêmicos e pessoais.

Agradecimentos

Aos meus pais e irmão, que me perguntavam incessantemente "Como está o TCC?" todos os dias, e que me incentivaram o tempo todo durante meu tempo como aluno da Universidade de Brasília.

Aos meus amigos, que me permitiram momentos de leveza durante os estresses da vida acadêmica.

Ao professor Marcelo Marotta, por ter aceitado ser meu orientador e por sempre ter sido aberto e compreensivo para todas minhas dúvidas.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

O trabalho em questão compara três protocolos principais - BLE (Bluetooth Low Energy), NFC (Near Field Communication) e RFID (Radio Frequency Identification) - como potenciais opções para implementação em sistemas de entrada sem chave em veículos. A análise considerou fatores críticos como o alcance, a segurança e o custo dos componentes de cada protocolo. O BLE destacou-se como a opção mais viável devido ao seu alcance superior, segurança robusta e baixo custo dos componentes, tornando-se o candidato ideal para esta aplicação. Contudo, o NFC também se apresentou como uma alternativa viável, especialmente devido à sua praticidade para o usuário (uso via celular) e segurança focada na proximidade, embora tenha um alcance limitado em comparação ao BLE. Assim, é importante considerar o perfil de uso antes de fazer a escolha final. Trabalhos futuros podem incluir o desenvolvimento de protótipos para uso em veículos e a integração com dispositivos móveis para o controle de acesso.

Palavras-chave: Keyless entry, Bluetooth Low Energy, NFC

Abstract

This work compares three main protocols - BLE (Bluetooth Low Energy), NFC (Near Field Communication), and RFID (Radio Frequency Identification) - as potential candidates for implementation in keyless entry systems for vehicles. The study evaluates critical factors, including the range, security, and cost of components for each protocol. BLE emerged as the most viable option, offering superior range, robust security, and comparatively low component costs, making it the ideal candidate for this application. However, NFC also proved to be a potentially viable alternative, especially due to its user convenience (use via mobile phone) and proximity-focused security, despite its limited range compared to BLE. Therefore, the final decision should consider the usage profile. Future work may include the development of prototypes for use in vehicles and integration with mobile devices for access control.

Keywords: Keyless entry, Bluetooth Low Energy, NFC

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

O uso do chamado *keyless entry* tem se tornado cada vez mais comum em veículos automotivos. No entanto, essa forma de desbloquear e ligar o carro pode ser usada por pessoas mal-intencionadas para tomar controle do veículo. Os ataques contra essa tecnologia de destravamento de automóveis podem ser facilmente replicados utilizando componentes e softwares já disponíveis há bastante tempo no mercado [16](FRANCILLON, Aurélien; DANEV, Boris; CAPKUN, Srdjan, 2011). Além disso, com veículos cada vez mais inteligentes que armazenam informações sobre a rotina e até mesmo o movimento dos olhos de seus condutores, o problema de acesso indevido ao automóvel deixa de ser somente material e se torna também um problema para a proteção de dados [17](Zhang, Sylvia, 2018).

A principal causa desta falta de segurança vem dos algoritmos utilizados para criptografar a comunicação entre o carro e a chave. Esta última geralmente é fabricada com a longevidade da bateria em mente e, por isso, usa chips *low power* que contêm baixo poder de processamento e armazenamento. Com isso, as fabricantes ficam limitadas a algoritmos fracos e que podem ser decifrados facilmente.

1.1 Evolução da Chave do Automóvel

Os veículos automotivos foram, desde sua criação, um bem de alto valor monetário cobiçado por muitos. Desde cedo a maneira utilizada para proteger esse bem foi a chave, que ao ser inserida na ignição destravava o sistema elétrico do carro. Nos veículos atuais ela não precisa mais ser inserida na ignição, e apenas estar dentro do carro já libera o automóvel para dar partida. Em alguns casos ela já foi inclusive substituída pelos telefones celulares.

A *keyless entry* utiliza tecnologias como o Bluetooth, NFC (Near Field Communication) ou até mesmo sinais de radiofrequência para estabelecer a comunicação entre a

chave e o veículo. Isso oferece uma experiência mais conveniente para os motoristas, eliminando a necessidade de procurar uma chave física ou apertar botões em um controle remoto. Além disso, a *keyless entry* também pode incluir recursos adicionais, como ajustes automáticos dos bancos, espelhos retrovisores e configurações personalizadas para cada motorista.

É importante mencionar que, embora a tecnologia de *keyless entry* ofereça comodidade e facilidade de uso, também apresenta desafios de segurança, como ataques de *relay* e outros métodos de roubo de sinal.

1.2 Dispositivos Low Energy

Dispositivos de comunicação de baixa energia, também conhecidos como dispositivos Low Energy (LE), são uma categoria de dispositivos eletrônicos projetados para consumir quantidades mínimas de energia durante a comunicação sem fio. Esses dispositivos são amplamente utilizados em várias aplicações, como Internet das Coisas (IoT), equipamentos hospitalares, dispositivos pessoais de saúde e automação residencial.

A principal característica desses dispositivos é a eficiência energética, o que os torna ideais para aplicações que envolvem baterias ou fontes de energia limitadas. Ao minimizar o consumo de energia, esses dispositivos podem operar por longos períodos de tempo sem a necessidade de troca frequente de baterias, oferecendo maior conveniência e eficiência.

Os dispositivos Low Energy, oferecem uma ampla gama de recursos e funcionalidades, e permitem a troca de dados, o controle remoto, o monitoramento de sensores e a interação com o ambiente. Esses dispositivos são geralmente projetados para operar em curto alcance, normalmente dentro de alguns metros, o que os torna adequados para cenários de uso próximo, como transferência de dados entre smartphones e controles remoto e de acesso.

1.3 Comunicação de Dispositivos Low Energy

A comunicação de dispositivos Low Energy (LE) é uma área em constante crescimento que envolve a troca eficiente de informações entre dispositivos eletrônicos com baixo consumo de energia. Essa forma de comunicação tem impulsionado o desenvolvimento de tecnologias inovadoras, como Radio Frequency Identification (RFID), Near Field Communication (NFC) e Bluetooth Low Energy (BLE), que desempenham um papel fundamental em diversas aplicações. Essas tecnologias de comunicação LE têm impulsionado o avanço da conectividade entre dispositivos, permitindo soluções mais eficientes e inovadoras em diversas áreas.

Figura 1.1: Logo do RFID [1], NFC [2]
e BLE [18]

1.3.1 Radio Frequency Identification (RFID)

O RFID é um sistema que permite a identificação automática de objetos por meio do uso de tags e leitores. As tags RFID podem ser passivas, não possuindo fonte de energia própria, ou ativas, com uma fonte de energia interna. Elas armazenam informações que podem ser lidas e gravadas pelos leitores de RFID usando radiofrequência. Essa tecnologia é amplamente utilizada em setores como logística, controle de estoque, transporte e controle de acesso.

1.3.2 Near Field Communication (NFC)

O NFC é uma tecnologia de comunicação de curto alcance que permite a troca de dados entre dispositivos compatíveis quando estão próximos um do outro, geralmente a uma distância de alguns centímetros. O NFC combina a funcionalidade de comunicação por campo de proximidade, semelhante ao RFID, com a capacidade de interação entre dispositivos móveis. Essa tecnologia é comumente usada em pagamentos móveis, transferência de arquivos, emparelhamento de dispositivos e interações simples e intuitivas.

1.3.3 Bluetooth Low Energy (BLE)

O BLE é um protocolo de comunicação sem fio desenvolvido para oferecer uma solução de baixo consumo no espcetro do já estabelecido Bluetooth. Essa tecnologia é usada principalmente em aplicações IoT, em automação residencial e em dispositivos *wearables*. Assim como o NFC, o Bluetooth Low Energy fornece mais funcionalidades se comparado ao RFID, uma vez que estabelece uma conexão persistente entre os dispositivos. Além disso, ela possui um maior alcance para estabelecer a conexão entre as duas partes, aumentando ainda mais a gama de aplicações em que pode ser usada.

1.4 Objetivos

Este estudo tem como objetivo principal realizar uma comparação detalhada e análise criteriosa dos diversos protocolos de comunicação Low Energy disponíveis, focando em identificar aqueles que oferecem o equilíbrio ideal entre segurança robusta e eficiência no uso de recursos. O intuito é selecionar o protocolo mais adequado para a implementação de um sistema eficiente de *keyless start* especificamente para motocicletas.

Para alcançar este objetivo, a pesquisa será embasada em uma extensa revisão de documentações técnicas especializadas, análise de artigos acadêmicos já publicados na área e consulta de outras fontes de literatura relevantes ao tema. Através desta abordagem, esperamos não apenas identificar o protocolo mais eficaz e seguro, mas também contribuir com esclarecimentos valiosos para a otimização de sistemas de controle de veículos, particularmente em aplicações de motocicletas, onde a eficiência energética e a segurança são de suma importância.

1.4.1 Objetivo Geral

Analisar diferentes protocolos de comunicação em dispositivos Low Energy para verificar qual tem o melhor equilíbrio entre segurança e eficiência de recursos.

1.4.2 Objetivos Específicos

- Comparar os protocolos Bluetooth Low Energy, NFC e RFID
- Comparar o alcance entre os diferentes protocolos;
- Comparar a segurança entre os diferentes protocolos;
- Comparar o custo de implementação entre os diferentes protocolos; e
- Identificar qual a melhor opção, dentre as estudadas, para ser usada em situações de keyless entry

1.5 Motivação

A motivação deste trabalho surge de um projeto do autor com a empresa Origem, que produz motos elétricas. Durante o período de desenvolvimento do produto, foi necessário realizar um estudo sobre a comunicação entre o controle e a moto, com o objetivo de aumentar a segurança do protocolo utilizado e prevenir possíveis ataques. A ideia inicial era alterar a forma como a criptografia das mensagens era realizada, substituindo um sistema de criptografia simétrica por um assimétrico. No entanto, as limitações do processador

da chave da moto tornaram essa abordagem inviável. Portanto, decidiu-se buscar outras alternativas para o problema apresentado.

Este trabalho pretende explorar outras maneiras de aprimorar a segurança da comunicação, implementando protocolos de comunicação já estabelecidos no mercado, enquanto se mantém um baixo custo para produção em larga escala.

1.6 Estrutura do Texto

Este texto está organizado da seguinte forma: na seção 2 serão detalhadamente discutidos os conceitos por trás de alguns algoritmos de criptografia e da estrutura das camadas de rede de uma aplicação, revelando as funções de cada camada. Na seção 3, é realizada uma revisão da literatura sobre o uso dos diferentes protocolos em casos de Internet das Coisas, além de estudos sobre possíveis ameaças e melhorias para sistemas de *keyless entry*. Na seção 4, apresenta-se o contexto no qual esse trabalho se aplica e as métricas que foram usadas para comparar os três protocolos, assim como a metodologia usada para fazer essas comparações. Na seção 5, são exibidos os resultados que foram obtidos através da análise extensa da literatura e dos documentos oficiais de cada componente testado. Por fim, na seção 6, são discutidos os resultados encontrados, e também qual dos protocolos analisados se mostra como a melhor opção para ser usado em uma aplicação de *keyless entry*.

Capítulo 2

Fundamentação Teórica

Neste capítulo abordaremos conceitos importantes relacionados à criptografia simétrica e assimétrica e de camadas de rede.

2.1 Criptografia Simétrica

A criptografia simétrica, ou criptografia de chave simétrica, é um tipo de criptografia que envolve o uso de uma chave secreta responsável por criptografar e descriptografar o conteúdo da comunicação e é compartilhada entre todos que fazem parte do processo de comunicação.

Neste tipo de criptografia as partes envolvidas devem concordar em uma chave antes de iniciar a comunicação, essa chave deve ser mantida em segredo durante todo o tempo. Existem diversas abordagens para garantir que essa transmissão inicial da chave seja feita de maneira segura, e que somente os dispositivos interessados tenham acesso à ela. Entre as possíveis abordagens, as mais utilizadas são o pré-compartilhamento de chaves, a

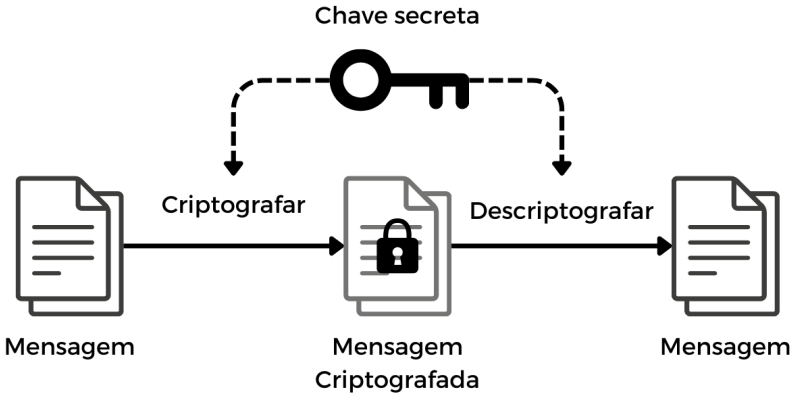

Figura 2.1: Esquema da Criptografia Simétrica

distribuição de chaves usando criptografia assimétrica e os protocolos de acordo de chave.

Pré-compartilhamento de chaves: Neste método, os dispositivos já possuem uma chave compartilhada em comum sem nunca terem se comunicado. Ela pode ter sido distribuída fisicamente na fábrica, por exemplo. O pré-compartilhamento é frequentemente usado em sistemas que exigem comunicação regular e de longo prazo entre dispositivos.

Distribuição de chaves com criptografia assimétrica: Cada dispositivo tem duas chaves, sendo uma delas privada e a outra publica. Para enviar a chave secreta, um dispositivo X pode ofuscá-la com a chave pública de Y e este, por sua vez, pode descriptografá-la com a sua chave privada.

Protocolos de acordo de chaves: Esses protocolos são projetados para permitir que dois dispositivos concordem em uma chave secreta comum, mesmo se nunca tiverem compartilhado uma chave anteriormente. Alguns exemplos populares de protocolos de acordo de chaves são o Diffie-Hellman e o ECDH (Elliptic Curve Diffie-Hellman). Esses protocolos utilizam propriedades matemáticas para garantir que a chave secreta seja a mesma para os dois dispositivos.

Os algoritmos de criptografia simétrica podem ser divididos em duas categorias principais:

- Cifras de Bloco: Esses algoritmos criptografam os dados em blocos de tamanho fixo. Os blocos são geralmente de 64 ou 128 bits. O principal algoritmo de cifra de blocos é o Advanced Encryption Standard (AES).
- Cifras de Fluxo: Esses algoritmos criptografam os dados um bit ou um byte de cada vez. São mais adequados para criptografar dados que variam em tamanho e são transmitidos ao longo de canais de comunicação com velocidades variáveis. Entre os seus principais algoritmos estão o Rivest Cipher 4 (RC4) e o ChaCha20.

Esses algoritmos costumam ser mais rápidos que os algoritmos de criptografia assimétrica. Entretanto, eles são menos flexíveis, devido à necessidade de compartilhar e gerenciar a distribuição da chave secreta.

2.1.1 Advanced Encryption Standard (AES)

O AES utiliza um tamanho de bloco fixo de 128 bits dividido em 16 bytes, garantindo a consistência na entrada de dados, independentemente de seu tamanho. Ele suporta três tamanhos de chave diferentes - 128, 192 e 256 bits - cada tamanho contribui para a segurança e o número de operações realizadas durante a criptografia e descriptografia. A quantidade de rodadas, ou ciclos de transformação, escala apropriadamente com cada tamanho de chave, sendo 10, 12 e 14 rodadas para chaves de 128, 196 e 256, respectivamente.

O algoritmo AES executa quatro principais operações que são implementadas em uma matriz chamada State. As transformações não-lineares, chamadas SubBytes; ShiftRows, que realoca elementos de cada linha de bytes; MixColumns, que envolve uma etapa de mistura de colunas; e AddRoundKey, que incorpora a chave à matriz. Ao executar essas operações em várias rodadas, o AES garante um alto nível de segurança nos dados criptografados. No processo de descriptografia, ocorre uma inversão semelhante e controlada dessas operações.

A criptografia utilizando o Padrão de Criptografia Avançada (AES, do inglês Advanced Encryption Standard) é um processo complexo e robusto, dividido em várias etapas sequenciais. Inicialmente, ocorre a expansão da chave original. Nesta fase, a chave é expandida em um conjunto de chaves de rodada através de operações de substituição e deslocamento, fundamentais para o algoritmo.

Após a expansão da chave, o processo segue para a etapa de adição da chave da rodada inicial, onde a chave derivada é combinada com o texto plano usando uma operação XOR, resultando na criação de uma matriz conhecida como State. Esta matriz contém o texto original mesclado com a chave da rodada.

Segue-se então a fase SubBytes, um passo crucial para a segurança do algoritmo. Aqui, cada byte da matriz State é substituído por outro byte, de acordo com uma tabela pré-definida chamada S-box. Esta tabela é uma matriz de 16x16 que contém todos os valores possíveis de um byte, e essa substituição garante uma transformação não-linear, aumentando significativamente a entropia e a complexidade do texto cifrado.

O próximo passo é o ShiftRows. Durante esta fase, os bytes na matriz State são deslocados ciclicamente. A primeira linha permanece inalterada, enquanto as demais linhas são deslocadas para a esquerda em um número incremental de bytes, contribuindo para a difusão do texto.

Em seguida, temos a fase MixColumns, onde cada coluna da matriz State é misturada usando uma multiplicação matricial em um campo finito. Este passo é crucial para misturar os dados de toda a coluna e, combinado com o ShiftRows, garante uma difusão ainda mais eficiente dos bytes do texto cifrado.

Após isso, a etapa AddRoundKey é repetida. A chave de rodada atual é combinada com a matriz State através de outra operação XOR. Este processo resulta em um texto cifrado intermediário, que se torna cada vez mais seguro a cada rodada repetida.

Finalmente, as etapas de SubBytes a AddRoundKey são repetidas por um número pré-definido de rodadas. Ao final dessas rodadas, alcança-se o texto cifrado final. Este processo intrincado e detalhado do AES, que está exemplificado na figura 2.2, é o que o torna um dos algoritmos de criptografia mais seguros e amplamente utilizados atualmente.

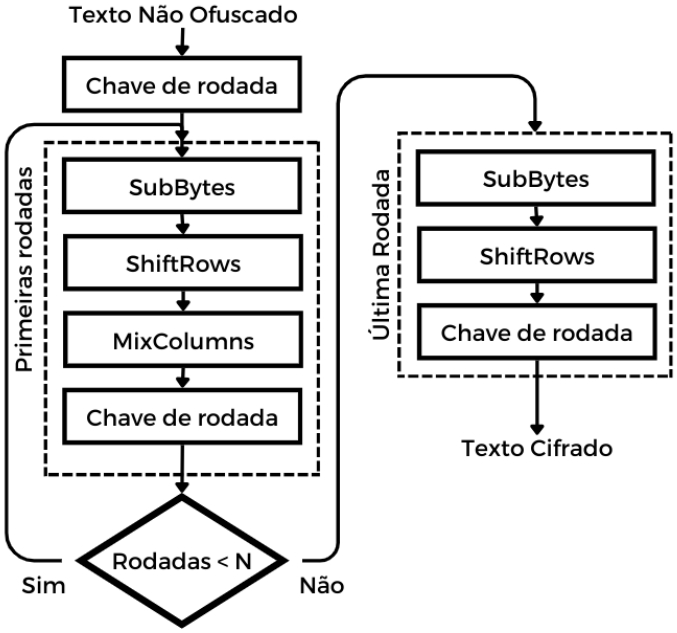

Figura 2.2: Esquema da criptografia AES

2.2 Criptografia Assimétrica

A criptografia assimétrica, é uma forma de criptografia que utiliza um par de chaves: uma chave pública e uma privada. Essas chaves estão matematicamente relacionadas, mas não podem ser deduzidas uma da outra. A chave pública pode ser amplamente divulgada, enquanto a chave privada deve ser mantida em segredo pelo proprietário.

A criptografia assimétrica é amplamente utilizada para realizar diversas operações de segurança, tais como: Operações de Confidencialidade, Autenticação e, como mencionado anteriormente, Troca Segura de Chaves.

- Confidencialidade: A chave pública é usada para criptografar os dados, garantindo que apenas o proprietário da chave privada possa descriptografá-los. Como pode ser visto na figura 2.7.
- Autenticação: A chave privada é usada para assinar digitalmente uma mensagem, fornecendo uma prova de que a mensagem veio do proprietário da chave privada e não foi alterada durante a transmissão. Como pode ser visto na figura 2.4.
- Troca segura de chaves: A criptografia assimétrica pode ser usada para estabelecer uma chave secreta compartilhada entre duas partes, que pode ser posteriormente usada para comunicações simétricas mais eficientes.

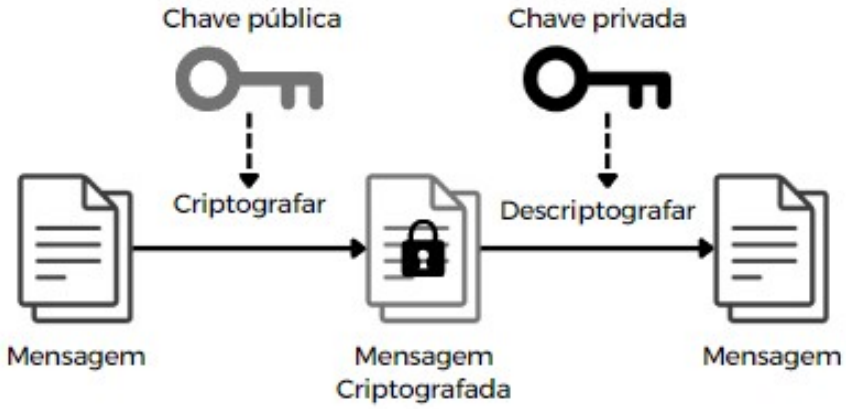

Figura 2.3: Operação de Confidencialidade

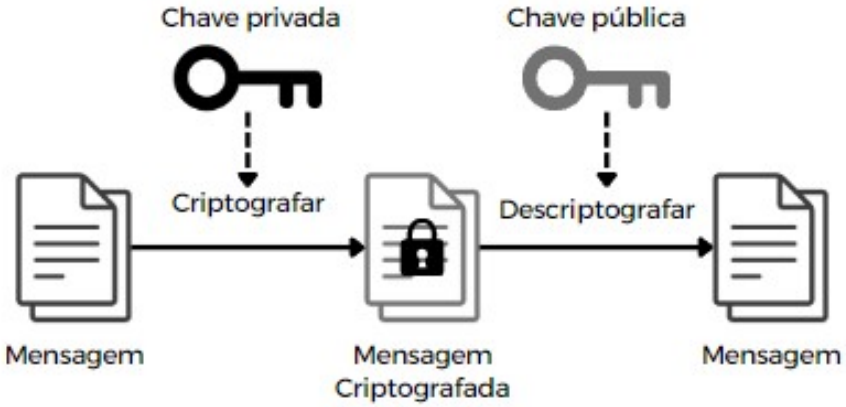

Figura 2.4: Operação de Autenticação

Existem vários algoritmos de criptografia assimétrica populares, cada um com suas próprias características e casos de uso:

Rivest-Shamir-Adleman (RSA): É um dos algoritmos mais amplamente utilizados na criptografia assimétrica. Ele se baseia na dificuldade de fatorar grandes números primos. O algoritmo RSA é frequentemente usado para criptografia digital de texto, autenticação de sistemas e criação de assinaturas digitais. Uma das principais vantagens do RSA é a sua segurança de longa data, mas em contrapartida, tem um desempenho computacional mais lento em comparação com outros algoritmos de criptografia assimétrica.

Diffie-Hellman: Este protocolo é usado para estabelecer uma chave secreta compartilhada entre duas partes em um canal de comunicação inseguro. Baseia-se no problema de logaritmo discreto e é frequentemente usado em conjunto com outros algoritmos de criptografia simétrica em sistemas de criptografia híbrida. É importante notar que o Diffie-Hellman é usado para o acordo de chaves, e não para a criptografia direta de dados ou assinaturas digitais.

Curvas Elípticas (ECC): A criptografia de curvas elípticas é uma abordagem mais recente à criptografia assimétrica que se baseia na matemática das curvas elípticas sobre campos finitos. A principal vantagem da ECC é que ela fornece o mesmo nível de segurança que outros algoritmos de criptografia assimétrica, como o RSA, com chaves significativamente menores. Isso a torna mais eficiente em termos de processamento e largura de banda. A ECC é frequentemente usada em dispositivos com recursos limitados, como smartphones, dispositivos IoT e sistemas embarcados.

2.2.1 Rivest-Shamir-Adleman (RSA)

Devido à sua resistência à fatoração de números primos grandes e ao amplo suporte da indústria, o RSA estabeleceu-se como uma escolha confiável para comunicações seguras, autenticação e assinaturas digitais. Diferente dos algoritmos de criptografia simétrica, que utilizam a mesma chave para criptografar e descriptografar a informação, o RSA utiliza um par de chaves distintas: uma pública e outra privada. A chave pública é utilizada para criptografar os dados enquanto a chave privada é empregada para descriptografá-los. Embora essas chaves sejam matematicamente relacionados, é extremamente difícil obter a chave privada a partir da chave pública, garantindo a segurança do algoritmo.

O processo de criptografia e descriptografia no RSA começa com a geração de chaves, escolhendo dois números primos grandes e multiplicando-os para formar um número semiprimo. A chave pública é derivada desse semiprimo e de um expoente, enquanto a chave privada é derivada do semiprimo e de um expoente inverso multiplicativo. Por conta disso, o algoritmo RSA depende fortemente da escolha de números primos suficientemente grandes. Além disso, embora seguro, possui um desempenho computacional relativamente mais lento em comparação com outros algoritmos de criptografia assimétrica, como a criptografia de curvas elípticas.

2.2.2 Diffie-Hellman

O protocolo Diffie-Hellman é um método utilizado para compartilhar chaves secretas através de um canal inseguro, sem que as partes tenham que trocar informações diretamente. Foi proposto por Whitfield Diffie e Martin Hellman em 1976 e é uma das primeiras implementações práticas da criptografia assimétrica.

O algoritmo se base na matemática de grupos de números no campo, e funciona da seguinte forma: Duas partes concordam em um primo grande (p) e outro número (g), conhecido como gerador, que é menor que p. Estes dois números são públicos e podem ser compartilhados. Uma das partes, vamos chamar de Alice, agora escolhe um número secreto (a), calcula $A = g^a mod p$ e envia A. A outra parte, chamada Bob, faz o mesmo

procedimento para um número secreto b. Agora, Alice e Bob podem calcular a chave secreta compartilhada realizando as operações $S = B^a mod p$ e $S = A^b mod p$, como pode ser visto na imagem 2.5.

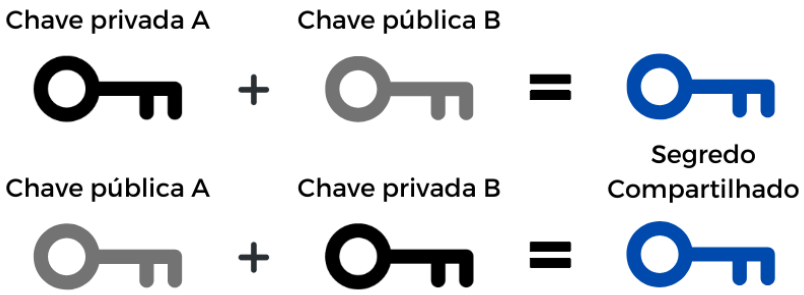

Figura 2.5: Exemplificação de criptografia Diffie-Hellman

No final do processo, os valores de S calculados por Alice e Bob serão iguais. Ambos podem usar a chave secreta compartilhada (S) para criptografar e descriptografar mensagens entre si, usando, por exemplo, um algoritmo de criptografia simétrica.Embora o protocolo Diffie-Hellman possa ser vulnerável a ataques de homem no meio, ele foi a base para o desenvolvimento de muitos outros sistemas de criptografia assimétrica, como o protocolo de troca de chaves RSA e a criptografia de curvas elípticas. Esses sistemas são frequentemente usados hoje em dia para proteger a comunicação na internet, garantindo a segurança e a privacidade dos dados trocados entre as partes.

2.2.3 Criptografia de Curvas Elípticas

A criptografia de curvas elípticas (ECC, do inglês Elliptic Curve Cryptography) é uma abordagem de criptografia de chave pública baseada na matemática das curvas elípticas sobre campos finitos. Introduzida no início dos anos 1980, a criptografia de curvas elípticas tornou-se uma alternativa popular aos sistemas de criptografia mais antigos, como RSA, devido à sua eficiência e segurança aprimoradas. As curvas elípticas são curvas planas definidas pela equação geral $y^2 = x^3 + ax + b$. Um exemplo desta curva pode ser visto na imagem 2.6

Na criptografia de curvas elípticas, as operações de soma e multiplicação são definidas de forma diferente das operações aritméticas convencionais e são baseadas na geometria da curva. Por exemplo, Adicionar dois pontos na curva resulta em um terceiro ponto que também se encontra na mesma curva. A multiplicação, por outro lado, é uma soma repetida de um ponto com ele mesmo. A base da criptografia de curvas elípticas é o problema do logaritmo discreto elíptico, que é considerado computacionalmente difícil de resolver. Isso significa que, dada uma curva elíptica, um ponto gerador G e um ponto P na

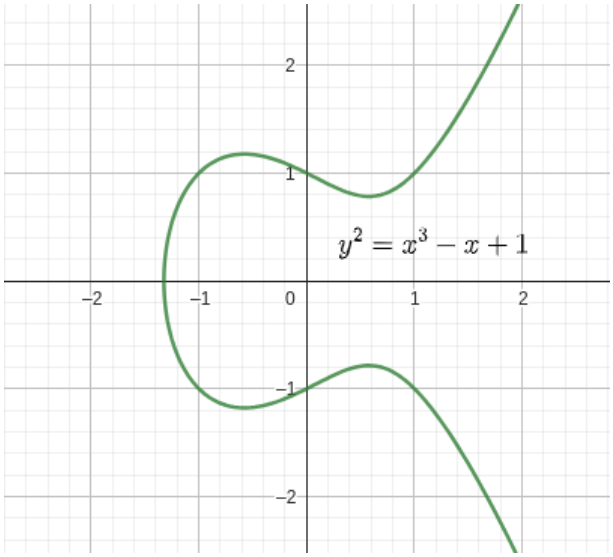

Figura 2.6: Plot de uma curva elíptica, com $a = -1$ e $b = 1$

curva, é muito difícil determinar o número inteiro k tal que $P = k * G$, onde * representa a operação de multiplicação elíptica.

A criptografia de curvas elípticas é usada em uma ampla gama de aplicações criptográficas, como troca de chaves de sessão, assinaturas digitais e criptografia de mensagens. Entre os muitos esquemas criptográficos baseados em curvas elípticas estão o ECDH (Elliptic Curve Diffie-Hellman) e o ECDSA (Elliptic Curve Digital Signature Algorithm). A principal vantagem da criptografia de curvas elípticas é que ela oferece a mesma segurança que outros esquemas, como o RSA, com chaves significativamente menores. Esta característica reduz os requisitos de memória e largura de banda, tornando a ECC uma escolha atraente para dispositivos com recursos limitados, tais como telefones celulares e dispositivos da Internet das Coisas (IoT). No entanto, as operações matemáticas em curvas elípticas são mais complicadas e podem ser mais lentas do que os métodos baseados em fatoração, como o RSA, especialmente se não forem otimizadas.

2.3 Camadas de Rede

As camadas de rede referem-se a uma abordagem estruturada usada para organizar e implementar as funcionalidades de comunicação em uma rede de computadores. Elas representam diferentes níveis de abstração e fornecem serviços específicos para garantir a transferência confiável de dados entre os dispositivos conectados em uma rede. O modelo mais comumente usado para camadas de rede é o modelo TCP/IP, que é composto por quatro camadas principais:

Camada de Aplicação: A camada de aplicação é responsável por fornecer serviços e protocolos que permitem a comunicação entre aplicativos de software em diferentes dispositivos. Ela inclui protocolos como o HTTP, SMTP e DNS.

Camada de Transporte: A camada de transporte é responsável por garantir a transferência confiável de dados entre os dispositivos finais. Ela segmenta os dados em pacotes menores, gerencia o controle de fluxo, o controle de congestionamento e fornece a confiabilidade dos dados. Alguns de seus protocolos são o TCP e o UDP.

Camada de Rede: A camada de rede é responsável por rotear os pacotes de dados entre diferentes redes. Ela define os endereços IP dos dispositivos, bem como os algoritmos e protocolos para o roteamento eficiente dos pacotes. O protocolo IP é um exemplo amplamente utilizado nessa camada.

Camada de Enlace: A camada de enlace lida com a transmissão confiável de dados entre dispositivos adjacentes na mesma rede física. Ela é responsável por garantir a integridade dos dados, a detecção de erros e o controle de acesso ao meio físico. Exemplos de protocolos de enlace incluem Ethernet e Wi-Fi.

Figura 2.7: Esquema das Camadas de Rede do Protocolo TCP/IP

Essas camadas de rede trabalham em conjunto para garantir a comunicação eficiente e confiável entre dispositivos em uma rede. Além de, permitir a modularidade e a interoperabilidade entre diferentes dispositivos e tecnologias de redes.

2.4 Discussão

O estudo aprofundado de criptografias simétricas, como o AES (Advanced Encryption Standard), e assimétricas, como o RSA (Rivest-Shamir-Adleman) e ECC (Elliptic Curve

Cryptography), desempenha um papel crucial na análise de segurança de protocolos de comunicação sem fio como NFC (Near Field Communication), BLE (Bluetooth Low Energy) e RFID (Radio-Frequency Identification). A criptografia simétrica, exemplificada pelo AES, é conhecida por sua eficiência e robustez, essencial para proteger dados em sistemas de baixo consumo energético, como os empregados em dispositivos BLE e RFID. Por outro lado, a criptografia assimétrica, especialmente nas formas de RSA e ECC, oferece vantagens únicas em termos de segurança e autenticação, fundamentais para estabelecer conexões seguras em transações NFC, onde a integridade e a confidencialidade dos dados são críticas. A compreensão desses algoritmos permite aos pesquisadores e desenvolvedores identificar e implementar as melhores práticas de segurança, adequando-as às características específicas e aos requisitos de cada tecnologia. Assim, o estudo dessas formas de criptografia não apenas fortalece a segurança dos protocolos existentes, mas também impulsiona a inovação para o desenvolvimento de novos sistemas mais seguros e eficientes.

O estudo das camadas de rede é essencial para entender os protocolos NFC, BLE e RFID, pois permite analisar como os dados são manipulados, transmitidos e protegidos em cada etapa da comunicação. Na camada física, foca-se nas especificações de transmissão de sinais e hardware. Na camada de enlace, explora-se o formato de dados, controle de acesso e correção de erros, cruciais para a eficiência da transmissão. Nas camadas superiores, questões de roteamento e segurança, como criptografia, são vitais para a proteção dos dados. Esse entendimento abrangente das camadas de rede não apenas revela aspectos técnicos fundamentais de cada tecnologia, mas também facilita a integração e otimização desses protocolos em sistemas mais complexos, realçando sua funcionalidade e segurança.

Em conclusão, a seção de Fundamentação Teórica abordou com profundidade as nuances das criptografias simétrica e assimétrica, destacando o AES, RSA e ECC, e examinou detalhadamente as camadas de rede, enfatizando sua relevância no funcionamento de protocolos como NFC, BLE e RFID. O entendimento da criptografia simétrica e assimétrica é crucial para apreciar as estratégias de segurança aplicadas na transmissão de dados, enquanto a análise das camadas de rede oferece uma perspectiva essencial sobre a manipulação, transmissão e proteção dos dados em diferentes níveis. Esta combinação de conhecimentos proporciona uma base sólida para compreender não apenas o funcionamento técnico dessas tecnologias, mas também as implicações práticas em termos de segurança e eficiência. Tal compreensão é indispensável para o desenvolvimento, aprimoramento e aplicação efetiva desses protocolos em sistemas de comunicação modernos.

Capítulo 3

Trabalhos Relacionados

Há uma variedade considerável de estudos publicados com diferentes abordagens sobre a segurança e desempenho de protocolos de comunicação com dispositivos low energy. Essas pesquisas abrangem desde protocolos já conhecidos, como o ZigBee, até a proposta de criação de novos protocolos baseados no padrão IEEE Low Consumption. Neste contexto, o presente trabalho propõe uma revisão aprofundada da literatura, com ênfase nos estudos que discutem o uso de tecnologias já estabelecidas no mercado para aplicações em IoT e dispositivos LE. A análise deles permitirá compreender as potencialidades e limitações de diferentes abordagens.

3.1 Protocolos de comunicação em IoT

No estudo realizado por Al-Sarawi, Anbar, Alieyan e Mahmood Alzubaidi [3], são apresentadas comparações de diferentes protocolos de comunicação comumente utilizados em aplicações de internet das coisas. O artigo faz uma breve introdução dos protocolos que irá analisar, dividindo-os de acordo com o tipo de rede que utilizam, como Low Power Wide Area Network (LPWAN) e Short Range Network que é onde os objetos de estudo desta monografia se encaixam.

O estudo tem como objetivo revisar e comparar diferentes protocolos de comunicação utilizados em aplicações de Internet das Coisas (IoT) e oferecer diretrizes para os pesquisadores escolherem o protocolo adequado para diferentes aplicações de IoT. A implementação do IoT requer protocolos de comunicação que possam gerenciar eficientemente as restrições de capacidade de processamento, volume de armazenamento, vida útil da energia e alcance do rádio. Portanto, o estudo foi realizado para analisar e comparar protocolos de comunicação IoT para fornecer insights sobre seus prós e contras, consumo de energia, velocidade e alcance.

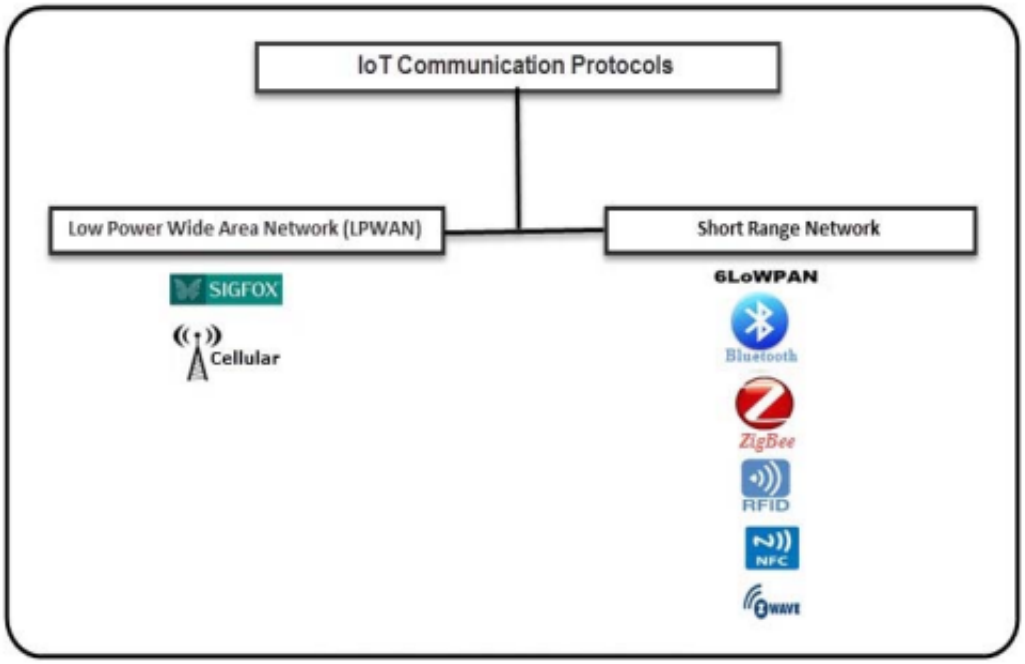

Figura 3.1: Protocolos de Comunicação vistos em Al Sarawi[3]

O estudo destaca quais os melhores tipos de aplicações para cada protocolo. Para implementações de baixo consumo ele cita o 6LoWPAN, ZigBee, BLE, Z-Wave e o NFC, uma vez que eles foram feitos pensando em dispositivos portáteis e com bateria limitada. Já no quesito de segurança ele menciona que os protocolos que utilizam o AES-CTR (counter mode, em que os blocos são processados de maneira paralela) são mais seguros e mais lentos do que os que utilizam o RC4. Entre aqueles que usam o AES-CTR está o NFC, enquanto o RFID utiliza o RC4.

Este estudo permite que o leitor crie uma fundamentação teórica para se guiar quando for escolher algum dos diversos protocolos de comunicação disponíveis. Além disso, o autor apresenta as aplicações em que cada protocolo são comumente utilizados.

3.2 Segurança dos Protocolos usados em IoT

O artigo de Tournier e Lesueur [4] é um levantamento de protocolos e suas questões de segurança, com o objetivo de oferecer uma abordagem genérica para comparar as *stacks* dos protocolos e descrever ataques dentro desse modelo abstrato. Ele analisa e compara pesquisas existentes relacionadas à segurança de dispositivos IoT, categorizando-as em três grupos: aquelas focadas em uma stack única de protocolos, as focadas em comparações à nível de camada e aquelas focadas na segurança de todo o sistema.

O texto foi idealizado com o intuito de abordar as questões de segurança fundamentais das redes IoT, independentemente da pilha de protocolos utilizados. O estudo visa consolidar o trabalho heterogêneo existente sobre os protocolos e segurança da Internet das Coisas em uma estrutura coerente, se concentrando em dois desafios principais: identificar uma abordagem genérica para comparar os stacks de protocolos, e encontrar uma maneira genérica de descrever ataques independentemente do protocolo.

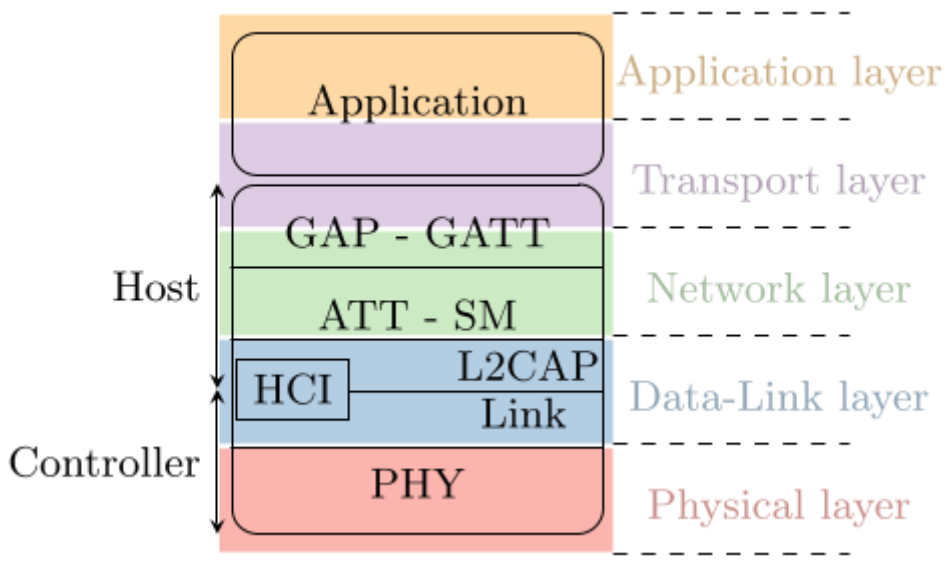

Figura 3.2: Pilha do Bluetooth Low Energy na pilha genérica de Tournier [4]

Para realizar as comparações e enfrentar o primeiro desafio, os autores definiram uma pilha genérica para comparar os protocolos com a seguinte estrutura: camada física e camada de link de dados, que especificam as funcionalidades da frequência de rádio; camada de rede, que define o roteamento e a segurança; e as camadas de transporte e de aplicação que especificam os comandos disponíveis em cada protocolo. Já para o segundo desafio, os autores dividem os ataques em três partes: ataques de pacotes, de protocolo e de sistemas, que são testados com o auxílio da pilha genérica de protocolos. Com isso, foi possível categorizar os ataques e estimar quais poderiam ser feitos de maneira semelhante contra outro protocolo e quais protocolos eram resistentes.

O artigo fornece uma visão bem recente do estado da segurança dos diferentes protocolos, como visto em 3.3, utilizados por sistemas de Internet das Coisas, além de criar um contexto para que se possa ser feita uma comparação justa entre os mesmos. Para o desenvolvimento deste trabalho, os dados levantados por Tournier são de extrema importância visto que sua comparação profunda da segurança e da pilha de cada protocolo permitiram fazer uma análise extremamente objetiva dos protocolos aqui estudados.

Table 2
IoT protocol summary.

		Protocolos						
		OS4I	BLE	ZigBee	Z-Wave	WirelessHart	LoRaWAN	SigFox
Features	Alcance	LAN < 100 m	LAN < 100 m	LAN < 100 m	LAN < 100 m	LAN < 100 m	WAN ~5 km	WAN ~10 km
	Openness	Open	Half-open	Half-open	Close	Close	Close	Close
	Interoperabilidade	Sim	Não	Não	Não	Não	Não	Não
	Topologia	Star, tree, mesh	Star, mesh	Star, tree, mesh	Mesh	Mesh	Cellular	Cellular
	Práticas Seguras	Sim	Sim	Sim	Não	Não	Não	Não
	Throughput	250 Kbps	100 Mbps	250 Kbps	40 Kbps	250 Kbps	50 Kbps	100 bps
	Banda de Freq.	2.4 GHz	2.4 GHz	2.4 GHz	sub-GHz	2.4 GHz	sub-GHz	sub-GHz
	Máximo de nós	Milhares	32,000	64,000	232	30,000	10^4 / BS	10^6 / BS
	Multi-hop	Sim	Sim/Não	Sim	Sim	Sim	No	Não
	Autenticação	Sim	Sim/Não	Sim	Sim	Sim	Sim	Não
	Criptografia	AES-CCM	AES-CCM	AES-CCM	AES-CCM	AES-CCM	AES	Não

Figura 3.3: Sumário dos Protocolos de Comunicação estudados em Tournier [4]

3.3 Comparação da desempenho do BLE e do RFID

O estudo de Gendy et al. [5] discute a implementação de soluções IoT autônomas, de baixo custo e baixo consumo de energia para rastrear contato entre pessoas em ambientes hospitalares e de escritórios. As soluções propostas utilizam o Bluetooth Low Energy e o RFID para medir a distância entre funcionários e para rastrear a presença deles em áreas internas. Para avaliar cada solução os autores consideraram a força do sinal (RSSI) de cada dispostivo e sua acurácia em perceber se havia uma pessoa presente na sala.

O estudo em questão foi conduzido durante a pandemia de COVID-19, que teve impacto significativo em vários aspectos das vidas das pessoas. O objetivo do estudo foi de desenvolver um sistema que prevenisse contaminação de pessoal ao medir a proximidade entre pessoas, ao mesmo tempo que minimiza qualquer inconveniência aos indivíduos, como fazer check-in em aplicativos, por exemplo. O estudo visava abordar as limitações dos métodos tradicionais de rastreamento de contato manual e fornecer uma solução mais eficiente e escalável.

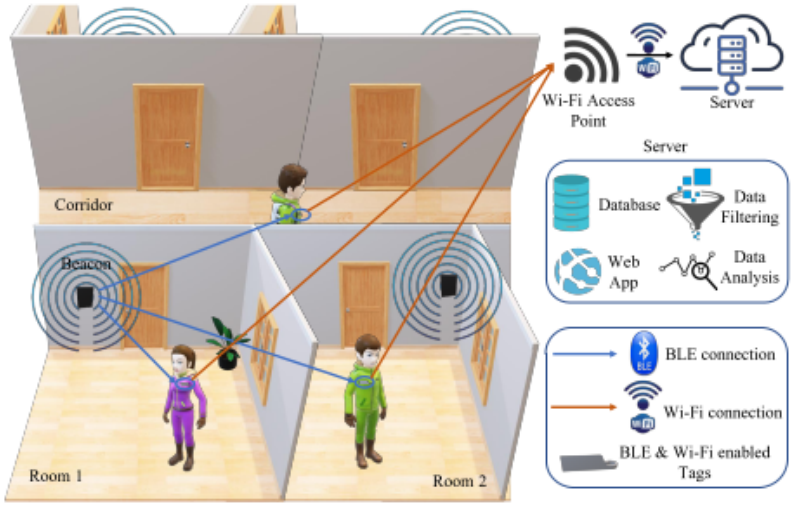

Figura 3.4: Esquema do estudo aplicado por Gendy [5]

O estudo revela que a combinação de BLE e RFID oferece uma solução mais eficaz e econômica. Experimentos em diferentes cenários confirmam a eficiência de ambos os sistemas em condições reais. A pesquisa conclui que a integração de BLE e RFID resulta em uma solução eficiente de rastreamento de contatos, com baixo custo, simplicidade e longa vida útil da bateria.

Este trabalho é de extrema ajuda para a presente tese, pois oferece esclarecimentos sobre a combinação do uso de BLE e RFID em sistemas de rastreamento de contatos. As descobertas e metodologias aplicadas neste estudo fornecem uma base sólida para a pesquisa em pauta, cujo objetivo é desenvolver soluções inovadoras e eficazes para a detecção da proximidade de dispositivos, com foco nas tecnologias IoT.

3.4 Protocolo para o uso seguro de Keyless entry

O estudo de Glocker et al. [15] descreve um protocolo seguro para um sistema de entrada remota sem chave em veículos. O sistema é composto por um transceptor automotivo e um chaveiro com interface de programação. O protocolo emprega criptografia simétrica e um algoritmo de criptografia leve para garantir a segurança das comunicações sem fio entre o chaveiro e o transceptor do carro. O protocolo proposto oferece várias vantagens em comparação a outros protocolos comumente utilizados em sistemas de entrada remota segura, como facilidade de implementação, eficiência energética e proteção contra diferentes tipos de ataques.

O estudo foi conduzido motivado pela crescente necessidade de fortalecer a segurança dos sistemas de entrada sem chave, que estão se tornando alvos frequentes de ataques cibernéticos. Tais ataques exploram as fraquezas dos métodos de autenticação padrão, comprometendo a segurança dos veículos e de seus condutores.

O estudo introduz um algoritmo de criptografia leve e fornece uma análise comparativa detalhada com as técnicas de autenticação existentes. Os autores concluem que o novo protocolo reduz consideravelmente a probabilidade de ataques bem-sucedidos, como o *Scan, Playback* e Previsão. Ademais, o protocolo proposto é destacado por sua eficiência energética e facilidade de implementação. Para os resultados, os autores testaram o seu protocolo contra outros três protocolos comumente utilizados nesse cenário: código fixo, *rolling code* e desafio-resposta. Então, cada ataque foi classificado de acordo com a sua facilidade de ser executado contra os protocolos como fácil (0), difícil (1), muito difícil (2) e extremamente difícil (3). Os resultados foram apresentados na tabela 3.1.

Este artigo é especialmente relevante para a presente tese, que foca na segurança cibernética em sistemas automotivos. O protocolo apresentado oferece uma perspectiva valiosa sobre como aumentar a segurança nos sistemas de entrada sem chave, um aspecto

Tabela 3.1: Nível de diferentes ataques vs. técnicas de autenticação. Fácil (0), Difícil (1) e Muito Difícil (2). Fonte: [15]

	Código Fixo	**Rolling Code**	**Desafio Resposta**	**Protocolo Proposto**
Scan Attack	1	1	2	3
Playback Attack	0	1	2	3
Fwd. Pred. Attack	0	1	2	3

crucial no contexto da segurança veicular moderna. Além disso, o enfoque na criptografia simétrica e a análise de vulnerabilidades são diretamente aplicáveis ao âmbito da pesquisa em questão.

3.5 Algoritmos de criptografia leves para dispositivos IoT

O artigo de Singh et al. [6] discute a importância da criptografia leve para dispositivos IoT devido às suas restrições de recursos, como poder computacional limitado, vida útil da bateria e tamanho reduzido. Destaca os desafios enfrentados pelo IoT, tais como o manuseio de grandes volumes de dados, consumo de energia e ameaças de segurança. Também apresenta uma revisão de algoritmos de criptografia leves para dispositivos IoT. Propõem um novo esquema híbrido de algoritmo leve, combinando criptografia simétrica e assimétrica, otimizado para ambientes de IoT com recursos limitados.

A motivação do estudo advém da crescente necessidade de proteção de dados em dispositivos IoT, que geralmente têm limitações expressivas de memória, capacidade computacional e energia. Com o aumento do número de dispositivos inteligentes conectados em um ambiente IoT, há uma demanda crescente pelo uso de soluções criptográficas adequadas para proteger os dados transmitidos. A pesquisa busca soluções que equilibrem segurança e eficiência em recursos. A figura 3.5 mostra algumas características dos algoritmos leves e simétricos analisados pelo estudo.

O estudo apresenta uma análise detalhada de vários algoritmos existentes, enfatizando a necessidade de soluções que minimizem o consumo de energia e a complexidade computacional. O artigo propõe um Algoritmo Híbrido Leve (HLA) que combina algoritmos de criptografia simétrica e assimétrica leves para dispositivos IoT. O HLA é projetado para otimizar o uso de recursos limitados, como memória e energia, mantendo a segurança dos dados. O HLA analisa quatro parâmetros críticos de dispositivos IoT: tamanho dos

Algoritmo	Chave	Bloco	Estrutura	Rodadas
AES	128/192/256	128	SPN	10/12/14
HEIGHT	128	64	GFS	32
PRESENT	80/128	64	SPN	31
RC5	0–2040	32/64/128	Feistel	1–255
TEA	128	64	Feistel	64
XTEA	128	64	Feistel	64
LEA	128,192,256	128	Feistel	24/28/32
DES	54	64	Feistel	16
Seed	128	128	Feistel	16
Twine	80/128	64	Feistel	32
DESL	54	64	Feistel	16
3DES	56/112/168	64	Feistel	48
Hummingbird	256	16	SPN	4
Hummingbird2	256	16	SPN	4
Iceberg	128	64	SPN	16
Pride	128	64	SPN	20

Figura 3.5: Algortimos simétricos avaliados por Singh et al. [6]

dados, poder da bateria, espaço de memória e capacidade de processamento. Com base nestes parâmetros, o algoritmo determina a melhor abordagem de criptografia para um dispositivo específico. O HLA é particularmente adequado para ambientes com dispositivos de baixa capacidade, como redes de sensores sem fio e sistemas de identificação por radiofrequência (RFID), fornecendo uma solução de criptografia segura e eficiente em termos de recursos para o crescente ecossistema de dispositivos IoT.

Este artigo oferece uma contribuição significativa para o campo da criptografia em dispositivos IoT, apresentando um esquema que equilibra segurança e eficiência de recursos, um aspecto fundamental na minha pesquisa sobre segurança de dados em dispositivos IoT com capacidade limitada.

3.6 Segurança do Bluetooth Low Energy em dispositivos IoT

O estudo de Arup Barua et al. [7] se concentra nos desafios de segurança e privacidade associados ao uso de tecnologia Bluetooth Low Energy (BLE) em dispositivos IoT e wearables. O artigo explora várias ameaças à segurança e vulnerabilidades que po-

dem comprometer a integridade e a confidencialidade dos dados transmitidos por esses dispositivos.

A pesquisa foi motivada pelo uso cada vez maior de dispositivos BLE em aplicativos críticos, como sistemas de saúde e dispositivos vestíveis, onde a segurança e a privacidade são de suma importância. A necessidade de entender e mitigar as vulnerabilidades do BLE em ambientes IoT é essencial para garantir a proteção de informações sensíveis.

O artigo oferece uma análise abrangente das técnicas de ataque comuns, incluindo ataques de *man-in-the-middle*, *eavesdropping* e *spoofing*, em que um agente malicioso desfaz uma conexão e toma o lugar de um dos dispositivos (representado na figura 3.6). Além disso, discute as medidas de segurança atuais e suas limitações, sugerindo melhorias nas práticas de segurança para BLE, como por exemplo, evitar o uso do método *Just works* para estabelecer uma conexão e transmitir todos dados criptografados com AES-128. O estudo conclui que, embora o BLE ofereça benefícios significativos em termos de eficiência energética e custo, é crucial reforçar suas medidas de segurança para prevenir violações de dados em aplicativos críticos.

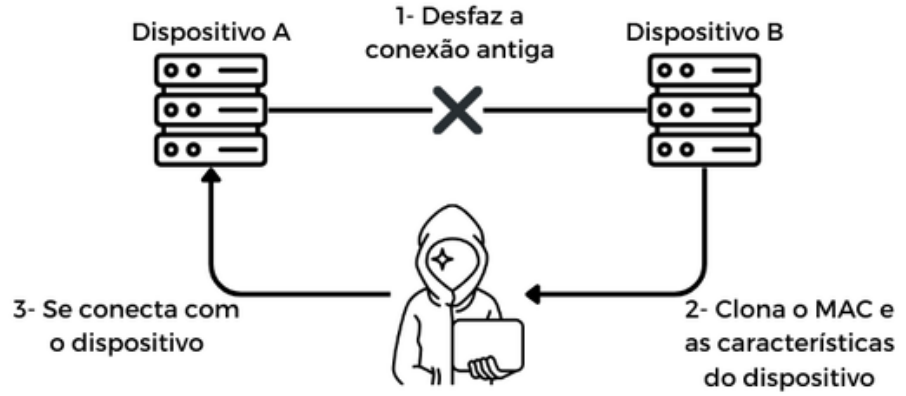

Figura 3.6: Funcionamento de um ataque de *spoofing* por Barua et al. [7]

O estudo proporciona uma compreensão profunda das ameaças de segurança e privacidade no contexto do BLE, o que é crucial para o desenvolvimento de estratégias de segurança e privacidade mais robustas na pesquisa em desenvolvimento. A pesquisa de Barua et al. serve como um valioso guia para identificar e mitigar potenciais vulnerabilidades em dispositivos BLE, alinhando-se diretamente com o escopo e os objetivos da pesquisa em andamento.

3.7 Estado atual da segurança do uso de Keyless entry

O artigo de Lennert Wouters et al. [8] foca em identificar e explorar vulnerabilidades em sistemas que utilizam *Passive Keyless Entry and Start - PKES* (Entrada e Ignição passiva sem chave), com ênfase na segurança de cifras proprietárias e na análise de protocolos. Além disso, eles discutem estratégias de mitigação de curto prazo para lidar com as fraquezas de segurança encontradas, o documento também menciona a resposta de fabricantes de veículos, como Tesla Motors, que introduziram atualizações de software e melhorias de segurança em resposta às descobertas da pesquisa.

O estudo foi motivado pela ampla adoção de PKES em veículos de luxo e pela falta de atenção dedicada à segurança desses sistemas, o estudo visa evidenciar possíveis falhas e riscos de segurança. Os pesquisadores visaram demonstrar a possibilidade de realizar ataques de clonagem e emulação de chaves remotamente, permitindo o desbloqueio e a partida do veículo sem a necessidade da chave original. O objetivo era chamar a atenção dos fabricantes de veículos e fornecedores para a importância de implementar medidas de segurança mais robustas nesses sistemas. O esquema de desafio-resposta usado pelo protocolo PKES estudado pode ser visto na imagem 3.7.

Identificaram-se múltiplas vulnerabilidades, incluindo o uso de cifras inadequadas e a falta de autenticação mútua nos protocolos. O artigo também descreve a implementação de um ataque de prova de conceito eficiente, que permite clonar um chaveiro de um Tesla Model S em segundos usando equipamentos comuns. O estudo reconhece que as soluções de curto prazo para mitigar as vulnerabilidades identificadas exigiriam uma extensa reformulação de hardware e software. Eles também destacam a importância de ter procedimentos documentados para que pesquisadores de segurança possam relatar vulnerabilidades em produtos críticos de segurança e solicita que os fabricantes de veículos trabalhem mais de perto com seus fornecedores para prevenir esses problemas no futuro.

Este artigo é relevante para a pesquisa em questão ao evidenciar falhas em sistemas de segurança veiculares e destacar a importância da autenticação robusta e cifras seguras. O método e os achados podem informar estratégias para fortalecer a segurança em sistemas PKES, que é um foco da tese em desenvolvimento.

3.8 Discussão

Na seção de Trabalhos Relacionados, foram investigados uma série de estudos que ofereceram perspectivas fundamentais para a análise de protocolos de comunicação entre dispositivos de baixa energia e automóveis no contexto de sistemas de entrada sem chave.

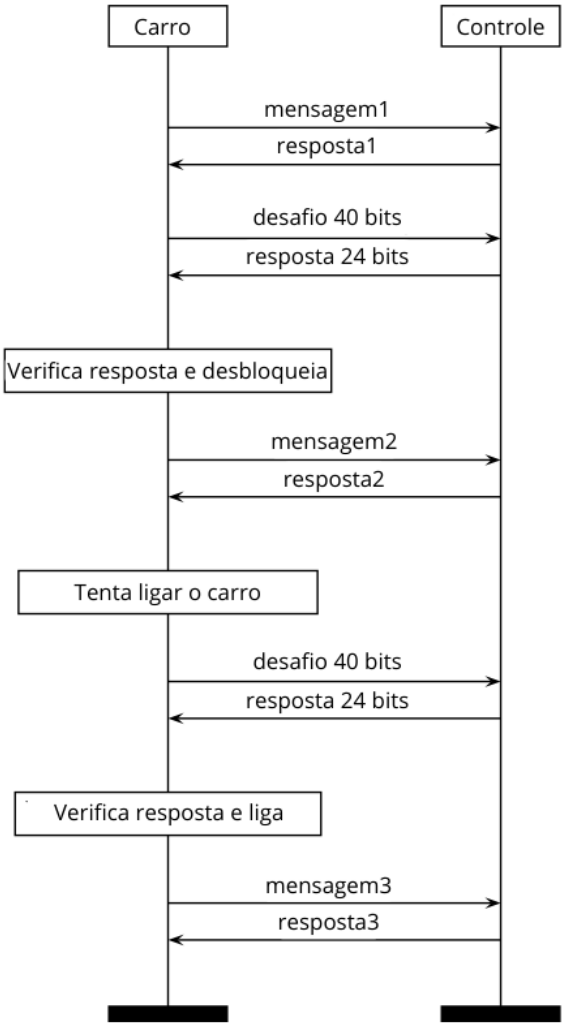

Figura 3.7: Protocolo Desafio-Resposta de PKES por Lennert et al. [8]

Artigos como os de Al-Sarawi et al [3]. e Tournier et al [4]. forneceram um entendimento profundo sobre os protocolos de comunicação em IoT, um componente crítico para a eficiência energética em sistemas de *keyless entry*. O estudo de Glocker et al. [15] foi particularmente relevante, focando em protocolos seguros de entrada sem chave usando criptografia simétrica, enquanto Singh et al. [6] exploraram algoritmos de criptografia leves, adequados para dispositivos IoT de baixa energia. Barua et al. [7] e Wouters et al. [8] trouxeram à tona importantes considerações sobre as ameaças de segurança associadas ao BLE, um protocolo frequentemente empregado em sistemas de entrada sem chave em automóveis. Esses trabalhos coletivamente enriquecem o entendimento sobre os desafios e as nuances na implementação de protocolos de comunicação eficientes e seguros para sistemas de *keyless entry* em veículos, estabelecendo uma base sólida para análise e pesquisa futura nessa área.

Capítulo 4

Proposta de Comparação

No capítulo atual, são detalhadas as metodologias utilizadas para os testes e comparações dos protocolos NFC, BLE e RFID. Primeiramente, será explicado o contexto no qual os testes serão realizados, o que inclui uma discussão detalhada sobre as configurações de hardware e software necessárias. Em seguida, serão expostas as métricas pelas quais cada um dos protocolos será avaliado.

4.1 Contexto da Aplicação

Para avaliar o desempenho dos protocolos em estudo, será configurado um ambiente de teste consistindo em um modelo genérico de interação entre dois dispositivos. Neste modelo, um dos dispositivos será caracterizado por seu baixo consumo energético, refletindo as condições reais de uso em aplicações práticas. Idealmente, ambos os dispositivos deverão ser capazes de manter uma conexão estável e contínua dentro de um alcance de até 1 metro. Os protocolos submetidos a teste terão como objetivo principal garantir o envio seguro e eficiente de pacotes de dados entre estes dois dispositivos. Esta configuração visa simular cenários de uso realísticos, permitindo uma avaliação precisa da eficácia, segurança e eficiência energética dos protocolos em questão.

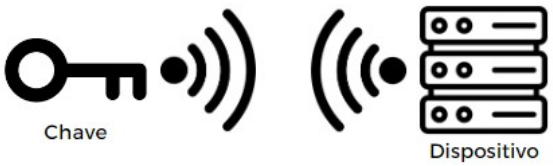

Figura 4.1: Cenário da Aplicação, com uma chave de baixo consumo e um dispositivo sem restrições

Para aproximar o ambiente ao mundo real, será definido que o dispositivo de baixo consumo é uma chave eletrônica com um processador ARM com 128 KB de memória Flash e 36 KB de memória RAM, alimentada por uma bateria CR2032 de 200 mAh. O outro dispositivo será um processador com memória e alimentação suficientes para realizar qualquer tarefa necessária. Portanto, os testes se concentrarão na chave, que será responsável por possíveis restrições que possam ocorrer.

Para a implementação efetiva dos protocolos em questão, a seleção de módulos específicos é essencial. O chip nRF52810 [19], desenvolvido pela Nordic Semiconductor, foi escolhido para o módulo de Bluetooth Low Energy, destacando-se por oferecer uma saída TX de até +4 dBm. No contexto do RFID, optamos pela tag RF-HDT-DVBB-N2 [20] da Texas Instruments, que se notabiliza por seus 2048 bits de memória. Para as funções de leitura RFID, o leitor MFRC52202 [21] da NXP foi selecionado. Ademais, o *System-On-Chip* nRF5340 [22], também da Nordic Semiconductor, foi identificado como a escolha ideal para funções de leitor e emissor NFC, com o benefício adicional de suportar Zigbee e Bluetooth Low Energy. A escolha desses componentes foi guiada não apenas pela sua disponibilidade em plataformas de varejo de componentes eletrônicos, mas também pela vasta quantidade de literatura técnica e prática disponível sobre eles, facilitando sua integração e uso em nosso projeto.

4.2 Métricas de Avaliação

Na subseção a seguir, serão focadas as métricas de avaliação específicas utilizadas para analisar e comparar os protocolos RFID, BLE e NFC. Estas métricas representam os aspectos mais importantes do desempenho desses protocolos e fornecerão a estrutura para a comparação sistemática de suas capacidades e características.

A primeira métrica, alcance, é um componente essencial que define a distância máxima que uma transmissão pode alcançar sem uma degradação significativa do sinal. Através desta métrica, será possível avaliar a adequação de cada protocolo em diferentes cenários de aplicação, variando de proximidade imediata a distâncias mais longas, e considerando um caminho livre de obstáculos.

A segunda métrica, segurança do protocolo, é de extrema importância, especialmente quando o produto final considerado tem alto valor agregado, como um automóvel. Esta métrica permitirá compreender os riscos aos quais cada um dos protocolos está sujeito, permitindo a seleção do protocolo mais resistente a ataques maliciosos.

Por fim, o custo de implementação dos componentes associados a cada protocolo será considerado. Esta métrica trata especificamente do custo monetário dos componentes necessários para implementar cada protocolo - incluindo, por exemplo, o custo do hardware

de leitura para RFID e NFC, ou os módulos BLE incorporados. A análise do custo dos componentes é vital para fornecer uma perspectiva sólida sobre a viabilidade financeira de cada protocolo. Serão também discutidas as dimensões de cada componente e sua compatibilidade com as tecnologias já utilizadas.

4.2.1 Alcance de Transmissão

Nesta primeira parte da análise, será avaliado o alcance de cada protocolo. O alcance é uma das métricas cruciais quando se considera a utilização de um protocolo de comunicação sem fio. Ele representa a distância máxima que um sinal de comunicação pode viajar entre dois dispositivos sem perda significativa de informação.

No contexto dos protocolos RFID, BLE e NFC, o alcance pode variar bastante dependendo de vários fatores, incluindo a energia do transmissor, o ambiente de transmissão, obstáculos potenciais, entre outros. Como resultado, entender o alcance de transmissão de cada protocolo é essencial para determinar a solução mais adequada para um determinado contexto ou aplicação.

No cenário do estudo, não será necessário que os dispositivos tenham um grande alcance de transmissão, uma vez que quanto mais próximos forem, mais segura será a interação. No entanto, também é desejável manter um nível de conforto para o usuário, impedindo que ele tenha que retirar a chave da mochila, por exemplo. Dessa forma, fica determinado que o alcance operacional do protocolo deve ser de no máximo 1 metro, conforme exemplificado na figura 4.2.

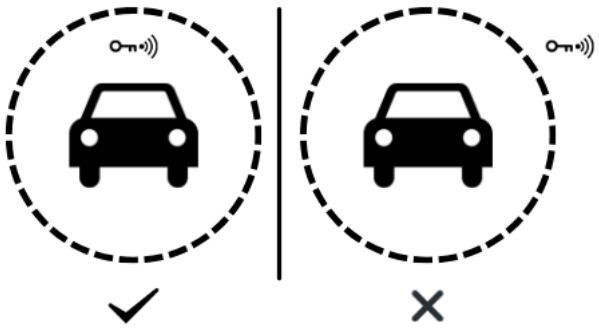

Figura 4.2: Cenário da Aplicação em que o raio de ação da chave é de 1 metro

4.2.2 Segurança dos Dados

Para esta parte da análise, serão discutidos os pontos fortes e fracos de segurança e privacidade de cada protocolo. Cada um dos protocolos estudados possui características de segurança únicas que os tornam adequados para determinados contextos, bem como

potenciais vulnerabilidades que podem ser exploradas. Entre esses aspectos, estão os tipos de criptografia utilizados, a robustez desses esquemas de criptografia e como são implementados, bem como as possíveis fraquezas decorrentes das especificidades de cada protocolo.

Ao trazer esses aspectos à tona, busca-se proporcionar uma visão mais clara do panorama de segurança desses protocolos, permitindo uma escolha mais informada para os usuários e implementadores em potencial. A segurança dos dados é um pilar fundamental para gerir o acesso aos dispositivos, e o entendimento das forças e fraquezas de cada protocolo é essencial para garantir a integridade e a privacidade dos dados.

Na análise, os protocolos serão avaliados principalmente pela sua resistência aos ataques *man-in-the-middle* e *replay*, que, como vistos em Tournier [4], são os ataques mais comuns contra dispositivos IoT e fáceis de replicar. Além disso, será verificado o quão oneroso é o processo de criptografia dos protocolos, visto que os dispositivos em que serão usados possuem pouca capacidade de processamento. Durante a avaliação, levar-se-á em consideração tanto os atributos de design próprios quanto as implementações adicionais de segurança que eles permitem, como os diferentes modos de pareamento do Bluetooth Low Energy, por exemplo.

4.2.3 Custos Atribuídos

Nesta métrica de avaliação, serão considerados fatores primordiais para a implementação dos protocolos NFC, BLE e RFID em dispositivos pequenos produzidos em larga escala. O primeiro aspecto crucial nesta avaliação é o custo dos componentes necessários para cada protocolo. Cada um deles, com seus chips, tags e leitores específicos, possui seus custos associados, que devem ser analisados minuciosamente.

Num segundo momento, o espaço físico ocupado por cada componente do protocolo é de importância vital em um dispositivo de tamanho reduzido. A compacidade dos componentes de cada protocolo deve ser avaliada, pois influi diretamente no projeto final do dispositivo. Um componente de menor tamanho pode proporcionar mais flexibilidade no design, além de reduzir potencialmente os custos de fabricação devido à menor quantidade de materiais necessários.

Dessa forma, a análise dos Custos Atribuídos fornece uma compreensão detalhada dos desafios e benefícios financeiros associados à escolha entre NFC, BLE e RFID para a implementação em dispositivos de pequeno porte produzidos em larga escala, como controles de carros.

4.3 Metodologia

Para conduzir uma análise abrangente das métricas discutidas neste estudo, foi realizada uma coleta extensiva de dados a partir de uma variedade de fontes confiáveis e pertinentes. Isso incluiu documentação técnica detalhada de cada protocolo, fichas técnicas dos componentes escolhidos, publicações técnicas de renomados fabricantes, bem como pesquisas anteriores relevantes no campo. Um enfoque especial foi dado aos estudos prévios, visando incorporar dados práticos e atualizados do mundo real. Em situações onde ocorreram discrepâncias entre as fontes, optou-se por priorizar aquelas com informações mais recentes. Essa decisão foi baseada no entendimento de que tanto os componentes quanto os protocolos em questão estão sujeitos a evoluções e mudanças contínuas, fazendo com que os dados mais atuais ofereçam uma visão mais precisa e relevante para a análise.

Capítulo 5

Resultados

Este capítulo apresenta os resultados da investigação sobre a adequação de três protocolos de IoT proeminentes para aplicações de keyless entry em veículos: Bluetooth Low Energy (BLE), Radio Frequency Identification (RFID) e Near Field Communication (NFC). Avaliou-se cada protocolo com base em três critérios críticos: segurança, alcance de transmissão e custos atribuídos. Esses critérios foram considerados cruciais para garantir um sistema de entrada sem chave seguro, confiável e econômico. As descobertas apresentadas aqui fornecerão informações valiosas para desenvolvedores e fabricantes da indústria automotiva que buscam incorporar soluções avançadas de keyless entry em seus veículos.

Os resultados apresentados neste artigo foram obtidos a partir de uma revisão abrangente da literatura, incluindo documentação técnica dos componentes e protocolos, outras pesquisas da área e códigos desenvolvidos pelo autor.

5.1 Alcance de Transmissão

O alcance de transmissão é uma métrica importante para aplicações de IoT que exigem comunicação a distâncias significativas. Em aplicações de entrada sem chave, o alcance de transmissão é fundamental para garantir que o chaveiro seja capaz de se comunicar com o veículo de forma confiável, mesmo em ambientes com obstáculos.

Nesta seção, foram apresentados os resultados da avaliação do alcance de transmissão dos protocolos Bluetooth Low Energy (BLE), Radio Frequency Identification (RFID) e Near Field Communication (NFC).

5.1.1 Bluetooth Low Energy

No âmbito teórico, a potência do BLE 5 pode chegar a alcançar até 400 metros [23] com a potência máxima e, dependendo da antena escolhida, este alcance pode ser ainda maior. Entretanto, ao calcular uma estimativa do alcance máximo dos componentes escolhidos utilizando a calculadora oficial do Bluetooth SIG [24], e usando uma antena AN043 [25], comumente utilizada por ser compacta, chegou-se aos valores de 54 a 129 metros ao utilizar a potência máxima do módulo nRF52810. E, diminuindo sua potência em -20 dBm, atinge-se um alcance de menos de 15 metros. O gráfico 5.1 mostra o alcance teórico do conjunto, alterando a potência TX num passo de 4 dBm.

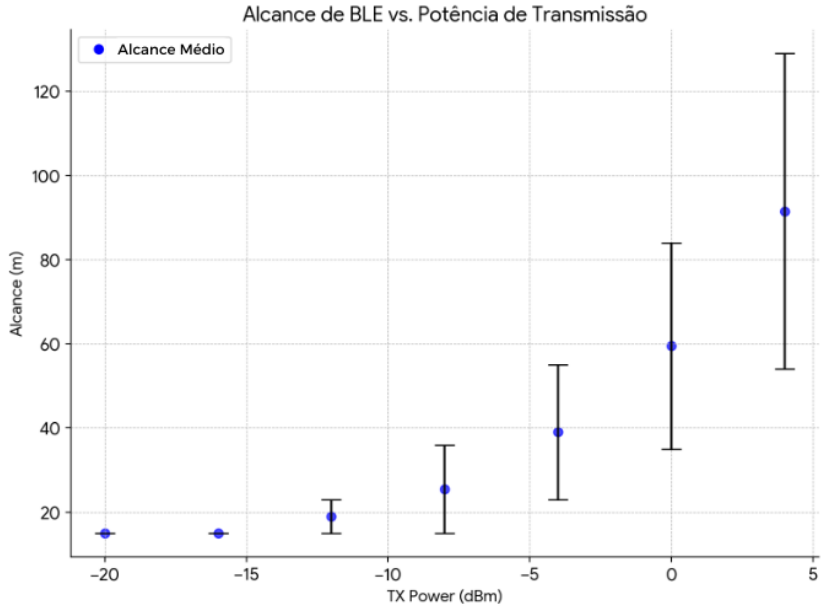

Figura 5.1: Alcance Teórico do BLE 5 com módulo nRF52810

Já na prática, esses valores costumam ser bem menores. De acordo com os dados encontrados no artigo de Gendy e Tham [5], onde o módulo foi testado com a mesma antena usada nos cálculos, a força do sinal recebido (RSSI) apresentou uma variação em relação à distância: de 1 a 2 metros, o RSSI médio era de -66dB, enquanto que de 2 a 3 metros, o RSSI médio caía para -74dB, como pode ser apreciado em 5.2. Isso evidencia que o módulo nRF52810 com a antena F invertida tem um alcance eficaz de aproximadamente 2 a 3 metros antes de enfrentar uma queda significativa na força do sinal em um ambiente padrão.

Considerando o cenário em estudo, fica claro que o alcance de transmissão do módulo nRF52810 emitindo Bluetooth Low Energy é mais do que suficiente, mesmo quando se limita ao máximo o consumo de energia do dispositivo.

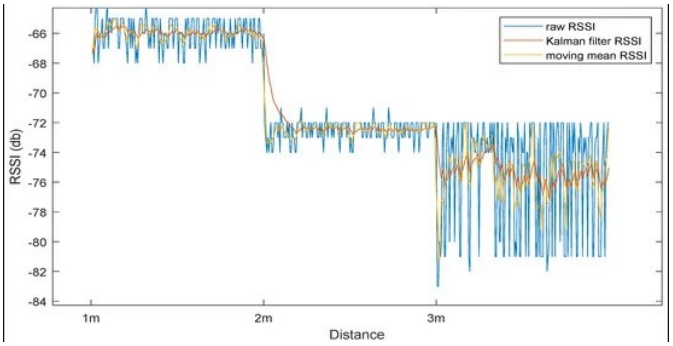

Figura 5.2: Força do Sinal BLE. Fonte: [5]

5.1.2 RFID e NFC

A tag de RFID escolhida funciona na frequência de 13,56 MHz, que é a mesma que o NFC opera. Segundo a literatura, essa frequência consegue manter conexão entre dispositivos por até 1m [26].

Teoricamente, para que o alcance de um dispositivo que utiliza a tecnologia de *Near Field* seja de 1m, sua antena circular deve ter um raio de 1.414m [9]. Entretanto, uma antena dessas dimensões seria inviável para o cenário em pauta, ao aumentar o número de voltas, é possível diminuir o tamanho deste raio para que ela caiba em dispositivos compactos. A equação 5.1, demonstra o cálculo da indutância desta nova antena, em que r_o é o raio exterior, r_i é o raio interior, N é o número de voltas, $a = (r_i + r_o)/2$ e $b = r_o - r_i$.

$$L = \frac{(0.3937)(aN)^2}{8a + 11b} \tag{5.1}$$

Sendo assim, ao utilizarem-se uma antena espiral de loop de raio 3cm, com fio de 0.1cm de diâmetro e 9 voltas é possível garantir teoricamente um alcance de 20 cm para os módulos NFC e RFID. A antena discutida pode ser vista na imagem 5.3.

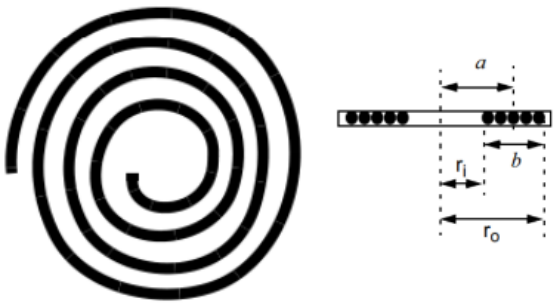

Figura 5.3: Antena Espiral em Loop. Fonte: [9]

Na prática, esses valores diferem positivamente para o RFID e negativamente para o NFC. No caso do RFID, a literatura mostra que um sistema com o módulo de leitura MFRC52202 consegue ler tags passivas num alcance de até 1m [27], enquanto que os dispositivos de leitura NFC, atingem distâncias de leitura de apenas 5cm [28].

5.1.3 Discussão

Os três protocolos analisados atenderam aos requisitos do cenário proposto, mas dois deles se destacaram positivamente: o Bluetooth Low Energy (BLE) e o RFID. Ambos possuem alcances maiores do que o NFC, o que traz a comodidade de não precisar de contato direto entre os dispositivos.

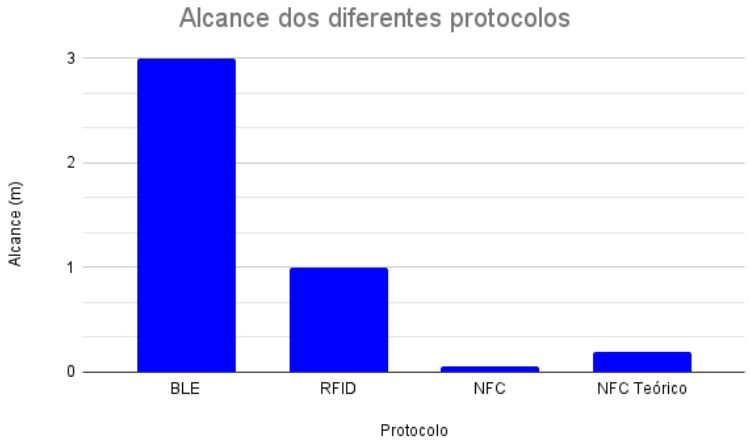

Figura 5.4: Comparativo do alcance teórico e prático

Em uma análise mais detalhada, o BLE se mostrou a melhor opção, pois oferece alcances ainda maiores que os outros dois protocolos, mantendo um tamanho compacto por não precisar de antenas tão grandes. Essa característica permite uma maior flexibilidade para o desenvolvimento de produtos, pode-se observar pela figura 5.4 que o Bluetooth usando os módulos escolhidos tem pelo menos 3 vezes o alcance do RFID, e 60 vezes maior que o do NFC, permitindo assim uma maior flexibilidade para os desenvolvedores na hora de definir um alcance de atuação pro controle.

5.2 Segurança dos Dados

É de suma importância que a segurança da comunicação entre os dispositivos do cenário seja mantida, e que os dados trocados entre eles permaneçam privados. Uma vez que, uma falha de segurança acarreta não somente na perda de privacidade mas também na perda de bens de alto valor agregado. Por isso, nesta seção, foram analisados o estado

atual das medidas de proteção adotadas pelos protocolos sob estudo, a fim de avaliar sua eficácia em garantir a segurança dos dados.

5.2.1 RFID

O RFID (Identificação por Rádio Frequência) é um protocolo de comunicação que proporciona o rastreamento e identificação de objetos e pessoas. No entanto, a segurança do RFID tornou-se uma preocupação crescente, especialmente em relação à privacidade dos dados. Diversos ataques podem ser perpetrados contra este sistema, incluindo a interceptação e leitura não autorizada de dados, clonagem de etiquetas e ataques de negação de serviço [29]. Esses ataques podem ser potencialmente danosos, principalmente quando o RFID é empregado em sistemas sensíveis, como os de controle de acesso de veículos.

No cenário apresentado, existem duas possibilidades de uso do protocolo, a primeira é utilizando apenas a tag passiva do módulo RF-HDT-DVBB-N2 e a segunda é fazendo uso do processador ARM da chave eletrônica. A primeira situação é a menos segura entre as duas, pois a "senha"armazenada na tag pode ser facilmente lida. Desse modo, num hipotético ataque, seria suficiente um breve contato da tag com um dispositivo leitor mal-intencionado para que o segredo fosse comprometido, permitindo que o invasor gerasse inúmeras cópias da chave.

Na segunda situação, seria viável utilizar o processador ARM para regravar a chave armazenada na tag após cada leitura. Essa nova chave poderia ser gerada e transmitida por outro dispositivo, um carro, por exemplo, e este só permitiria que a nova chave fosse usada. Dessa maneira, caso a chave fosse duplicada por um agente mal-intencionado, ela se tornaria uma chave expirada caso não fosse rapidamente utilizada após a clonagem. Assim, limita-se o potencial para a chave ser usada inadequadamente, reforçando a segurança do sistema.

5.2.2 NFC

O protocolo NFC (Comunicação de Campo Próximo) é uma tecnologia amplamente utilizada para fins de comunicação sem fio de curto alcance, tornando-o uma alternativa viável para sistemas de controle de acesso. No entanto, como qualquer sistema tecnológico, ele não está imune a possíveis falhas de segurança e explorações mal-intencionadas. Neste trecho, discutiremos os possíveis ataques aos quais o NFC está vulnerável e as vantagens inerentes ao seu uso em sistemas de controle de acesso.

Um dos ataques mais comuns contra o NFC é o eavesdropping, que é a interceptação de comunicações por indivíduos não autorizados. Este tipo de ataque é viável principalmente devido à natureza sem fio do NFC. Outros ataques potenciais incluem a alteração de dados,

onde um invasor modifica a informação transmitida entre dispositivos e o ataque de relay, no qual o invasor engana os dispositivos de comunicação NFC fazendo-os acreditar que estão próximos um do outro.

Apesar dessas potenciais ameaças, o NFC traz consigo diversas vantagens quando utilizado em sistemas de controle de acesso. A primeira e mais notória é a conveniência: a habilidade de simplesmente tocar ou aproximar um dispositivo para obter acesso é uma grande melhoria em relação aos métodos tradicionais. Além disso, a natureza de curto alcance do NFC torna mais difícil a interceptação da comunicação por invasores, já que precisariam estar fisicamente próximos para tal. Finalmente, existem diversas medidas de segurança que podem ser empregadas para aumentar ainda mais a segurança do NFC, tais como criptografia de dados e autenticação robusta.

5.2.3 BLE

A adoção do protocolo BLE (Bluetooth Low Energy) em sistemas de controle de acesso está em crescimento devido ao seu baixo consumo de energia e capacidade de conectar vários dispositivos de maneira eficiente. No entanto, é crucial analisar a segurança deste protocolo, uma vez que é suscetível a certos tipos de ataques. Neste trecho, serão explorados os possíveis ataques que o BLE pode sofrer e discutidas as vantagens de sua utilização em sistemas de controle de acesso.

Alguns dos ataques mais comuns ao BLE incluem ataques de interceptação, onde os dados transmitidos entre dispositivos são capturados por um invasor; ataques de spoofing, onde um dispositivo falso se passa por um legítimo para obter acesso ou informações; e ataques de força bruta, onde um invasor tenta adivinhar continuamente uma senha ou chave de criptografia.

Apesar destes desafios, o protocolo BLE oferece várias vantagens quando aplicado ao controle de acesso. O BLE permite uma conexão altamente escalável e eficaz em termos de energia, o que é especialmente útil para dispositivos que operam com bateria. Outra vantagem é a capacidade de 'pareamento permanente', onde, uma vez que dois dispositivos estão emparelhados, sempre reconhecerão um ao outro, aumentando assim a usabilidade e segurança. Além disso, com uma criptografia robusta e autenticação de dois fatores, é possível assegurar que o BLE se mantenha seguro contra muitos ataques comuns.

5.2.4 Discussão

A análise dos protocolos RFID, NFC e BLE revela vantagens e desafios específicos para cada tecnologia no contexto de sua aplicação em sistemas de controle de acesso.

O RFID, apesar de ser fácil de implementar e utilizar, apresenta consideráveis desafios de segurança, sendo vulnerável à leitura não autorizada de dados e clonagem de etiquetas. A opção de regravar a chave armazenada na tag depois de cada leitura, usando o processador ARM, surge como uma estratégia potencial para mitigar a possibilidade de uso indevido da chave.

Por outro lado, o NFC, apesar de também ser suscetível a ataques como eavesdropping e modificação de dados, oferece vantagens significativas para seu uso em sistemas de controle de acesso. A comodidade de obter acesso simplesmente aproximando um dispositivo, aliada a medidas de segurança adicionais como a criptografia de dados e autenticação robusta, tornam o NFC uma opção viável e segura.

O BLE, apesar dos desafios de segurança inerentes, como ataques de interceptação, spoofing e força bruta, oferece atraentes vantagens para o controle de acesso. Sua eficiência energética, escalabilidade de conexão e a capacidade de "pareamento permanente", juntamente com medidas de segurança robustas, como criptografia e autenticação de dois fatores, destacam o BLE como uma promissora opção para sistemas de controle de acesso.

Essas análises ressaltam a importância de analisar cuidadosamente tanto os aspectos de segurança quanto as vantagens práticas de cada protocolo ao selecionar a tecnologia mais adequada para a implementação de sistemas de controle de acesso. Pesquisas adicionais poderiam continuar a mitigar os desafios de segurança enfrentados e otimizar o aproveitamento das vantagens fornecidas por cada protocolo.

5.3 Custos Atribuídos

Para que produtos que implementam os protocolos analisados sejam desenvolvidos e fabricados em massa, é necessário que seus custos sejam baixos. Portanto, nesta seção, serão analisados os custos monetários dos componentes e as dimensões físicas, que também influenciam o preço das placas de circuito. O objetivo é determinar qual dos três protocolos é mais eficaz em relação custo-benefício, isto é, qual apresenta o melhor desempenho por unidade de área.

5.3.1 RFID

Para a implementação de um sistema usando as tags de RFID, são necessários três elementos: a tag, o módulo leitor e uma antena para esse leitor. Além disso, o uso de tags passivas pode reduzir os custos de produção, uma vez que o processador ARM e a pilha da chave não seriam mais necessários. No gráfico 5.5, é possível observar a relação dos custos dos componentes.

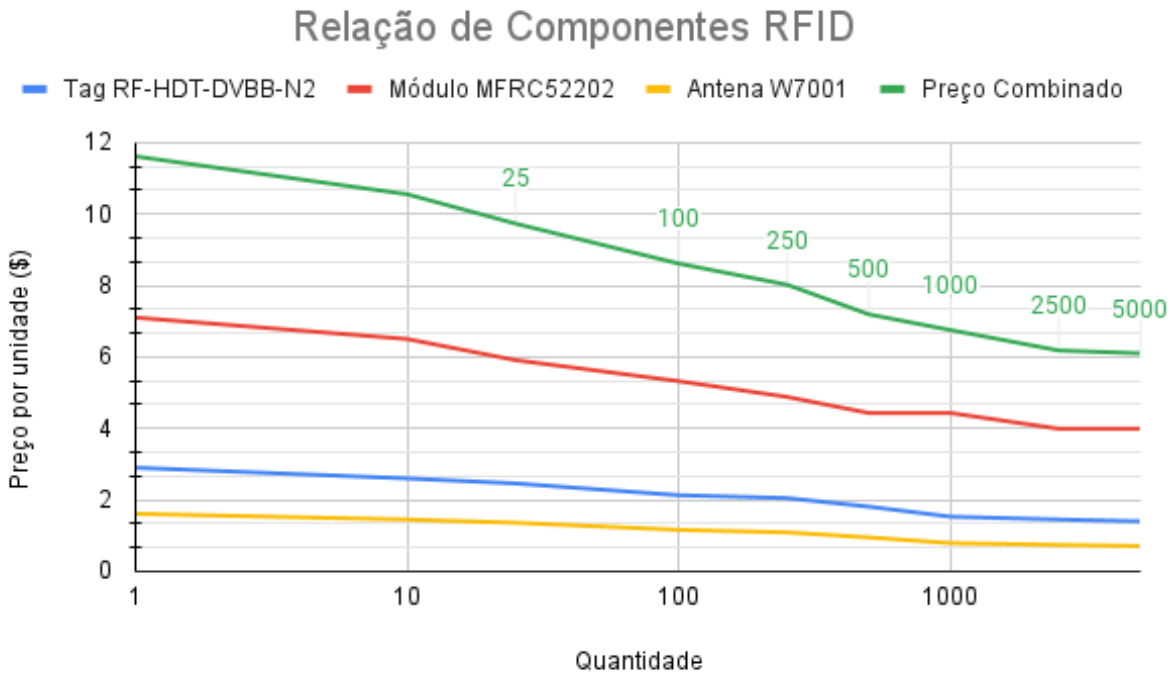

Figura 5.5: Custo dos componentes para um sistema de RFID. Fonte: [10], [11], [12]

É possível observar que o RFID tem um custo inicial elevado, no qual, para um kit para desenvolvimento contando com apenas uma unidade de cada módulo, seria necessário desembolsar $11.61. Isso acaba gerando um alto custo de entrada para o desenvolvimento de MVPs e protótipos, sendo o principal causador disso o módulo leitor MFRC52202. Entretanto, ao aumentar o número de unidades compradas, é possível ver uma diminuição de quase 48% no custo total de cada conjunto de emissor, tag e antena, fazendo com que o preço final seja de $6.10.

Além disso, deve-se considerar o tamanho físico dos componentes para manter um design compacto das chaves. Deste modo, para esta comparação, serão considerados apenas os componentes da chave. Assim, para o RFID, observa-se que a tag ocupa uma área de aproximadamente $380mm^2$.

5.3.2 NFC

Para a incorporação do protocolo NFC no projeto, são necessários 4 componentes, sendo eles: 2 módulos NRF5340, um para a chave e um para o leitor, e 1 antena para cada módulo. Com isso, será possível estabelecer uma conexão entre os dois dispositivos. O custo total deste conjunto de componentes, atualmente, seria de 21.3 dólares para a

compra de um conjunto. Porém, para compras em larga escala, o custo cai para 10.82, resultando em uma diminuição de 49%.

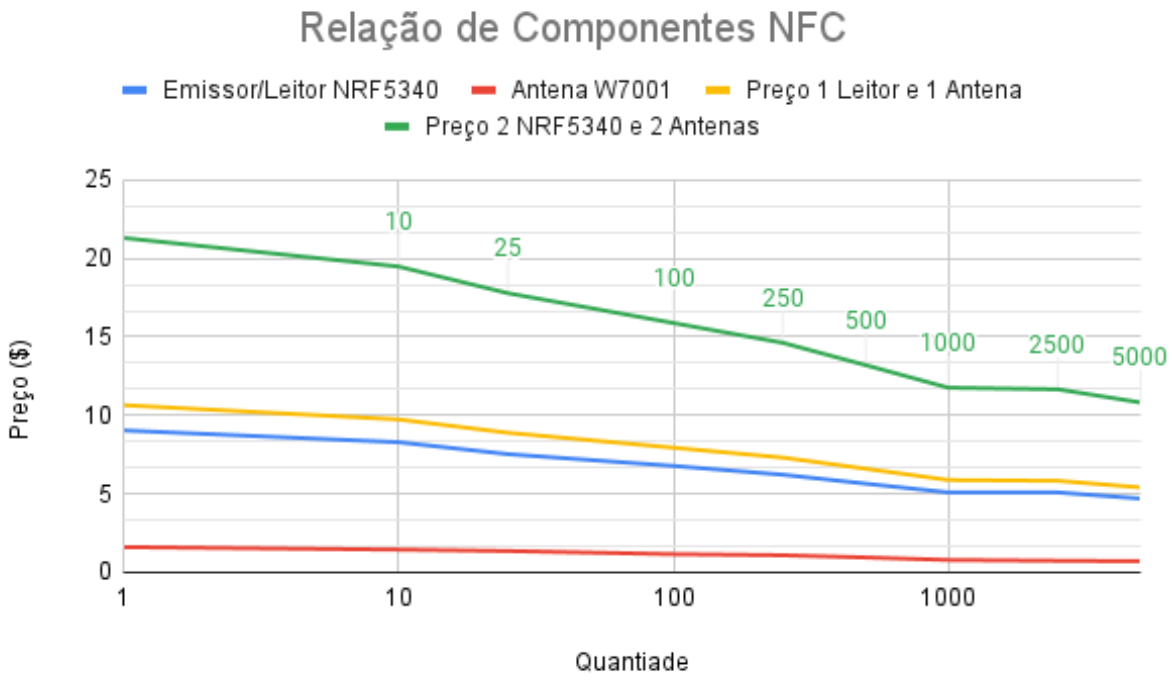

Figura 5.6: Custo dos componentes para um sistema de NFC. Fonte: [13] e [10]

Semelhante ao caso do RFID, o custo de entrada para o desenvolvimento de sistemas com tecnologia NFC é extremamente alto. Contudo, diferente do RFID, o NFC continua com preço elevado mesmo quando há compras em altas quantidades para a produção em larga escala de dispositivos compatíveis. No quesito tamanho, o chip nRF5340 apresenta uma área de $49mm^2$, que somado à antena de $625mm^2$, resulta em uma área total de $674mm^2$.

No entanto, o NFC possui uma vantagem que não se encontra no protocolo RFID, a implementação em telefones celulares. Conforme a literatura ([30] e [31]), em 2020, 90% de todos os aparelhos celulares dispunham da tecnologia NFC já integrada. Com isso, seria possível substituir completamente a chave eletrônica pelo celular do usuário, necessitando apenas do custo de desenvolvimento de um aplicativo ou cartão digital para ser utilizado como chave. Esta alternativa reduziria pela metade os custos dos componentes do NFC, chegando a $5.41 para compras de alto volume, como observado na linha amarela da figura 5.6.

5.3.3 BLE

A implementação física do protocolo Bluetooth Low Energy é a que contém menos elementos quando comparada com as duas alternativas anteriores, necessitando de apenas dois módulos nRF52810, um para cada dispositivo.

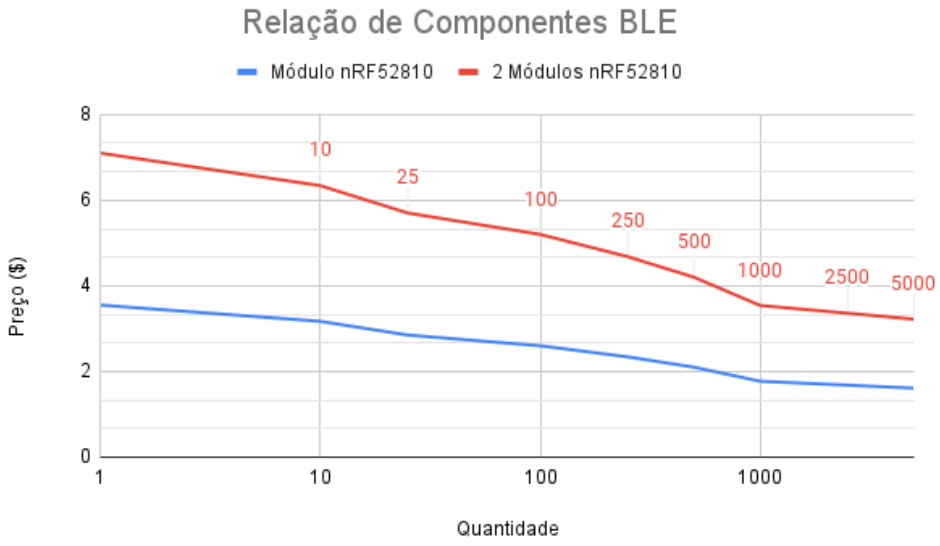

Figura 5.7: Custo dos componentes para um sistema de BLE. Fonte: [14]

Pode-se observar, com o auxílio da figura 5.7, que o BLE, além de ter o menor custo de entrada, 7.10 dólares, também apresenta os maiores descontos na compra em quantidade, fazendo com que seu preço chegue a $3.22 em compras de mais de 5000 peças, um desconto de 54%. E, assim como o NFC, o Bluetooth está amplamente difundido em aparelhos telefônicos, permitindo também o uso deles como chave no cenário proposto. Com isso, seria possível reduzir ainda mais o custo de produção por componente. Ao analisar a área ocupada, é perceptível que o BLE também é o protocolo que demanda a menor superfície, utilizando apenas $36mm^2$ para o módulo nRF52810.

5.3.4 Discussão

Após avaliar individualmente cada protocolo, é possível fazer uma comparação entre os três para decidir qual é o mais indicado para aplicação no caso em questão. Ao cotejar os custos, é fácil perceber que o Bluetooth Low Energy é o mais vantajoso, enquanto que o NFC prova-se ser significativamente mais caro, conforme pode ser observado na figura 5.8.

É evidente que o RFID torna-se a próxima escolha caso haja a intenção de usar uma outra opção além do BLE, mesmo ainda sendo o dobro do valor do Bluetooth. Contudo,

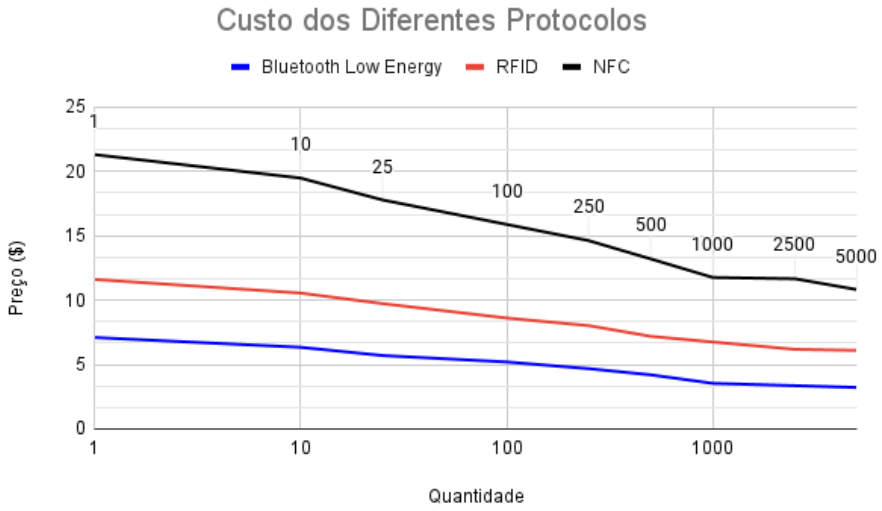

Figura 5.8: Relação do custo dos componentes de cada protocolo

se se considerar a ideia de utilizar o celular como chave, desenvolvendo uma aplicação que crie um "cartão"para o bloqueio e desbloqueio do automóvel, o cenário modifica-se, já que, com isso, os custos com NFC tornariam-se menores do que os dos componentes de RFID.

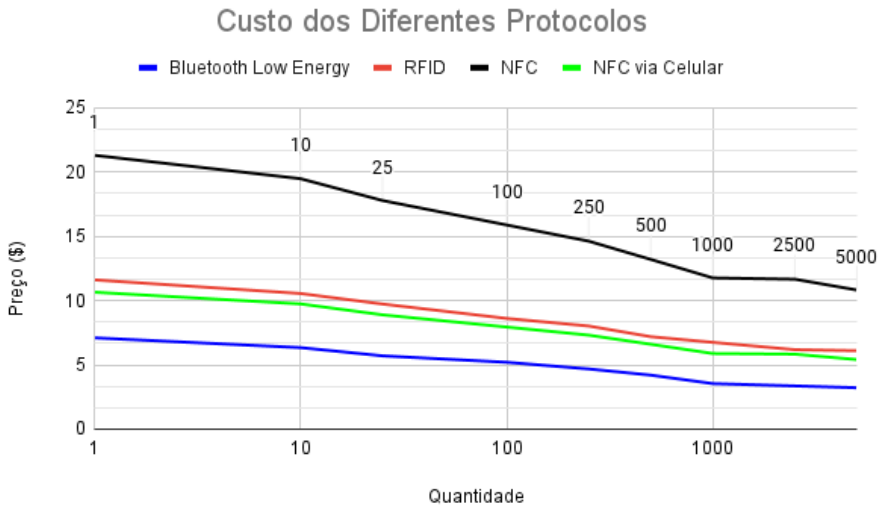

Figura 5.9: Custo de componentes mais NFC via celular

Além disso, também é preciso fazer a análise das dimensões dos componentes, levando em consideração que o tamanho médio de um controle de carro é de 3cm de largura por 3cm de comprimento. Deste modo, utilizar uma antena quadrada com 2.5 cm de lado, como é o caso da W7001, tornaria mais complexa a produção das placas de circuito integrado do controle.

Capítulo 6

Conclusão

Em resumo, este trabalho comparou três protocolos principais - BLE (Bluetooth Low Energy), NFC (Near Field Communication) e RFID (Radio Frequency Identification) - como potenciais candidatos para implementação em sistemas de entrada sem chave para veículos. A análise levou em conta diversos fatores críticos, incluindo o alcance de cada protocolo, a segurança oferecida e o custo dos componentes necessários.

A partir desta análise detalhada, o BLE emergiu como a opção mais viável para o propósito em questão. Seu alcance superior, aliado à uma segurança robusta e componentes de custo comparativamente baixo, torna-o o candidato ideal para essa aplicação.

No entanto, o NFC também se mostrou uma alternativa potencialmente viável. Embora seu alcance seja limitado em comparação ao BLE, particularidades como a sua praticidade para o usuário - uso via celular - e uma segurança focada na proximidade, pode torná-lo uma alternativa interessante dependendo do cenário de uso. Portanto, é relevante considerar o perfil de uso antes da decisão final.

6.1 Trabalhos Futuros

Este estudo estabelece um marco para explorar um amplo leque de possibilidades futuras na implementação de sistemas de entrada sem chave (*keyless entry*), utilizando protocolos de comunicação otimizados para dispositivos de baixo consumo energético. Com os resultados alcançados, abre-se a porta para pesquisas subsequentes focadas na avaliação prática de cada protocolo. Estas investigações poderiam ser conduzidas em contextos variados do mundo real, incluindo testes em metrópoles densamente povoadas ou em ambientes controlados de montadoras, onde uma multiplicidade de dispositivos operando sob o mesmo protocolo coexistem.

Um dos avanços mais promissores derivados desta pesquisa seria a implementação e análise comparativa desses protocolos em veículos de grandes fabricantes automobilísticos,

como carros e motocicletas. Essa fase poderia ser enriquecida com a realização de pesquisas de satisfação do cliente, visando não apenas medir a eficácia técnica dos sistemas, mas também capturar percepções e preferências dos usuários finais. Isso permitiria identificar outras métricas de desempenho relevantes, além das já examinadas neste estudo, fornecendo insights valiosos sobre o que realmente importa para os consumidores no uso cotidiano dessas tecnologias.

Referências

[1] International Organization for Standardization: *rfid_logo.png*. `https://www.iso.org/obp/ui#iso:grs:7000:3010`, 2023. Acessado em 5 de Dezembro de 2023. ix, 3

[2] NFC Forum: *nvf_logo.png*. `https://nfc-forum.org/build/branding`, 2023. Acessado em 5 de Dezembro de 2023. ix, 3

[3] Al-Sarawi, Shadi, Mohammed Anbar, Kamal Alieyan e Mahmood Alzubaidi: *Internet of things (iot) communication protocols*. Em *2017 8th International conference on information technology (ICIT)*, páginas 685–690. IEEE, 2017. ix, 16, 17, 25

[4] Tournier, Jonathan, François Lesueur, Frédéric Le Mouël, Laurent Guyon e Hicham Ben-Hassine: *A survey of iot protocols and their security issues through the lens of a generic iot stack*. Internet of Things, 16:100264, 2021. ix, 17, 18, 19, 25, 29

[5] Gendy, Maggie Ezzat Gaber, Phi Tham, Flynn Harrison e Mehmet Rasit Yuce: *Comparing efficiency and performance of iot ble and rfid-based systems for achieving contract tracing to monitor infection spread among hospital and office staff*. Sensors, 23(3), 2023, ISSN 1424-8220. `https://www.mdpi.com/1424-8220/23/3/1397`. ix, 19, 32, 33

[6] Singh, Saurabh, Pradip Kumar Sharma, Seo Yeon Moon e Jong Hyuk Park: *Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions*. Journal of Ambient Intelligence and Humanized Computing, páginas 1–18, 2017. ix, 21, 22, 25

[7] Barua, Arup, Md Abdullah Al Alamin, Md Shohrab Hossain e Ekram Hossain: *Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey*. IEEE Open Journal of the Communications Society, 3:251–281, 2022. ix, 22, 23, 25

[8] Wouters, Lennert, Eduard Marin, Tomer Ashur, Benedikt Gierlichs e Bart Preneel: *Fast, furious and insecure: Passive keyless entry and start systems in modern supercars*. IACR Transactions on Cryptographic Hardware and Embedded Systems, páginas 66–85, 2019. ix, 24, 25

[9] Microchip Technology Inc.: *MCRF200, MCRF210 RF Identification Devices – Rev. 4 – 4 Dec. 2001*. Relatório Técnico, Microchip Technology Inc., 2001. ix, 33

[10] Digi-Key Electronics: *W7001 Pulse Electronics | RF/IF and RFID*. `https://www.digikey.com/en/products/detail/pulse-electronics/W7001/4169647`, 2023. Acessado em 9 de Dezembro de 2023. ix, 38, 39

[11] Digi-Key Electronics: *MFRC52202HN1,115 NXP USA Inc. | RF/IF and RFID*. https://www.digikey.com/en/products/detail/nxp-usa-inc/MFRC52202HN1-115/4020895, 2023. Acessado em 9 de Dezembro de 2023. ix, 38

[12] Digi-Key Electronics: *RF-HDT-DVBB-N2 Texas Instruments | RF/IF and RFID*. https://www.digikey.com/en/products/detail/texas-instruments/RF-HDT-DVBB-N2/2095793, 2023. Acessado em 9 de Dezembro de 2023. ix, 38

[13] Digi-Key Electronics: *NRF5340-CLAA-R Nordic Semiconductor ASA | RF/IF and RFID*. https://www.digikey.com/en/products/detail/nordic-semiconductor-asa/NRF5340-CLAA-R/14323741, 2023. Acessado em 9 de Dezembro de 2023. ix, 39

[14] Digi-Key Electronics: *NRF52810-QFAA-R7 Nordic Semiconductor ASA | RF/IF and RFID*. https://www.digikey.com/en/products/detail/nordic-semiconductor-asa/NRF52810-QFAA-R7/7725408, 2023. Acessado em 9 de Dezembro de 2023. ix, 40

[15] Glocker, Tobias, Timo Mantere e Mohammed Elmusrati: *A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography*. Em *2017 8th International Conference on Information and Communication Systems (ICICS)*, páginas 310–315, 2017. x, 20, 21, 25

[16] Francillon, Aurélien, Boris Danev e Srdjan Capkun: *Relay attacks on passive keyless entry and start systems in modern cars*. 2011. 1

[17] Zhang, Sylvia: *Who owns the data generated by your smart car*. Harv. JL & Tech., 32:299, 2018. 1

[18] Bluetooth SIG, Inc.: *Bluetooth_CM_ColorBlack*. https://www.bluetooth.com/media/le-audio/, 2023. Acessado em 5 de Dezembro de 2023. 3

[19] Nordic Semiconductor: *nRF52810 - Multi-protocol SoC supporting Bluetooth, ANT and 2.4 GHz RF*. https://www.nordicsemi.com/products/nrf52810, 2023. Acessado em 7 de Dezembro de 2023. 27

[20] Texas Instruments Incorporated: *RF-HDT-DVBB-N2*. https://www.ti.com/product/RF-HDT-DVBB/part-details/RF-HDT-DVBB-N2?keyMatch=RF-HDT-DVBB-N2, 2023. Acessado em 7 de Dezembro de 2023. 27

[21] Digi-Key Electronics: *MFRC522 - RFID Reader/Writer, 13.56 MHz*. https://mm.digikey.com/Volume0/opasdata/d220001/medias/docus/373/MFRC522.pdf. 27

[22] Nordic Semiconductor: *nRF5340 - High-end multiprotocol SoC supporting Bluetooth 5.2, Bluetooth Mesh, NFC, Thread and Zigbee*. https://www.nordicsemi.com/products/nrf5340, 2023. Acessado em 7 de Dezembro de 2023. 27

[23] Nordic Semiconductor: *Things you should know about Bluetooth range*. https://blog.nordicsemi.com/getconnected/things-you-should-know-about-bluetooth-range, 2023. Acessado em 8 de Dezembro de 2023. 32

[24] Bluetooth SIG, Inc: *Range - Key attributes - Bluetooth*. https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/, 2023. Acessado em 8 de Dezembro de 2023. 32

[25] Wallace, R.: *Antenna selection guide*. Relatório Técnico AN058, Texas Instruments, Dallas, TX, USA, 2010. 32

[26] Impinj: *How can RFID systems be categorized?* https://www.impinj.com/products/technology/how-can-rfid-systems-be-categorized, 2023. Acessado em 8 de Dezembro de 2023. 33

[27] Tompunu, Alan Novi, Yulian Mirza *et al.*: *Room door security system using microcontroller-based on e-ktp*. Em *Journal of Physics: Conference Series*, volume 1500, página 012115. IOP Publishing, 2020. 34

[28] Orange IoT Journey: *FAQ: What Is the Difference Between NFC and RFID?* https://iotjourney.orange.com/en/support/faq/what-is-the-difference-between-nfc-and-rfid, 2023. Acessado em 8 de Dezembro de 2023. 34

[29] Juels, Ari: *Rfid security and privacy: A research survey*. IEEE journal on selected areas in communications, 24(2):381–394, 2006. 35

[30] Statista: *Cellular NFC-enabled handset shipment share worldwide from 2014 to 2020*. https://www.statista.com/statistics/788220/worldwide-cellular-nfc-enabled-handset-shipment-share/, 2023. Acessado em 9 de Dezembro de 2023. 39

[31] NFC Forum: *Fresh Smartphone Statistics And What They Mean For You, NFC, And The World*. https://nfc-forum.org/news/2019-12-fresh-smartphone-statistics-and-what-they-mean-for-you-nfc-and-the-world/, 2023. Acessado em 9 de Dezembro de 2023. 39