Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Bacharelado em Ciência da Computação

Arcabouços para Coleta de RSSI e Evolução de Técnicas de Acordo de Chaves em Redes LoRaWAN

Leonardo Azalim de Oliveira

JUIZ DE FORA
JANEIRO, 2023

Arcabouços para Coleta de RSSI e Evolução de Técnicas de Acordo de Chaves em Redes LoRaWAN

Leonardo Azalim de Oliveira

Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Bacharelado em Ciência da Computação

Orientador: Luciano Jerez Chaves

Coorientador: Edelberto Franco Silva

JUIZ DE FORA

JANEIRO, 2023

Arcabouços para Coleta de RSSI e Evolução de Técnicas de Acordo de Chaves em Redes LoRaWAN

Leonardo Azalim de Oliveira

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM CIÊNCIA DA COMPUTAÇÃO.

Aprovada por:

Luciano Jerez Chaves
Doutor em Ciência da Computação

Edelberto Franco Silva
Doutor em Ciência da Computação

Alex Borges Vieria
Doutor em Ciência da Computação

Francisco Henrique Cerdeira Ferreira
Mestre em Ciência da Computação

JUIZ DE FORA

16 DE JANEIRO, 2023

Resumo

Os meios de transmissão sem fio são considerados vulneráveis do ponto de vista da segurança dos dados trafegados. Uma abordagem comumente utilizada para solucionar essa questão é a de criptografia. No contexto de *Internet of Things* (IoT), em que o número de dispositivos não para de crescer, os métodos de geração distribuída de chaves simétricas que usam de características da camada física se destacam como possíveis soluções para o problema da distribuição de chaves. Dentre as diversas características, o *Received Signal Strength Indication* (RSSI) é um forte candidato, dada a facilidade em obter-se medidas deste parâmetro, que explora a coesão de canal, principalmente em redes *Long Range Wide Area Network* (LoRaWAN). Com foco na reprodutibilidade de pesquisas, este trabalho apresenta os arcabouços de código aberto LoRa RSSI Grabber e RSSignal. O LoRa RSSI Grabber é capaz de coletar e armazenar medidas simultâneas de RSSI em ambos os lados de uma conexão *Long Range* (LoRa) (dispositivo e *gateway*). Através deste arcabouço, foi gerado um conjunto de dados abertos abrangendo diferentes cenários. Por sua vez, o RSSignal implementa a geração distribuída de chaves baseadas no indicador RSSI. As chaves geradas a partir de diferentes conjuntos de dados foram validadas estatisticamente na suíte de testes 800-22 do *National Institute of Standards and Technology* (NIST). Os resultados confirmam a efetividade do método implementado.

Palavras-chave: IoT, LoRa, LoRaWAN, conjuntos de dados de RSSI, geração de chaves.

Abstract

Wireless media are considered vulnerable from a data transmission perspective. A common solution to tackle this issue is the use of cryptography. In the context of *Internet of Things* (IoT), with a growing number of devices, the distributed symmetric key generation methods through physical layer characteristics stand out as possible solutions for the problem of key distribution. Among the available characteristics, the *Received Signal Strength Indication* (RSSI) is a strong candidate, given the ease of obtaining measurements of this parameter, that explores the channel cohesion mainly on *Long Range Wide Area Network* (LoRaWAN) networks. Focusing on research reproducibility, this work proposes the open source frameworks LoRa RSSI Grabber and RSSignal. The LoRa RSSI Grabber enables the collection and storage of RSSI measurements simultaneously on both sides (device and gateway) of a *Long Range* (LoRa) connection. Through this framework, an open data set which comprises multiple scenarios was created. Nevertheless, the RSSignal implements the distributed key generation based on the RSSI indicator. The keys generated using different data sets where statistically validated on the 800-22 *National Institute of Standards and Technology* (NIST) test suite. The obtained results confirm the effectiveness of the deployed method.

Keywords: IoT, LoRa, LoRaWAN, RSSI data set, key generation.

Agradecimentos

Aos meus pais Ana Luce e José Geraldo pelo apoio e incentivo.

A minha irmã Cecília, pela amizade e parceria imprescindível ao desenvolvimento das atividades deste trabalho.

Aos professores Luciano e Edelberto pela orientação, e principalmente, pela troca de conhecimentos sem os quais este trabalho não se realizaria.

Aos membros Rogério, Thiago e Mateus do Laboratório de Telecomunicações Aplicadas (LTA) da Faculdade de Engenharia, pelo compartilhamento de conhecimento relacionado ao material utilizado na parte prática deste trabalho.

Aos integrantes Francisco, Felipe, Salverino, Matheus e Rafael da Coordenação de Infraestrutura de TI do Centro de Gestão do Conhecimento Organizacional (CGCO) da Universidade Federal de Juiz de Fora (UFJF), pelo aconselhamento durante o tempo em que trabalhamos juntos e também pelo apoio durante a parte prática deste trabalho.

Ao Pedro Ivo autor de uma das principais referências utilizadas por este trabalho, pela paciência em transmitir seu conhecimento durante a fase inicial de implementação do arcabouço RSSignal.

Aos professores do Departamento de Ciência da Computação (DCC) pelos seus ensinamentos e aos funcionários do curso, que durante esses anos, contribuíram de algum modo para o meu enriquecimento pessoal e profissional.

"O futuro dependerá daquilo que fazemos no presente".

Mahatma Gandhi

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviações

AD	*Adaptive Data Rate*
ADB	*Android Debug Bridge*
ADR	*Adaptive Data Rate*
AES	*Advanced Encryption Standard*
API	*Application Programming Interface*
Bi-LSTM	*Bidirectional Long Short Term Memory*
BW	*Bandwidth*
CDF	*Cumulative Distribution Function*
CSS	*Chirp Spread Spectrum*
dB	*Decibel*
dBm	*Decibel-milliwatts*
DIY	*Do it yourself*
GPS	*Global Positioning System*
IEEE	*Institute of Electrical and Electronics Engineers*
IoT	*Internet of Things*
IP	*Internet Protocol*
LCDF	*Lossy Cumulative Distribution Function*
LoRa	*Long Range*
LoRaWAN	*Long Range Wide Area Network*
LPWAN	*Low Power Wide Area Network*
LPWA	*Low Power Wide Area*
LRM2M	*Long-Range Machine-to-Machine*
LTE	*Long-Term Evolution*
MAC	*Medium Access Control*
MSD	*Mean and Standard Deviation*
MQTT	*Message Queue Telemetry Transport*
NIST	*National Institute of Standards and Technology*
OTA	*Over-the-Air*
OTAA	*Over-the-Air Activation*
RSSI	*Received Signal Strength Indication*
SHA	*Secure Hash Algorithm*
SNR	*Signal-to-Noise Ratio*
SF	*Spreading Factor*

TTN *The Things Network*

UFJF Universidade Federal de Juiz de Fora

USB *Universal Serial Bus*

V2I *Vehicle to Infrastructure*

V2X *Vehicle to Everything*

V2V *Vehicle to Vehicle*

1 Introdução

Redes de dispositivos conectados à Internet das Coisas (*Internet of Things* (IoT)) estão se tornando cada vez mais pervasivas, de modo que, são cada vez mais comuns nos mais diversos locais e para as mais diversas aplicações. Elas estão presentes em vários ambientes, como os de cidades inteligentes (PASOLINI et al., 2018) e de comunicação entre dispositivos *Long-Range Machine-to-Machine* (LRM2M) (WANG; FAPOJUWO, 2017), chegando até mesmo a serem aplicadas em fazendas inteligentes (CODELUPPI et al., 2020). É estimado que em 2025 existirão aproximadamente 75 bilhões de dispositivos IoT ativados mundialmente (STATISTA, 2016). Esses dispositivos vão gerar cerca de 25 bilhões de conexões, sendo que destas, 11% serão exclusivamente utilizadas por dispositivos de tecnologias *Low Power Wide Area* (LPWA) (MACHINA; GARTNER, 2016).

Em meio aos inúmeros desafios em redes IoT, é possível destacar as questões de segurança envolvendo transmissões de dados em ambiente sem fio. Nesse contexto, inicialmente é exposto o problema abordado neste trabalho (Seção 1.1). Na sequência, são explicitados os objetivos e as principais contribuições alcançadas (Seção 1.2). Por fim, é apresentada a organização do restante deste documento (Seção 1.3).

1.1 Contextualização e Problema

Dentre as tecnologias LPWA para redes IoT, o *Long Range* (LoRa) destaca-se para ambientes de sensores operando com restrições no consumo de energia, pois é otimizado para a transmissão de pequenas quantidades de dados por grandes distâncias, principalmente quando comparado com tecnologias como o Wi-Fi, *Bluetooth* ou *Zigbee* (NETWORK, 2022c). Os dispositivos LoRa operam na faixa de rádio frequência não licenciada abaixo de $1GHz$, e utilizam a modulação de sinal *Chirp Spread Spectrum* (CSS), de propriedade da empresa *Semtech*® (SEMTECH, 2015).

As especificações para dispositivos LoRa detalham apenas o protocolo da camada física e suas configurações. Por sua vez, o LoRaWAN é um protocolo de rede otimizado

para dispositivos LoRa alimentados por baterias, que podem ser móveis ou fixos, capazes de integrar as redes IoT (YEGIN; SORNIN et al., 2017). O LoRaWAN especifica as configurações da camada lógica da infraestrutura de dispositivos LoRa e também a arquitetura das demais seções da rede.

O meio de transmissão sem fio (onde os sinais não são guiados) permite que as mensagens trocadas entre dispositivos legítimos da rede possam estar sendo copiadas por dispositivos não autorizados (BADAWY et al., 2016). Uma possível abordagem para mitigar os riscos advindos deste cenário é a do uso de criptografia. As técnicas de criptografia embaralham os dados de forma que somente os dispositivos que possuem as chaves certas possam ler o conteúdo das transmissões. As chaves podem ser sequências de *bits*, que são usadas par a par (quando se usa o esquema de criptografia de chave pública-privada) ou é uma sequência específica que é distribuída entre os dispositivos (no esquema de chave simétrica). Nesse contexto, é de suma importância que as chaves sejam geradas e distribuídas de forma segura, já que elas são responsáveis por fazer os processos de embaralhamento e de retorno do conteúdo ao seu estado original (legível). O problema de distribuição de chaves ainda é uma área em que ocorre ampla discussão e há diversas propostas como a de se utilizar um canal seguro de distribuição, ou de utilizar-se uma entidade de terceira parte que é confiável, ou mesmo de se fazer uma geração de chaves distribuída (sendo esta última técnica a que foi utilizada neste trabalho).

É importante destacar que redes de dispositivos IoT tendem a possuir um número elevado de nós com limitações em recursos computacionais. Considerando a necessidade de criptografar os dados trafegados no meio sem fio e também as limitações de implementação dos aspectos de segurança nos dispositivos de uma rede LoRaWAN, o problema de distribuição de chaves merece especial atenção neste cenário (JAYASURIYA, 2021).

O conceito de usar características da camada física para geração distribuída de chaves foi apresentado inicialmente por (HERSHEY; HASSAN; YARLAGADDA, 1995) e, desde então, tem recebido contribuições significativas em diferentes sistemas e cenários. Especificamente, a utilização da entropia do indicador *Received Signal Strength Indication* (RSSI) como entrada para geração distribuída de chaves simétricas de criptografia em redes LoRaWAN se mostra uma opção atraente para driblar os desafios da distribuição

de chaves entre as partes (KITAURA; IWAI; SASAOKA, 2007) (DA CRUZ; SUYAMA; LOIOLA, 2021) (HAN et al., 2022), já que o indicador RSSI pode apresentar considerável variabilidade, está presente nas mais diversas tecnologias sem fio e, normalmente, pode ser obtido ou calculado de forma simples.

Quando se trata de tecnologias sem fio amplamente utilizadas, como o padrão IEEE 802.11 (conhecido comercialmente por Wi-Fi), é possível encontrar *softwares* que coletam medidas de RSSI e até mesmo constroem *heatmaps* de forma automatizada. Um exemplo, é o *software Acrylic®Wi-Fi Heatmaps*[1]. Porém, para o ambiente de redes LoRaWAN, não foram encontradas aplicações comerciais que cumpram com o objetivo de coletar medidas de RSSI. Através de uma busca na Internet, foram encontrados alguns poucos projetos individuais no GitHub com este propósito, mas que carecem de documentação de uso e manutenção de código.

Particularmente, a ausência de *softwares* neste sentido resulta na baixa disponibilidade de conjuntos de dados abertos de medidas de RSSI em redes LoRa. Mais difícil ainda é encontrar conjuntos de dados públicos que contenham as medidas de RSSI do dispositivo LoRa e do *gateway* LoRaWAN coletadas simultaneamente. Essa característica é relevante, pois tem aplicação direta na proposta de novas soluções de segurança, incluindo a geração de chaves de criptografia de maneira distribuída.

1.2 Objetivos e Contribuições

O objetivo geral deste trabalho é desenvolver soluções que realizem de forma sistematizada a medição do indicador de intensidade do sinal RSSI em dispositivos LoRa e no *gateway* LoRaWAN. Estes dados serão posteriormente utilizados como entrada para um arcabouço de geração distribuída de chaves baseadas na entropia do indicador RSSI.

Para o processo de medição e coleta do indicador RSSI, este trabalho apresenta o arcabouço LoRa RSSI Grabber. Esse arcabouço coleta simultaneamente as medidas de RSSI em ambos os lados de uma conexão LoRa (dispositivo e *gateway*), acompanhada da localização geográfica do dispositivo obtida através de sinal de *Global Positioning System* (GPS). Com o auxílio do LoRa RSSI Grabber, foram realizadas cinco coletas

[1] ⟨https://www.acrylicwifi.com/en/wifi-heatmaps/⟩

de medidas de RSSI em um ambiente de teste, compreendendo cenários com diferentes padrões de mobilidade do dispositivo LoRa.

Para a etapa de geração distribuída de chaves baseadas na entropia do indicador RSSI, este trabalho apresenta o arcabouço RSSignal. Este arcabouço implementa, de maneira modular, as etapas de geração e validação de chaves, baseado na proposta apresentada por (DA CRUZ; SUYAMA; LOIOLA, 2021). O RSSignal foi testado a partir do conjunto de dados gerado neste trabalho e também a partir de conjuntos de dados de outros autores. As chaves geradas pelo arcabouço foram validadas com o auxílio da suíte 800-22 do *National Institute of Standards and Technology* (NIST), que confirmou a efetividade dos métodos implementados. Os resultados foram publicados no artigo intitulado "RSSignal: um Arcabouço para Evolução de Técnicas de Geração de Chaves Baseadas em RSSI" no XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg) de 2022 (DE OLIVEIRA; CHAVES; SILVA, 2022).

Todo o código fonte e documentação dos arcabouços, bem como o conjunto de dados gerados neste trabalho, estão publicados de forma aberta na Internet, favorecendo a reutilização, extensão e reprodução dos experimentos realizados. A disponibilização aberta destes arcabouços e do conjunto de dados pode beneficiar outros trabalhos que utilizam medidas de RSSI como parte fundamental das suas metodologias. Como exemplos, é possível citar os trabalhos de (DA CRUZ; SUYAMA; LOIOLA, 2021) e (HAN et al., 2022), que tratam de geração de chaves simétricas criptograficamente seguras em redes LoRaWAN; e de (AERNOUTS et al., 2018) que pesquisa a relação entre as medidas de RSSI e a localização de um dispositivo que possibilite fazer o rastreamento do mesmo em grandes áreas urbanas.

1.3 Organização do Documento

Os demais capítulos deste trabalho estão organizados como segue:

- O Capítulo 2 revisa detalhadamente os principais conceitos relacionados ao tema deste trabalho: padrões LoRa e LoRaWAN, indicadores de sinal e fundamentos de segurança em redes sem fio;

- O Capítulo 3 descreve brevemente alguns trabalhos relacionados e apresenta um comparativo das características abordadas pelos autores em relação à este trabalho;
- O Capítulo 4 introduz o arcabouço LoRA RSSI Grabber, detalhando o ambiente de testes e caracterizando os conjuntos de dados utilizados neste trabalho;
- O Capítulo 5 apresenta o arcabouço RSSignal, destacando os detalhes de implementação em cada uma das etapas do processo de geração de chaves;
- O Capítulo 6 descreve os resultados obtidos durante a validação das chaves geradas pelo RSSignal a partir dos conjuntos de dados coletados pelo LoRA RSSI Grabber;
- Por fim, o Capítulo 7 conclui este trabalho, destacando as principais contribuições, discutindo a relevância dos resultados e indicando possíveis trabalhos futuros.

2 Fundamentação Teórica

Este capítulo tem por finalidade apresentar a fundamentação teórica necessária para a compreensão dos principais tópicos abordados neste trabalho: os protocolos de camada física e rede LoRa e LoRaWAN (Seção 2.1), os indicadores de sinal de transmissões sem fio (Seção 2.2) e alguns fundamentos de segurança em redes sem fio (Seção 2.3). Esses conceitos são importantes para a compreensão deste trabalho, pois os protocolos LoRa e LoRaWAN são tecnologias base para os dispositivos IoT utilizados neste trabalho. Além disso, os indicadores de sinal serão utilizados em soluções de segurança para redes IoT.

2.1 Padrões LoRa e LoRaWAN

As tecnologias LPWA entram em cena quando cobertura, confiabilidade e custo benefício são requisitos de uma aplicação ou rede IoT. LPWA é um termo genérico para um grupo de tecnologias que proporcionam comunicações de longa distância que podem cobrir extensas áreas com baixo custo e alta eficiência energética. Até 2013 o termo LPWA nem mesmo existia, porém, quando o mercado de IoT se expandiu rapidamente, LPWA se tornou uma das áreas que mais cresceu dentro do ambiente de IoT (SINHA; WEI; HWANG, 2017).

2.1.1 O protocolo LoRa

O protocolo de camada física LoRa é um esquema de modulação proprietário, baseado na modulação CSS, que foi criado e é mantido pela empresa *Semtech*®. Este protocolo apresenta uma questão relacionada ao equilíbrio entre a taxa de transmissão e a sensibilidade dentro de um canal com *Bandwidth* (BW) fixa. LoRa também implementa uma taxa de transmissão variável, por meio de SFs ortogonais, que fazem com que o responsável por projetar o sistema tenha que lidar com o compromisso que existe entre a taxa de transmissão dos dispositivos e as características de alcance e gasto de energia do sistema (SEMTECH, 2015). A Figura 2.1, traz uma representação gráfica que demonstra esse compromisso de acordo com cada um dos SFs especificados no protocolo.

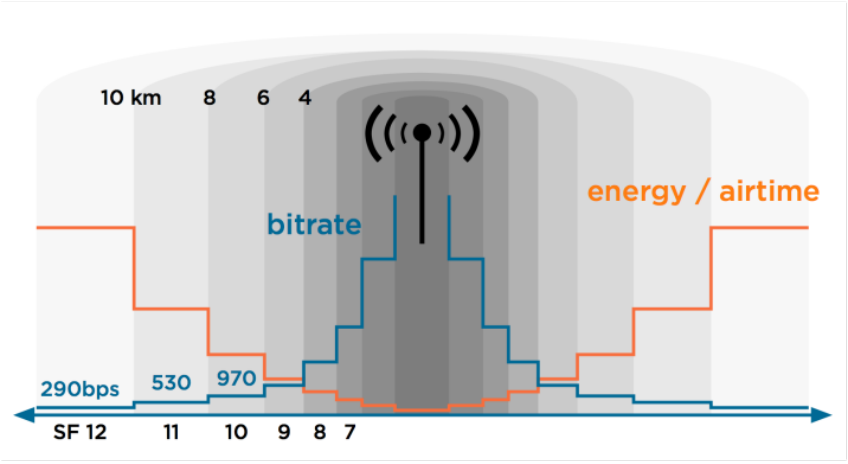


Figura 2.1: Relação entre os *Spreading Factor*s (SFs), suas taxas e tempos de transmissão e o gasto de energia do dispositivo transmissor. Fonte: (DEKKERS, 2022).

O protocolo LoRaWAN é um protocolo de rede que opera na camada de *Medium Access Control* (MAC), otimizado para dispositivos que são alimentados por baterias, que podem ser móveis ou montados em uma localização fixa (YEGIN; SORNIN et al., 2017). O LoRaWAN é um padrão que foi pensado para aplicações IoT baseado na modulação LoRa e que é promovida por entidades como a LoRa Alliance (GARLISI et al., 2021). A primeira especificação do protocolo foi lançada no mês de Janeiro de 2015, sendo as duas iterações mais recentes das especificações as versões 1.0.4 (para série 1.0) e 1.1 (para série 1.1), lançadas, respectivamente, em Outubro de 2020 e Outubro de 2017.

2.1.2 O protocolo LoRaWAN

A especificação do protocolo LoRaWAN trata de assuntos como a topologia da rede, as classes de operação dos dispositivos finais, as taxas de transmissão, e até mesmo sobre a segurança do transporte das informações transmitidas na rede.

A topologia da rede pode ser montada de duas principais formas: em forma de malha, ou em forma de estrela. Quando a rede está operando com seus nós em forma de malha, cada dispositivo final, além de atuar como nó transmissor de dados, atua também como retransmissor de mensagens provenientes de eventuais nós que se conectem à eles. Por outro lado, na operação de topologia em forma de estrela, cada dispositivo final somente atua como nó transmissor e, obrigatoriamente, deve estar dentro da área de cobertura de um dos *gateways* da rede à qual pertence.

Os dispositivos finais são divididos nas classes A, B e C de acordo com o funcionamento das janelas de recepção. Todos os dispositivos LoRaWAN são obrigados a implementar a Classe A de operação. As Classes B e C, podem ou não ser implementadas (YEGIN; SORNIN et al., 2017).

A Classe A, que é a que menos gasta energia, prevê que os dispositivos possam transmitir mensagens de forma bi-direcional e, que após o envio de uma transmissão (*uplink*), sejam abertas duas janelas de recebimento de mensagens (*downlink*). O *slot* de transmissão deve ser agendado seguindo um padrão aleatório de tempo (semelhante ao que acontece no protocolo ALOHA de redes *Internet Protocol* (IP)). Desse modo, todas as transmissões em direção ao dispositivo que precisarem ser feitas, terão de aguardar uma das janelas de recepção.

Já na Classe B, é previsto que o dispositivo possa abrir mais janelas de recepção que no modo de operação anterior. Além das duas janelas que são abertas após uma transmissão (*uplink*), o dispositivo abre mais janelas em outros períodos de tempo pré-determinados. O agendamento das janelas extras é feito por meio do envio de um pacote de sincronização (chamado de *Beacon*) que é enviado pelo *gateway*, que então controla esse parâmetro dos dispositivos.

Por fim, na Classe C os dispositivos permanecem ativos e abrem janelas de recepção praticamente de forma contínua, sendo que estas somente são fechadas nos momentos em que o nó está transmitindo alguma mensagem. Esse modo de operação é o que faz o dispositivo mais gastar energia, porém também produz as menores latências de comunicação entre os servidores e o dispositivo.

2.1.3 Arquitetura de redes LoRaWAN

As redes LoRaWAN, como mostra a Figura 2.2, são comumente compostas por quatro grupos de equipamentos (NETWORK, 2022a): Os dispositivos finais, os *gateways* (concentradores), o servidor de rede e o servidor de aplicação. Os dispositivos finais, cujos exemplos podem ser vistos na Figura 2.2, podem ser sensores ou atuadores dos mais diversos tipos, que geralmente são alimentados por baterias e podem encontrar-se em locais geograficamente isolados.

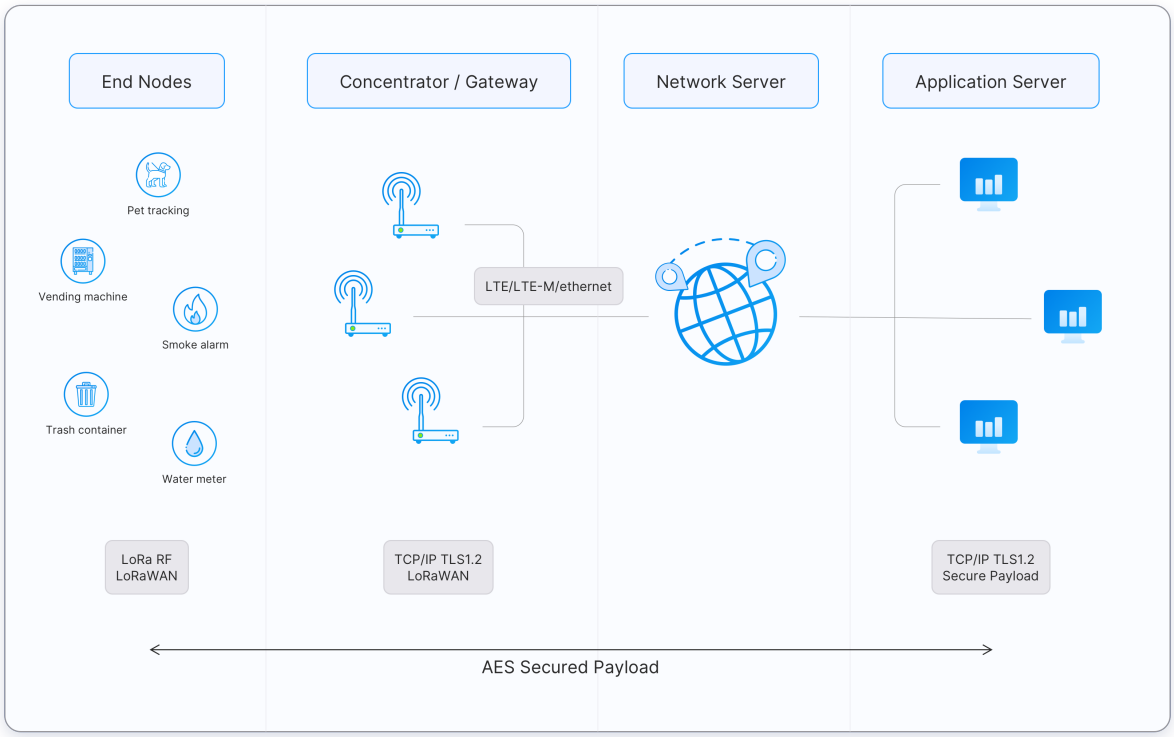


Figura 2.2: Arquitetura padrão de uma rede LoRaWAN. Fonte: (NETWORK, 2022a).

O *gateway* (que também pode ser chamado de concentrador) é o dispositivo responsável por receber as mensagens LoRa dos dispositivos finais e encaminhar elas para o Servidor de rede LoRaWAN. Existem dois tipos de *gateways*: os internos e os externos. Exemplos de *gateways* são mostrados na Figura 2.3. Os internos são construídos para serem plugados diretamente na tomada, são pequenos e usam antenas internas para propagar o sinal por distâncias curtas (como dentro de prédios que possuem muitas paredes internas, ou em locais muito fechados como porões). Já os externos são os que conseguem os melhores resultados quando se trata de alcance, sendo construídos de forma a poder serem conectados em antenas externas (como as feitas de fibra de vidro), e colocados dentro de caixas que permitem que sejam instalados em locais ao ar livre como telhados de prédios ou no alto de postes e antenas de telecomunicações.

O Servidor de rede é responsável por gerenciar os *gateways*, dispositivos, aplicações e usuários dentro de uma rede LoRaWAN, e possui diversas funções como, por exemplo, a de selecionar o melhor *gateway* para o envio das mensagens de *downlink* (mensagens essas que são as que chegam para o dispositivo final), fazer o roteamento dos pacotes de *uplink* (que são os pacotes que são enviados pelo dispositivo final) para o servidor de aplicação

Figura 2.3: Exemplos de *gateways* de redes LoRaWAN. Fonte: (NETWORK, 2022a).

correto, fazer a checagem da autenticidade e integridade das mensagens recebidas dos dispositivos, enviar os comandos do protocolo *Adaptive Data Rate* (ADR) com o objetivo de otimizar as taxas de transmissão dos dispositivos, responder a todas as mensagens da camada MAC, entre outros.

O Servidor de aplicação é o servidor que recebe os dados enviados pelos dispositivos finais podendo processá-los ou armazená-los. Ele também é o responsável por gerar as mensagens de *downlink* da camada de aplicação e enviá-las para os dispositivos finais por meio do servidor de rede.

Ainda dentro deste cenário, é possível destacar que a comunicação entre os dispositivos finais e o *gateway* ocorre por meio do protocolo de camada física LoRa. Os demais saltos podem operar por meio de redes celulares de padrões mais antigos (como 2G ou 3G) ou por meio de redes baseadas em IP (como as redes celulares *Long-Term Evolution* (LTE) e 5G), redes WiFi e Ethernet, ou até mesmo redes de fibra óptica).

2.2 Indicadores de Sinal em Redes Sem Fio

A qualidade de uma transmissão sem fio por rádio frequência pode ser medida por alguns parâmetros, dentre eles, o RSSI. Este indicador é uma medida da intensidade presente

em um sinal de rádio recebido. Em geral, algoritmos verificam a variância na intensidade do sinal para tomadas de decisão, como aquelas relacionadas à escolha da estação base a que devem se conectar (COMMITTEE et al., 2003).

A forma com a qual o RSSI é calculado varia de acordo com cada dispositivo, entretanto, como explicado no trabalho de (BENKIC et al., 2008), essa medida é influenciada pelo ruído do canal de transmissão, e o comportamento que ocorre em campo é quase sempre o da forma mostrada na Tabela 2.1.

Tabela 2.1: Comportamento do RSSI em relação à intensidade de sinal e ruído.

Intensidade de sinal	**Presença de ruído**	**Valor de RSSI**
Baixa	✓	Baixo
Baixa		Baixo
Alta		Alto
Alta	✓	Alto

Os valores de RSSI são representados na unidade de medida *Decibel-milliwatts* (dBm), que podem variar de 0 até o chamado limite de sensibilidade, que é um valor negativo. Por exemplo, para o chip *Semtech SX1272*, os valores poderiam ir de 0 até -137. Quanto maior o valor RSSI, ou seja, mais próximo de 0, mais forte o sinal. Considerando o contexto de dispositivos LoRa, é importante notar que o limite de sensibilidade do RSSI varia em função da BW e do SF (SANCHEZ et al., 2019).

Uma outra medida que pode ser obtida por dispositivos LoRa é o ruído (*noise*) do canal. Comumente esta medida é feita por módulos presentes no *hardware* dos *gateways* ou, em caso de experimentos controlados, por equipamentos industriais especializados.

Segundo o que é mostrado por (SEMTECH, 2022), os dispositivos LoRa podem operar abaixo do nível teórico do limite de ruído de fundo (medido na escala de *Decibel* (dB)) que é de aproximadamente -120 dB. Também é estimado que esse limite é influenciado pela carga atual do canal de transmissão, sendo que o modelo mostra que ele pode variar desde próximo à -150 dB (quando o canal está com 10% de carga) chegando próximo de -130 dB (quando a carga do canal está em 400%).

À partir das medidas de RSSI e de ruído, uma outra medida que pode ser inferida em ambientes de transmissões sem fio é o *Signal-to-Noise Ratio* (SNR). Segundo

(FINLEY, 2017), o SNR pode ser calculado à partir da divisão da potência do sinal de transmissão S pelo ruído do canal N, como mostra a Equação 2.1 abaixo:

$$SNR = \frac{S}{N} \tag{2.1}$$

No contexto de LoRa, é importante notar que: quanto menor o SF, menor o tempo de transmissão, porém também menor o SNR (VALACH; MACKO, 2018); e o ruído pode vir de dispositivos fora do alcance do *gateway*, mas ele ainda sim pode influenciar as transmissões dos dispositivos finais (SEMTECH, 2022).

Uma das possíveis configurações de uma rede LoRaWAN é a que um conjunto de dispositivos, alimentados somente por baterias, está disperso em uma área geograficamente isolada. Em cenários como este, é extremamente importante conhecer a área de cobertura de sinal do(s) *gateway(s)* da rede para o correto posicionamento dos transmissores de forma a evitar áreas de sombra de sinal (onde o sinal pode ser de baixa qualidade ou mesmo inexistente), já que realizar intervenções posteriormente pode ser custoso.

2.3 Fundamentos de Segurança em Redes Sem Fio

A característica natural do meio de transmissão sem fio (não guiado) faz com que as mensagens sejam transmitidas em *broadcast*, ou seja, todos os dispositivos dentro do raio de alcance da transmissão podem obter uma cópia do que está sendo enviado (BADAWY et al., 2016). Por conta disso, a segurança do conteúdo de uma comunicação sem fio merece especial atenção, principalmente em se tratando de uma tecnologia como LoRa cujo sinal atinge longas distâncias, o que consequentemente aumenta as chances de haver um usuário malicioso ou não autorizado na região passivamente escutando o meio.

Comumente são empregadas técnicas de criptografia para cifrar os dados enviados, sendo esta criptografia tratada pelas camadas superiores do protocolo de comunicação sem fio (BADAWY et al., 2016). O protocolo LoRaWAN, desde sua especificação 1.0, prevê a utilização de três diferentes chaves de criptografia de dados, que utilizam como base o algoritmo AES $-$ 128, da família *Advanced Encryption Standard* (AES). As chaves deste algoritmo possuem exatamente 128 *bits* de comprimento: a NwkSKey, a AppSKey e a

AppKey (NETWORK, 2022b). As chaves NwkSKey (*Network Session Key*) e AppSKey (*Application Session Key*) garantem, respectivamente, a segurança da comunicação entre o dispositivo LoRa e o servidor de rede, e do conteúdo (*payload*) da mensagem enviada pelo dispositivo até o servidor de aplicação. Estas chaves (que são parte importante dos processos de embaralhamento e de retorno do conteúdo ao seu estado original, ou seja, forma legível) são únicas para cada dispositivo sendo atreladas à seção, o que significa que, caso o dispositivo esteja utilizando a ativação *Over-the-Air Activation* (OTAA), as chaves serão renovadas a cada nova reconexão com a rede. Por outro lado, a chave AppKey (*Application Key*) somente deve ser conhecida pelo dispositivo e pela aplicação com a qual ele se comunica, já que no processo de OTAA esta chave (que idealmente é personalizada em cada dispositivo) é utilizada no processo de derivação das chaves de seção.

Apesar disso, ainda existem pontos que podem ser melhorados para mitigar vulnerabilidades, como por exemplo no *join procedure* (que foi introduzido nas especificações LoRaWAN à partir da versão 1.1) e consiste em um processo de autenticação do dispositivo LoRa, mas que atualmente é enviado em texto plano na rede e abre caminho para um série de ataques (BADAWY et al., 2016). Devido a complexidade de uma rede de sensores IoT, seja por conta dos desafios relacionados aos recursos computacionais limitados presentes nos nós, ou por conta do processo de distribuição das chaves, diversos autores têm estudado soluções para estes cenários, como visto em (BADAWY et al., 2016), (JAYASURIYA, 2021), (DA CRUZ; SUYAMA; LOIOLA, 2021) e (HAN et al., 2022).

3 Trabalhos Relacionados

O presente capítulo relata os principais trabalhos disponíveis na bibliografia de referência e que se relacionam com os temas abordados neste trabalho, como a utilização do indicador RSSI nas tecnologias LoRa e LoRaWAN (Seção 3.1), disponibilidade de conjuntos de dados de RSSI medidos na camada física dos dispositivos (Seção 3.2) e métodos de geração de chaves a partir da entropia do indicador RSSI (Seção 3.3).

3.1 Utilização do Indicador RSSI

O trabalho de (HIDAYAT et al., 2019) demonstra, de forma prática, como seria possível implementar e instalar uma rede de sensores sem fio utilizando dispositivos LoRa para monitoramento de uma área rural. Os autores focam na descrição do sistema, da metodologia e equipamentos utilizados. Após a coleta dos dados, uma avaliação é feita e conclui-se que: dos 11 pontos analisados na área de teste, somente um não possuiu conectividade (considerando-se a métrica de RSSI). O ponto com melhor performance (como esperado), foi o ponto que tinha visada livre para o *gateway*, sendo que, mesmo com os problemas encontrados, foi possível montar um sistema de monitoramento funcional que coletava os dados de temperatura, umidade e radiação solar e os enviava para nuvem.

A tecnologia LoRa foi a escolhida pelos autores de (LINKA et al., 2018) para o desenvolvimento de modelos para o cálculo de dispersão de sinal. Inicialmente, diferentes dispositivos com diferentes modelos de *chipsets* foram testados em ambiente controlado à fim de determinar a precisão das medidas de RSSI obtidas por eles. Então, numa tentativa de estimar a área de cobertura e o alcance de uma rede LoRaWAN, antes que esta fosse de fato instalada, os autores propõem o uso de 3 diferentes modelos de dispersão de sinal. Foram considerados na modelagem os algoritmos chamados de *Longely-Rice Irregular Terrain Model* (que faz o uso de dados de elevação de terreno do mundo real), Oulu e *Free Space Path Loss Model* no processo de cálculo das predições. Posteriormente, os resultados das simulações foram comparados com dados obtidos em testes reais (testes

estes que foram realizados numa área não muito densamente povoada da Alemanha). Ao analisar os resultados, os autores então concluem que, apesar de não terem encontrado um modelo de predição que se alinhasse perfeitamente com os dados obtidos em campo, o algoritmo *Longely-Rice Irregular Terrain Model* mostrou ser o mais consistente dentre os que foram avaliados, e então destaca-se que ele pode ser especialmente útil em regiões que contenham a presença de cadeias de montanhas. Também é citado que, para garantir uma boa qualidade de recepção de sinal, é desejável que haja uma redução na ocorrência de falsos positivos, mas que isso trará custos adicionais aos modelos e, portanto, o que deve ser considerado para futuras implementações, seria um modelo que possua um balanço entre falsos positivos e falsos negativos. Outro ponto que pode contribuir com uma melhora da precisão dos modelos seria por meio do uso de dados de reflexão e difração de sinal das superfícies presentes na área avaliada.

O trabalho dos autores de (SEYE et al., 2018) propõe um modelo para o cálculo da atenuação do sinal emitido por *gateways* LoRaWAN. Uma rede LoRaWAN experimental, contendo quatro *gateways* que foram instalados em pontos estratégicos, foi montada na cidade de Dakar, capital do Senegal. Então, foram feitas medições de valores de RSSI e SNR de modo que fosse possível estimar a cobertura da rede, esta etapa resultou na produção de *heatmaps*. Posteriormente, com os dados obtidos em campo, os autores procederam à concepção de um modelo de propagação de sinal de forma à estimar o alcance dos *gateways* e, por meio da análise do resultado desta etapa, permitir calcular a cobertura da rede atual ou mesmo realizar simulações com outras configurações possíveis e compará-las. Os autores concluem que à partir do RSSI e do SNR é possível derivar um modelo de estimativa de dispersão de sinal que permite estimar a cobertura de uma antena LoRa. O modelo pode contribuir com simulações feitas antes da instalação real, de forma a otimizar a distribuição de *gateways* em redes LoRaWAN e maximizar a cobertura do sinal deles.

O trabalho dos autores (LIU et al., 2021), propõe um método que, por meio de técnicas de aprendizado de máquina, faz estimativas da atenuação do sinal de dispositivos LoRa. Chamado de DeepLoRa, o método se apoia em sensoriamento remoto para reconhecer automaticamente as características do terreno em torno de um dispositivo

LoRa. O modelo utiliza ainda a técnica chamada de *Bidirectional Long Short Term Memory* (Bi-LSTM) para aprimorar ainda mais as predições feitas pelo DeepLoRa. Então, os autores utilizam dados de uma rede LoRaWAN real (contendo quatro *gateways* e seis dispositivos finais), que foi montada no campus da universidade em Michigan, Estados Unidos. Após avaliar a performance do modelo pelas métricas de acurácia da estimativa e aplicabilidade do modelo, os autores concluem que a solução proposta por eles proporcionou uma taxa de erro de estimativa na faixa de 4dB, o que afirmam ser duas vezes melhor que os resultados descritos até aquele momento pelo estado da arte. Outra descoberta que é destacada é de que não só o tipo de terreno que possui influência na dispersão do sinal transmitido, mas, de acordo com que a distância do caminho que o sinal percorre aumenta, a ordem em que se encontram os diferentes tipos de terreno também muda consideravelmente os resultados da atenuação do sinal. O problema de determinar qualitativamente quais seriam os valores corretos para os parâmetros foi solucionado pelos autores por meio da técnica de Bi-LSTM aplicada sobre imagens de sensoriamento remoto da região estudada.

Por meio de experimentos utilizando uma antena em áreas externas, os autores de (CALLEBAUT et al., 2019) coletaram e agruparam os resultados de cobertura de sinal em três diferentes ambientes do mundo real: uma área litorânea, uma floresta e uma área urbana. À partir dos dados de RSSI (que encontram-se disponíveis *online*), foram construídos *heatmaps*. Além dos dados obtidos, os autores também publicaram a metodologia e detalharam o *hardware* utilizado nos testes, aspecto que favorece a reprodutibilidade do experimento. Concluiu-se que, utilizando-se a faixa de frequência de $868MHz$ e com os transmissores à 1.5 metros de altura do solo e potência de transmissão de 20dBm, a cobertura máxima no ambiente urbano foi de até $1Km$, já no ambiente mais aberto e sem obstruções de visada, o alcance aumentou para até $4Km$ de distância. Os autores então destacam que a tecnologia LoRa é promissora para os ambientes (como na pecuária, no sensoriamento de áreas remotas, no setor de logística, entre outros) em que outras tecnologias *Low Power Wide Area Network* (LPWAN) não cumprem o requisito de alcance, tendo a LoRa as vantagens de não necessitar de assinaturas, e de já haverem opções de dispositivos de baixo custo disponíveis no mercado.

3.2 Conjuntos de Dados Abertos de RSSI

Conjuntos de dados que contenham medidas de RSSI possuem diversas aplicações, servindo de base, por exemplo, para o planejamento da instalação de redes de sensores, a criação de *heatmaps*, ou para alimentar arcabouços que utilizam as medidas como entrada.

O trabalho de (AERNOUTS et al., 2018) relaciona medidas de RSSI com a localização de dispositivos no mundo real que transmitem seus dados de localização via SigFox ou LoRa. De posse dos dados coletados em um ambiente densamente urbanizado, foi criado um conjunto de dados (que se encontra disponível para *download* na Internet). Os autores então propõem uma técnica de rastreamento e estimativa de localização por meio de um algoritmo e concluem que, para as medidas do conjunto de dados de LoRaWAN, obtiveram uma taxa de erro média de $398.4m$.

No trabalho de (GOLDONI et al., 2022), os autores relacionam as medições de RSSI obtidas por dispositivos LoRa em uma rede real montada em campo, com as características climáticas e ambientais locais, como a temperatura do ar, umidade, pressão e outros. É feita uma apresentação detalhada da metodologia aplicada nos experimentos; de quais os equipamentos utilizados; da configuração da arquitetura da rede; dos dados (e seus respectivos formatos e representações) contidos no conjunto de dados que foi construído durante os experimentos (e que encontra-se disponível *online*). Por fim, são feitas análises à partir destes dados obtidos concluindo-se que existe uma relação praticamente linear entre os valores de RSSI medidos e a temperatura ambiente.

Os autores de (SIMKA; POLAK, 2022) montaram e coletaram os resultados de três diferentes configurações de teste em ambientes internos com dispositivos LoRa. O objetivo do estudo era determinar se era possível utilizar a tecnologia de rádio LoRa como parte de um sistema de localização por meio da técnica de triangulação de sinal e medição de valores de RSSI, com os dispositivos operando na faixa de frequência (também não licenciada) de $2.4GHz$. Como resultado, os dados mensurados e utilizados nas análises foram publicados com acesso aberto na Internet. Também foi determinado que, dadas algumas condições (como a posição dos dispositivos LoRa e as características físicas do ambiente a ser monitorado), foram obtidos taxas de erro entre a localização estimada e a real na casa de 2 metros, o que os autores consideraram promissor.

3.3 Geração de Chaves Seguras a Partir do RSSI

O trabalho de (HAN et al., 2020) propõe a utilização de medidas de RSSI em dispositivos LoRa para geração de chaves seguras em redes veiculares com alta mobilidade dos nós. Com este enfoque em mente, os autores citam que os cenários de comunicação *Vehicle to Everything* (V2X) serão cada vez mais explorados, porém que existe uma lacuna em relação à segurança no que tange os processos de distribuição e gerenciamento de chaves, principalmente nos cenários de redes *Vehicle to Vehicle* (V2V) e *Vehicle to Infrastructure* (V2I). O trabalho contém uma proposta de um esquema para geração de chaves seguras aproveitando-se das características da camada física (mais especificamente, da capacidade de medir o RSSI), e do alcance que os dispositivos LoRa possuem. A proposta, que faz o uso de um algoritmo de quantização chamado de *multi-bit* (sendo este uma extensão do algoritmo de aquisição de chaves em cascata), é posta à prova em quatro diferentes cenários de teste no mundo real: um primeiro contendo um nó móvel e outro estático (para simular uma comunicação V2I), e mais três com nós móveis (para simular comunicações V2V), sendo que o movimento de cada um destes três testes funciona de forma a simular: um cenário em que os nós se aproximam com ambos se movendo na mesma direção, um outro onde os nós se aproximam se movendo em direções contrárias e, por fim, um onde os nós se aproximavam com menor velocidade. Ao final, os autores destacam o resultado de um experimento prático onde um atacante passivo tenta obter a chave gerada, afirmando que com a configuração do cenário testado, o atacante não seria capaz de obter a chave somente escutando o meio de transmissão, mesmo estando bem próximo de um dos nós legítimos, por conta da baixa correlação de canal entre ele e os nós legítimos. Como conclusão, tem-se que o método proposto é promissor, por ser considerado seguro, possuir uma boa taxa de geração de *bits* (*bitrate*) e alta taxa de derivação correta de chaves.

Os autores de (HAN et al., 2022) exploram a utilização de *Fuzzy Extractors* em conjunto com características da camada física (nomeadamente a coesão de canal e a medida de RSSI) de dispositivos LoRa para geração de chaves simétricas secretas para criptografia de dados. Durante as etapas de funcionamento do *framework* (chamado de FLoRa), os autores propõem um algoritmo de quantização adaptativo que extrai múltiplos *bits*, sem descarte de medidas de RSSI, de forma à aumentar a taxa de geração de chaves.

A depender da amplitude da sequência de medidas de RSSI obtidas na fase de coleta, o algoritmo de quantização divide a chave em regiões. Para lidar com a disparidade de *bits* que pode ocorrer por conta da extração múltipla, cada região é codificada usando *Gray Code*, de forma que a taxa de erro de *bit* de cada região seja no máximo de 1 *bit*. Na fase de reconciliação de chaves, fazendo-se o uso de um algoritmo de *hash* randomicamente selecionado, cada região é reconciliada separadamente, já que, por conta das características do meio sem fio, a extração de características possivelmente resultou na obtenção de medidas diferentes por cada nó, e as disparidades foram amplificadas pela extração múltipla realizada na etapa de quantização. Ao final da reconciliação de cada região, a chave é novamente concatenada para retornar ao seu comprimento total. Os autores implementam o *framework* em ambientes com dispositivos LoRa reais e realizam diversos testes de geração de chaves entre nós legítimos ao mesmo tempo em que há a presença de um atacante nas redondezas. Os resultados obtidos em seus testes demonstram que na presença de um atacante que se encontra distante dos nós legítimos (distância maior que 1/2 comprimento de onda), há uma baixa correlação de canal entre ele e os nós legítimos. Quando o atacante se aproxima (distância menor que 1/2 comprimento de onda), a correlação de canal entre ele e os nós legítimos aumenta consideravelmente, porém, apesar da possibilidade da amplificação de um eventual ataque de força bruta na chave, o método ainda seria considerado seguro a depender dos requisitos de segurança da aplicação que usará a chave gerada. O desempenho do *framework* FLoRa supera em quase todas as métricas todos os trabalhos com os quais ele foi comparado, e o resultado da análise da suíte de testes estatísticos do NIST demonstra que as chaves geradas são criptograficamente seguras. A proposta, ao contrário de outras soluções, não requer grande poder computacional, nem possui grande complexidade de execução, características desejáveis ao se considerar os dispositivos que integram redes IoT. Assim, conclui-se que a técnica proposta seria uma saída robusta, pois proporciona as características necessárias para manter a comunicação segura (alta taxa de geração de chaves (ou a quantidade de *bits* por unidade de tempo), alta taxa de sucesso na reconciliação de chaves, baixa sobrecarga na comunicação, e eliminação da dependência de uma terceira parte confiável).

O trabalho de (DA CRUZ; SUYAMA; LOIOLA, 2021) propõe um processo com

seis etapas bem definidas que fazem parte de um método de geração de chaves seguras a partir de medidas de RSSI feitas por dispositivos LoRa. Os autores abordam de uma forma mais técnica e demonstram como é possível (a partir do esquema com as etapas de: coleta, pré-processamento, quantização, troca de índices, reconciliação de chaves, e amplificação de privacidade), que nós de uma rede LoRaWAN possam gerar chaves simétricas seguras. Os autores também exploram de forma detalhada a metodologia aplicada durante a montagem do ambiente de testes (por exemplo, como foram feitas as coletas de dados, qual o posicionamento e caminho percorrido pelos nós, qual o esquema lógico por trás da implementação feita em cada um dos nós, entre outros) e, além do processo proposto, também propõem um algoritmo de quantização que se baseia em algoritmos de *Cumulative Distribution Function* (CDF), que é comparado com os algoritmos chamados de *Adaptive Data Rate* (AD) e *Mean and Standard Deviation* (MSD). Como conclusões é dito que, dadas algumas determinadas configurações de parâmetros do processo de geração de chaves, é possível obter chaves criptograficamente seguras em ambientes em que os nós possuam mobilidade (já que, como destacado pelos autores, ambientes com alta mobilidade não poderiam fazer uso da técnica proposta, pois, eventualmente as chaves não seriam suficientemente seguras (de acordo com os testes de validação feitos na suíte de testes do NIST) por conta de que a reciprocidade de canal é severamente afetada pela variação no canal neste tipo de cenário.

3.4 Considerações Finais

A Tabela 3.1 apresenta um resumo contendo, de forma agrupada, as principais características de todos os trabalhos citados neste capítulo. Dentre os aspectos avaliados, foram considerados o acesso aberto ao código fonte e ao conjunto de dados utilizados nos trabalhos. Em sua maioria, o código fonte não é disponibilizado pelos autores, que normalmente apresentam somente um pseudocódigo. Como estão sendo avaliados trabalhos que envolvem medidas de RSSI, os mesmos foram classificados em grupos que utilizam esta medida como entrada ou produzem conjuntos de dados como saída. Além disso, alguns dos trabalhos focam especificamente no problema de geração de chaves a partir da entropia do indicador de qualidade de sinal RSSI.

Tabela 3.1: Comparativo das principais características dos trabalhos relacionados.

Autores / Trabalhos	Arcabouço de Geração de Chaves	Acesso Aberto		Medidas de RSSI	
		ao Código Fonte	ao Conjunto de Dados	Utilizadas como Entrada	Produzidas como Saída
(HIDAYAT et al., 2019)				✓	
(LINKA et al., 2018)				✓	
(SEYE et al., 2018)				✓	
(LIU et al., 2021)				✓	
(CALLEBAUT et al., 2019)		✓	✓	✓	✓
(AERNOUTS et al., 2018)			✓	✓	✓
(GOLDONI et al., 2022)			✓		✓
(SIMKA; POLAK, 2022)			✓	✓	✓
(HAN et al., 2020)	✓	✓*		✓	
(HAN et al., 2022)	✓	✓*		✓	
(DA CRUZ; SUYAMA; LOYOLA, 2021)	✓			✓	
Este trabalho	✓	✓	✓	✓	✓

*Somente pseudocódigo

O presente trabalho contempla todas as características analisadas na Tabela 3.1. Conforme será apresentado no Capítulo 4, a solução LoRa RSSI Grabber pode ser utilizada para construção de conjuntos de dados de RSSI em redes LoRa. Posteriormente, no Capítulo 5, o arcabouço RSSignal utilizará as medidas de RSSI para geração de chaves. Destaca-se que todos os códigos fonte e os conjuntos de dados produzidos por ambas as soluções deste trabalho encontram-se publicamente disponíveis na Internet.

4 Conjuntos de dados de RSSI

O RSSI está presente em muitas tecnologias sem fio. Como a implementação feita por cada protocolo de transmissão e fabricante de dispositivo é diferente, o arcabouço de obtenção de medidas de RSSI deve ser personalizado de acordo com cada caso específico. É nesse contexto que surge a proposta do LoRa RSSI Grabber (Seção 4.1): um arcabouço de envio de pacotes de controle e coleta de medidas de intensidade de sinal em dispositivos LoRa da fabricante *Multitech* e gateways conectados à infraestrutura da *The Things Network* (TTN). Na sequência é apresentada o ambiente de testes deste trabalho (Seção 4.2), seguida da análise dos conjuntos de dados utilizados (Seção 4.3).

4.1 LoRa RSSI Grabber

O LoRa RSSI Grabber é um programa especialmente desenvolvido para coletar medidas de RSSI em ambos os lados de uma conexão LoRa (dispositivo e *gateway*), acompanhado da localização geográfica do dispositivo obtida através de sinal GPS. O código fonte deste programa encontra-se disponível publicamente no GitHub[2].

A arquitetura de obtenção de dados do LoRa RSSI Grabber pode ser vista na Figura 4.1. A comunicação com o aparelho celular ocorre via cabo *Universal Serial Bus* (USB) e com o auxílio do módulo *Android Debug Bridge* (ADB). O celular é configurado para captar o sinal de GPS, determinar as coordenadas de posição e enviá-las ao computador. O computador por sua vez, comanda o dispositivo LoRa conectando-se na placa programadora também via cabo USB. Ele envia comandos para o dispositivo de forma que os pacotes de controle sejam enviados e as medidas de RSSI sejam coletadas. Então, as informações são concatenadas e salvas no disco local em tempo real.

Existem dois *scripts* de conexão com as *Application Programming Interfaces* (APIs) da TTN no LoRa RSSI Grabber: um para consultar a API de *Storage*; e outro para se conectar no *end point Message Queue Telemetry Transport* (MQTT). O primeiro

[2] ⟨https://github.com/oliveiraleo/LoRa-RSSI-Grabber⟩

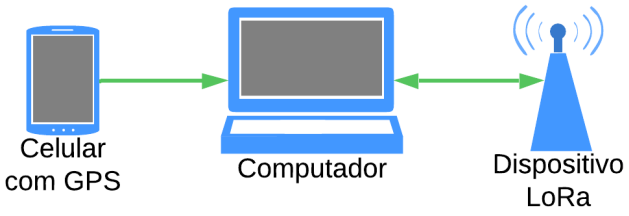


Figura 4.1: Arquitetura de comunicação utilizada pelo LoRa RSSI Grabber.

deve ser usado ao final do processo inicial de envio e recebimento de pacotes de controle, para recuperar os pacotes que chegaram ao *gateway* LoRa. Já o segundo deve ser acionado obrigatoriamente antes do envio dos pacotes, para atender aos requisitos do paradigma *publish-subscribe* utilizado pelo protocolo MQTT.

Por fim, um conjunto de *scripts* produz o arquivo que será parte do conjunto de dados. A Tabela 4.1 apresenta um exemplo do formato do arquivo final, onde os campos armazenados são, respectivamente: *Time* (horário local); *GPS Time* (horário reportado pelos satélites GPS); id (um identificador numérico do pacote de controle); Latitude (calculada via GPS); Longitude (calculada via GPS); Altitude (altura em metros acima do nível do mar); *GPS Precision* (*status* da precisão do sinal de GPS – quanto menor, melhor); *# Satellites* (quantidade de satélites que estão na vista do aparelho); ED RSSI (medida do RSSI do dispositivo LoRa); e GW RSSI (medida do RSSI do *gateway* LoRa).

Tabela 4.1: Exemplo de formato dos arquivos do conjunto de dados deste trabalho.

Time	**GPS Time**	**id**	**Latitude**	**Longitude**	**Altitude**	**GPS Precision**	**# Satellites**	**ED RSSI**	**GW RSSI**
18:40:04	21:40:04	0	−21.77806565	−43.371482533333335	905.1	1	14	−102	−112
18:40:12	21:40:04	1	−21.77806565	−43.371482533333335	905.1	1	14	−106	−112
18:40:20	21:40:12	2	−21.778065583333333	−43.37148258333333	905.1	1	14	−118	−114
18:40:29	21:40:20	3	−21.77806551666667	−43.3714826	905.1	1	14	−112	−110
18:40:37	21:40:29	4	−21.77806548333333	−43.37148268333333	905.1	1	14	−113	−115
18:40:45	21:40:37	5	−21.77802725	−43.37142226666667	905.6	1	14	−114	−111
18:40:53	21:40:45	6	−21.777808666666665	−43.37138255	905.6	1	14	−113	−109
18:41:01	21:40:53	7	−21.77749243333333	−43.37134171666667	902.3	1	14	−120	−120
18:41:09	21:41:01	8	−21.777109016666667	−43.37141931666667	898.2	1	14	−119	−119
18:41:17	21:41:09	9	−21.776702866666668	−43.37149251666666	891.1	1	14	−127	−119
18:41:25	21:41:17	10	−21.776323516666668	−43.371610933333336	889.7	1	14	−124	−118
18:41:33	21:41:25	11	−21.776006666666667	−43.371672833333335	888.8	1	14	−124	−119
18:41:42	21:41:33	12	−21.775928716666662	−43.371561033333336	888.6	1	14	−127	−118
18:41:50	21:41:42	13	−21.776127416666668	−43.37164801666667	886.3	1	14	−116	−116
18:41:58	21:41:50	14	−21.77639968333333	−43.37157441666667	886.0	1	14	−114	−120
18:42:06	21:41:58	15	−21.776708433333333	−43.3714626	888.3	1	14	−102	−113

4.2 Configuração do Ambiente de Testes

A arquitetura do ambiente real de teste pode ser vista na Figura 4.2. O dispositivo LoRa está conectado via barramento à uma placa programadora, que tem a função de alimentar o dispositivo e também serve de interface de comunicação entre ele e o computador. O computador envia comandos via porta serial para o dispositivo, sendo que os dados de localização são recebidos de um aparelho celular que capta sinais de satélites GPS. Além disso, uma conexão de rede (cujo primeiro salto é via WiFi) com as APIs da TTN é necessária para que os pacotes recebidos pelo servidor de aplicação possam ser recuperados e armazenados localmente. O servidor de rede possui conexão direta com o servidor de aplicação e com o *gateway*, que neste caso em específico tem como componentes uma antena LoRa que está conectada via conexão serial à um Raspberry Pi responsável por comandar a antena e se conectar via Internet com o servidor de rede. Cada uma das cores representa diferentes conexões, sendo o verde responsável pelas conexões seriais (USB / via barramento), o rosa pelos sinais de GPS, o preto pelas conexões de rede e, por fim, o vermelho destaca o salto LoRa. As linhas tracejadas sinalizam conexões sem fio e as preenchidas, cabeadas.

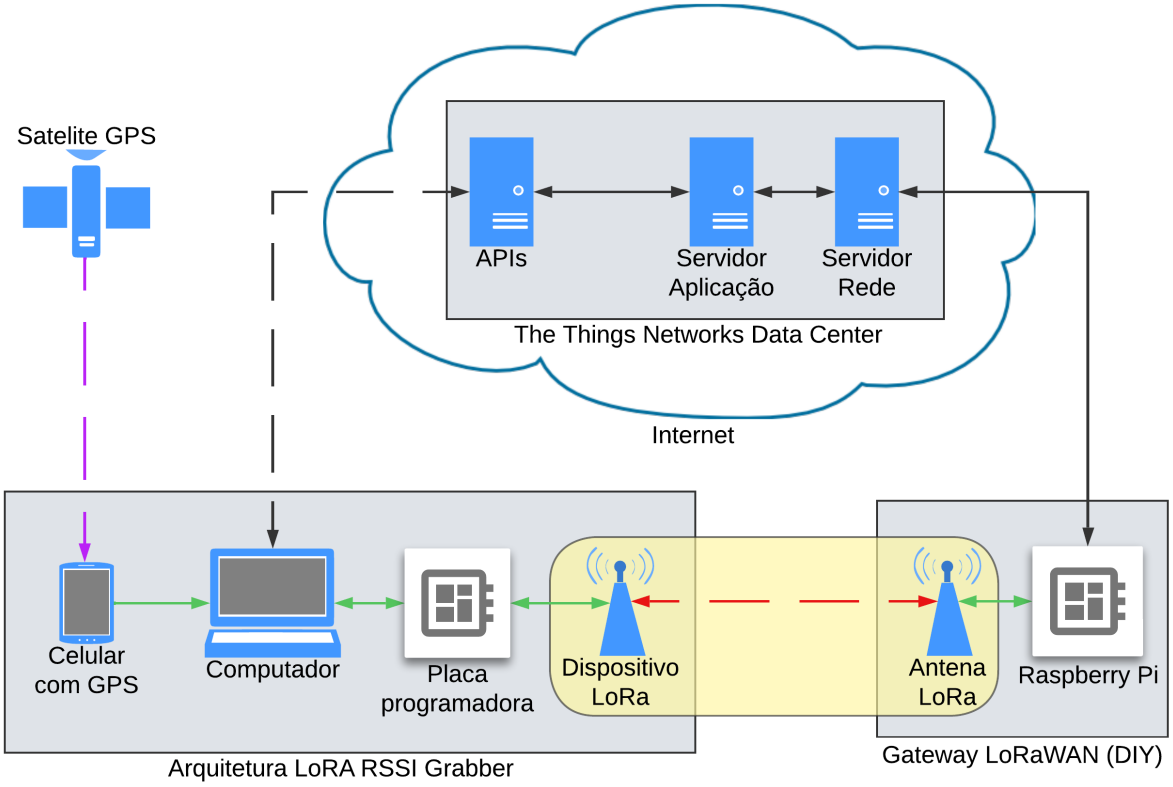


Figura 4.2: Arquitetura LoRaWAN para geração do conjunto de dados.

Os parâmetros técnicos e de configuração dos dois principais elementos LoRa do ambiente de testes (o dispositivo e o *gateway*) encontram-se listados logo abaixo:

- Dispositivo LoRa
  - Multitech mDot 915[3]
  - *Join Mode* (ativação): *Over-the-Air* (OTA)
  - Frequência: AU915 ($915MHz$)
  - Limiares de Sensibilidade
    - RSSI: $-140dB$ a $0dB$
    - SNR: $-20dBm$ a $20dBm$
  - Classe de Operação LoRa: Classe A
  - Potência de Transmissão: $30dB$
  - Ganho da Antena: $5dBi$
  - ADR: Desligado
  - SF: 12
  - BW: $125kHz$
- *Gateway Do it yourself* (DIY) (de baixo custo)
  - Raspberry Pi 3B+
  - Memória RAM: $1GB$
  - Armazenamento: Samsung SD Card EVO Plus (A1/V10) 64GB (130MB/s)
  - Fonte de Alimentação: 12V / 3A
  - Módulo LoRa (RP-SMA/USB)
    - MTAC-LORA 94557300LF[4]
    - Ganho: $3dBi$

[3] ⟨https://www.multitech.net/developer/products/multiconnect-dot-series/multiconnect-mdot/⟩

[4] ⟨https://www.multitech.com/models/94557300LF⟩, ⟨https://www.multitech.net/developer/products/multiconnect-conduit-platform/accessory-cards/mtac-lora/mtac-lora-antenna-specifications-and-connector/⟩

    - Impedância: 50Ω

  - Antena

    - Polidesign PLD COL890-960[5]
    - Material Externo: Alumínio
    - Material Interno: Fibra de Vidro
    - Comprimento: $180cm$
    - Diâmetro: $44mm$
    - Ganho: $9dBi$
    - Potência Máxima de Entrada: $200W$
    - Impedância: 50Ω

4.3 Análise dos Conjuntos de Dados

Nesta seção foram selecionados três conjuntos de dados com valores de RSSI medidos em redes LoRaWAN reais. Um dos requisitos observados para a escolha destes conjuntos foi a de que as medidas de RSSI deveriam ser realizadas de maneira sequencial e simultânea em ambos os lados da conexão (dispositivo e *gateway*), de modo a explorar a coesão do canal. O outro requisito observado foi o de que as medidas de RSSI deveriam refletir cenários com diferentes padrões de mobilidade dos nós.

O primeiro conjunto de dados foi gentilmente cedido por (DA CRUZ; SUYAMA; LOIOLA, 2021). Este conjunto possui três coletas distintas:

- Coleta 1 com 377 medições de RSSI variando entre -9 e -115, representando um ambiente de alta mobilidade;
- Coleta 2 com 676 medições de RSSI variando entre -13 e -65, representando um ambiente com alguma mobilidade; e
- Coleta 3 com 2087 medições de RSSI variando entre -61 a -116, também representando um ambiente com alguma mobilidade.

[5] ⟨https://polidesign.ind.br/produtos?categoria=9⟩

Já o segundo conjunto de dados foi disponibilizado em (SIMKA; POLAK, 2022). Este conjunto possui uma única coleta:

- Coleta 1 com 200 medições de RSSI variando entre -44 e -68, representando um ambiente sem mobilidade.

Por fim, utilizando o LoRa RSSI Grabber, foi produzido um terceiro conjunto de dados. Este conjunto possui acesso aberto por meio de um repositório no GitHub[6] e possui cinco coletas:

- Coleta 1 com 501 medições variando entre -87 e -119, representando um ambiente sem mobilidade;
- Coleta 2 com 508 medições variando entre -100 e -132, também representando um ambiente sem mobilidade;
- Coleta 3 com 496 medições variando entre -59 e -101, que também representa um ambiente sem mobilidade;
- Coleta 4 com 511 medições variando entre -65 e -132, representando um ambiente com alguma mobilidade; e
- Coleta 5 com 498 medições variando entre -76 e -133, representando um ambiente com alta mobilidade.

As principais características de cada uma das coletas analisadas neste trabalho estão sumarizadas na Tabela 4.2. Foram considerados a movimentação dos dispositivos, a linha de visada entre o dispositivo e o *gateway*, o ambiente de testes (interno ou externo) e o tipo da conexão (via *gateway* ou par a par).

A Figura 4.3 mostra as rotas percorridas durante a obtenção das medidas de RSSI das coletas 4 (cor vermelha) e 5 (cor azul) do conjunto de dados deste trabalho. Essas coletas representam diferentes modos de movimentação dos dispositivos: lenta (a pé); e rápida (de carro), respectivamente. A área utilizada para a troca de pacotes de controle compreende a região do campus da Universidade Federal de Juiz de Fora (UFJF).

[6] ⟨https://github.com/oliveiraleo/LoRa-RSSI-dataset-outdoor⟩

Tabela 4.2: Características dos ambientes de coleta de medidas de RSSI.

Referência	Coleta	Movimentação do dispositivo	Linha de Visada	Ambiente Externo	Conexão via Gateway
(DA CRUZ; SUYAMA; LOYOLA, 2021)	1	Rápida		✓	✓
	2	Lenta		✓	✓
	3	Lenta		✓	✓
(SIMKA; POLAK, 2022)	1	Estática	✓		
Este trabalho	1	Estática	✓	✓	✓
	2	Estática		✓	✓
	3	Estática	✓	✓	✓
	4	Lenta		✓	✓
	5	Rápida		✓	✓

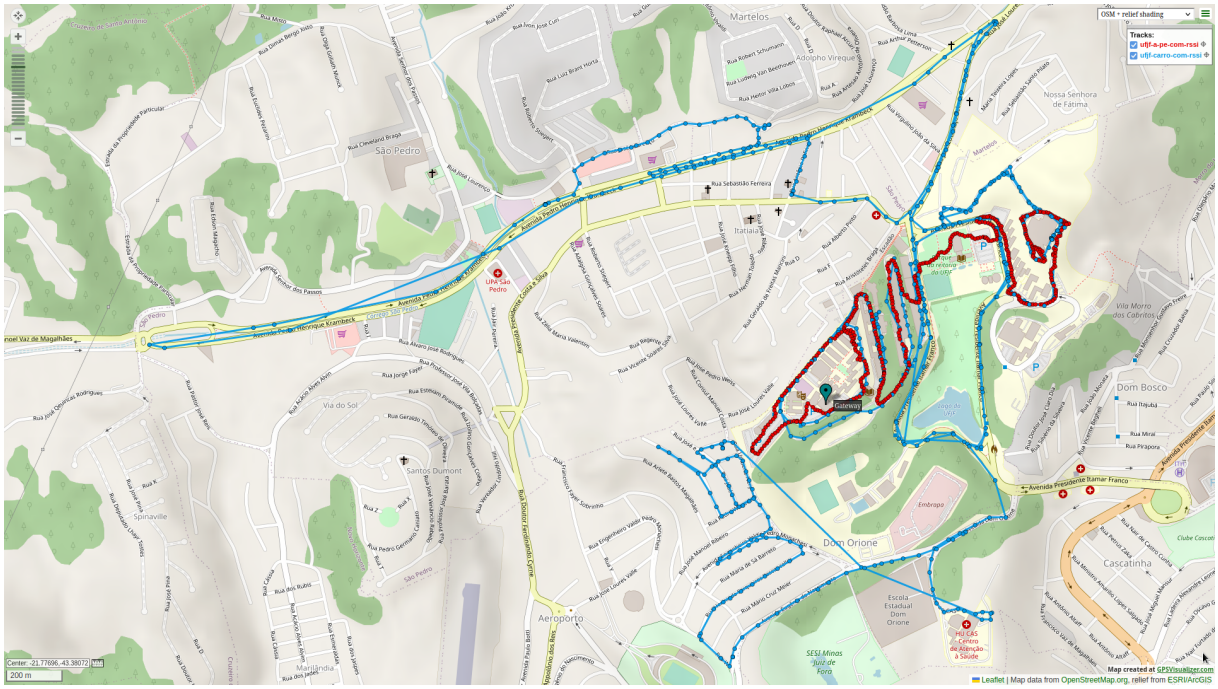


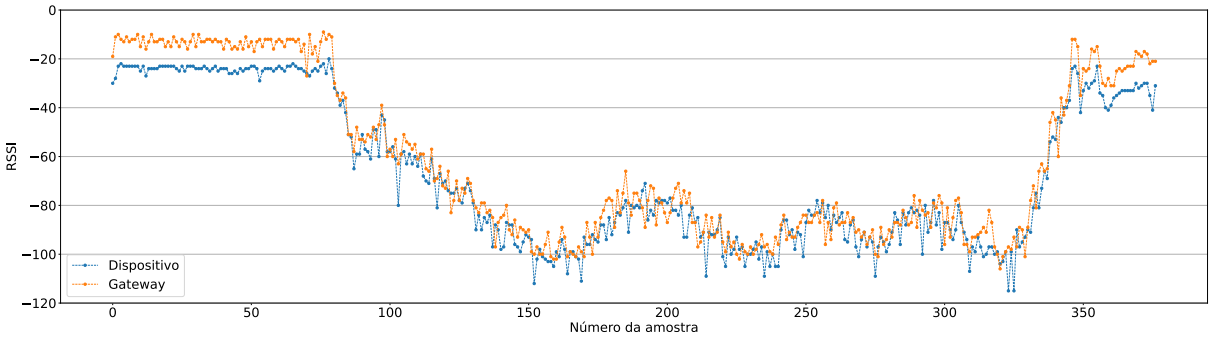
Figura 4.3: Região percorrida nas coletas 4 e 5 do conjunto de dados deste trabalho.

As Figuras de 4.4 a 4.10 mostram a distribuição e a variabilidade estatística das medidas de RSSI observadas em cada uma das coletas dos diferentes conjuntos de dados. É possível observar a grande diferença na quantidade de pacotes nas diferentes coletas dos conjuntos de dados de terceiros (Figuras 4.4 e 4.6). Já para o conjunto de dados deste trabalho (Figuras 4.8 e 4.9), o número de amostras é praticamente o mesmo em todas as coletas: aproximadamente 500 pacotes.

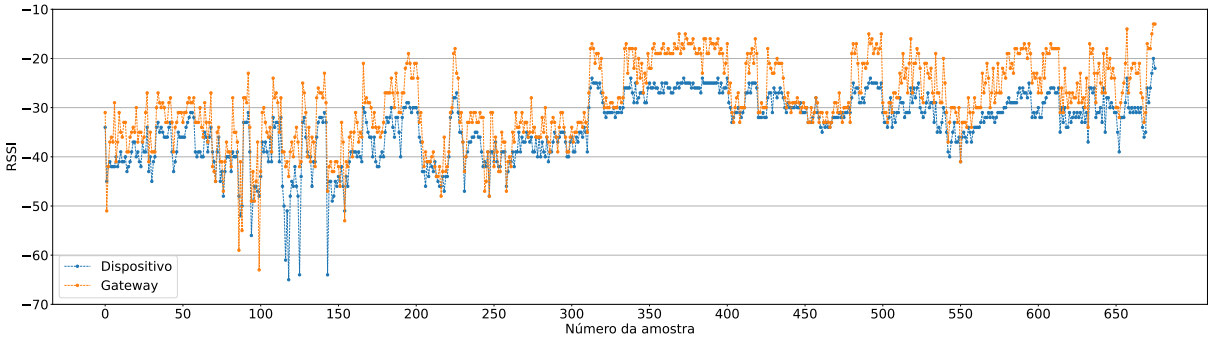
Em relação ao conjunto de dados de (DA CRUZ; SUYAMA; LOIOLA, 2021) (Figuras 4.4 e 4.5), é possível observar uma maior variabilidade no RSSI para a coleta

1, visto que a movimentação rápida do dispositivo nesta coleta tem influência maior na variação do indicador medido para a qualidade do sinal. Em relação ao conjunto de dados de (SIMKA; POLAK, 2022) (Figuras 4.6 e 4.7), é possível notar que a pequena quantidade de pacotes na amostra, obtidos a partir de uma coleta sem mobilidade do dispositivo (estática), resulta numa baixa variabilidade do indicador RSSI.

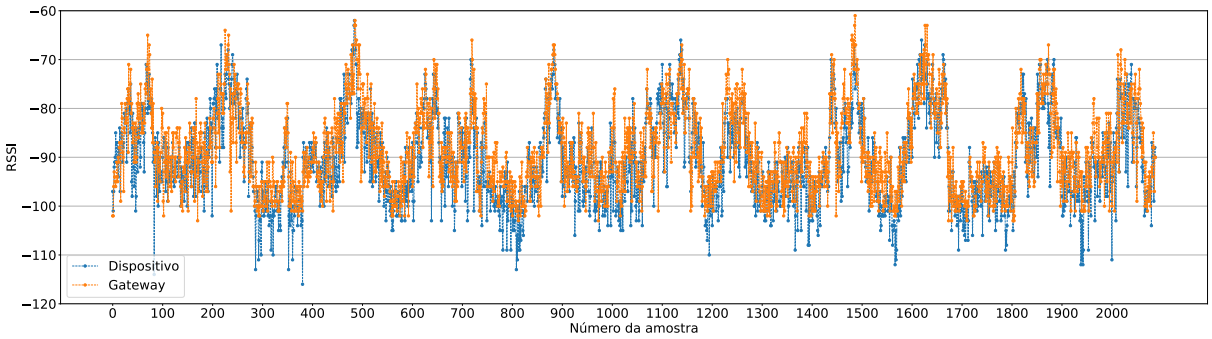
Em relação ao conjunto de dados deste trabalho (Figuras 4.8, 4.9 e 4.10), foram testados três diferentes tipos de ambientes de mobilidade: estático, com baixa mobilidade e com alta mobilidade. As coletas 1, 2 e 3, foram realizadas em ambientes estáticos e apresentam baixa variabilidade no RSSI. Especificamente, a coleta 2, sem linha de visada entre o dispositivo e o *gateway*, apresenta os resultados de RSSI com os menores valores observados. Já as coletas 4 e 5, realizadas em ambientes com mobilidade (lenta e rápida, respectivamente), apresentam maior variabilidade no RSSI. Especificamente, a coleta 5 conta com muitos valores *outliers* decorrentes da rápida movimentação do dispositivo.



(a) Coleta 1

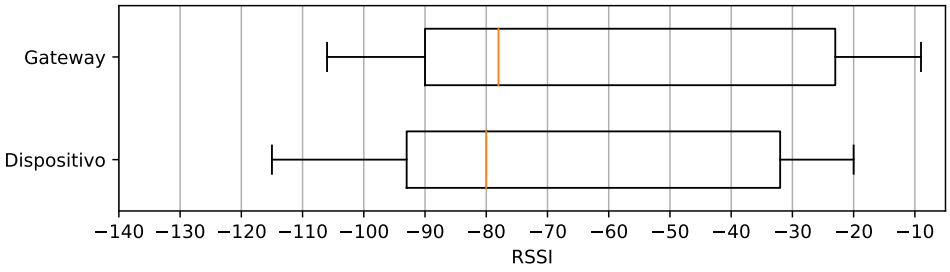


(b) Coleta 2

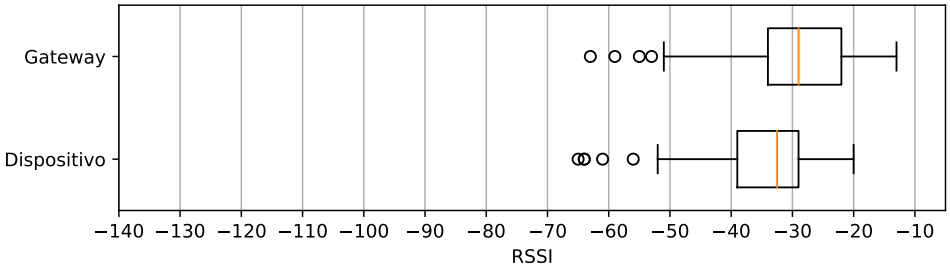


(c) Coleta 3

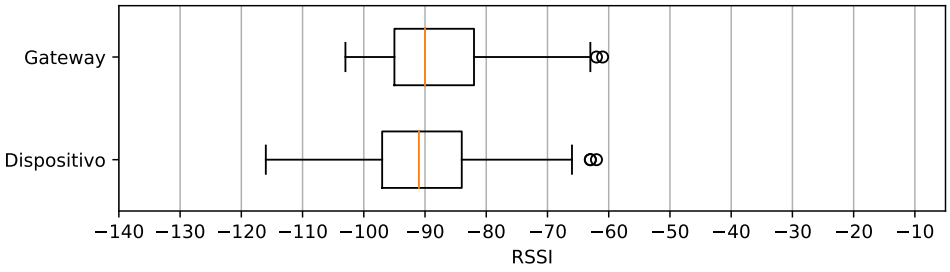
Figura 4.4: Medidas de RSSI do conjunto de (DA CRUZ; SUYAMA; LOIOLA, 2021).



(a) Coleta 1



(b) Coleta 2



(c) Coleta 3

Figura 4.5: Variabilidade das medidas de RSSI do conjunto de (DA CRUZ; SUYAMA; LOIOLA, 2021).

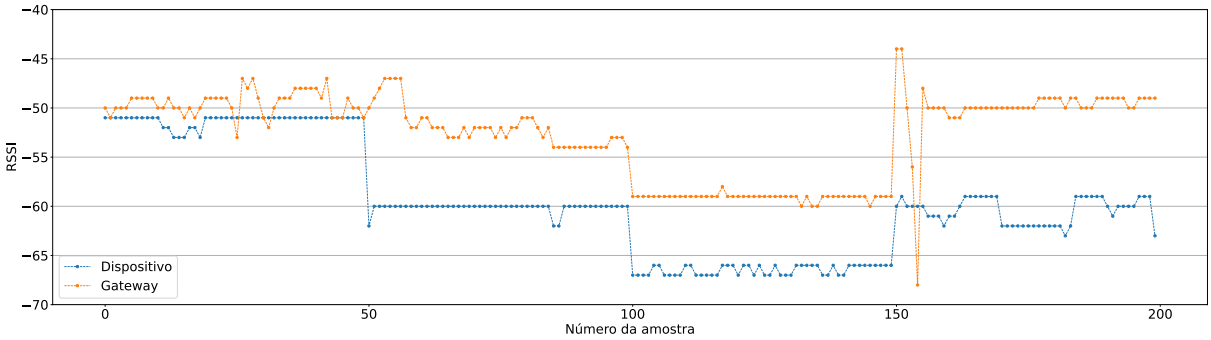


Figura 4.6: Medidas de RSSI do conjunto de (SIMKA; POLAK, 2022).

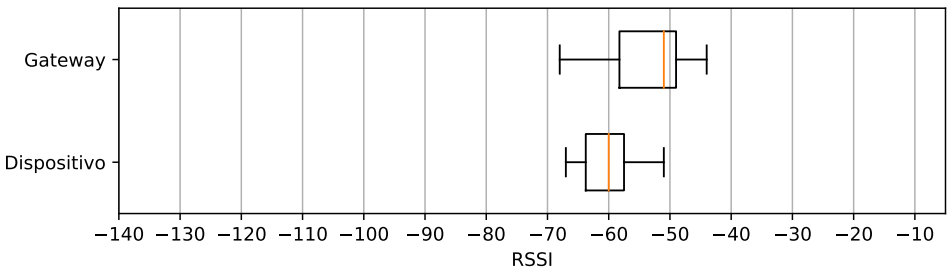
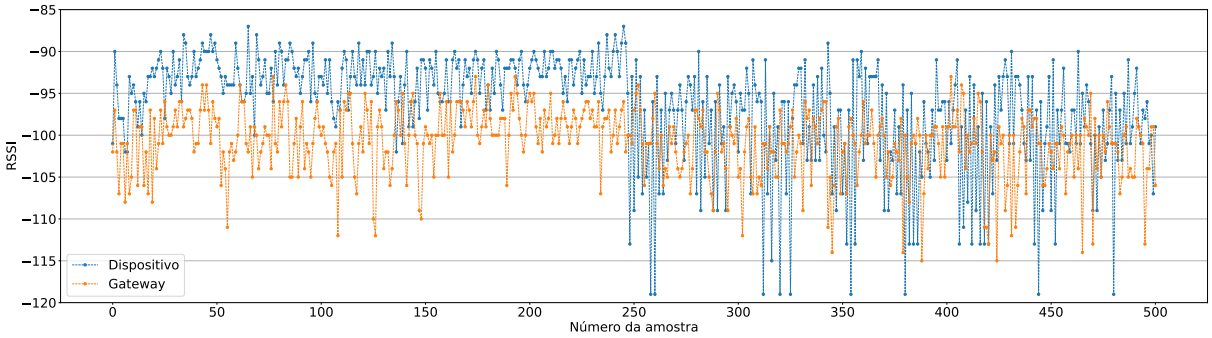
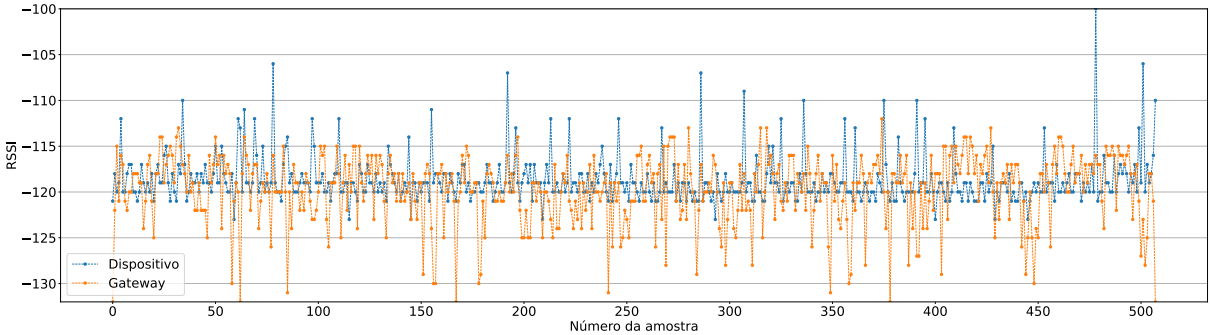


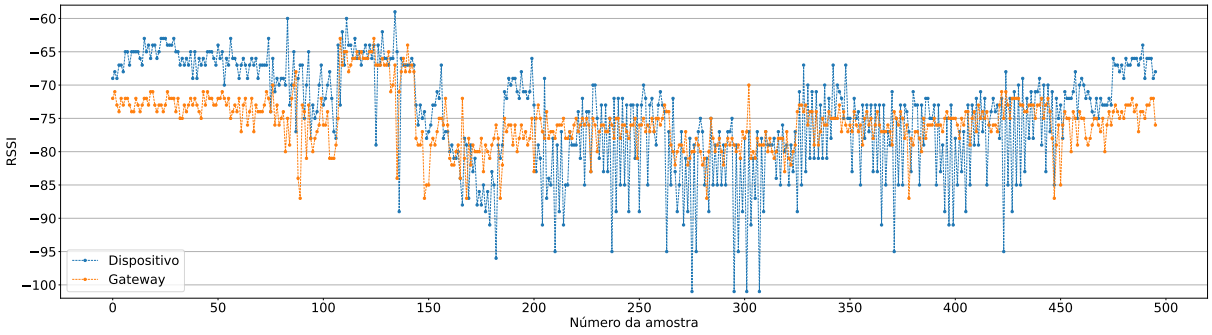
Figura 4.7: Variabilidade das medidas de RSSI do conjunto de (SIMKA; POLAK, 2022).



(a) Coleta 1

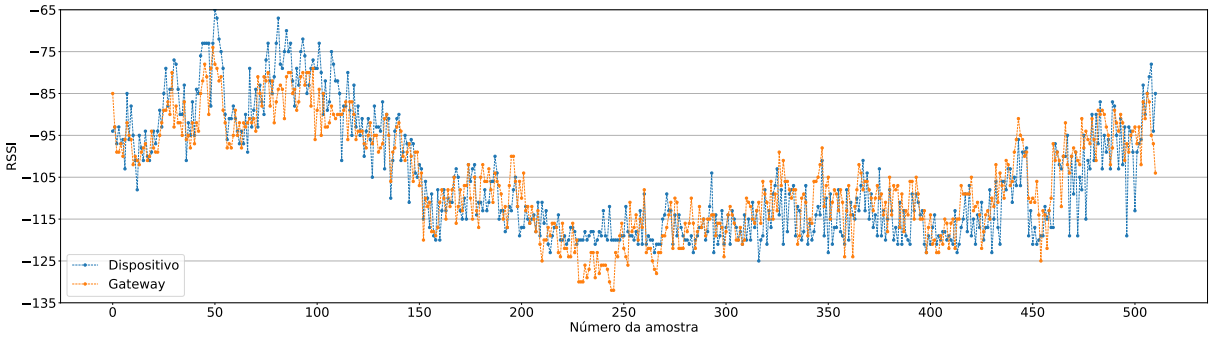


(b) Coleta 2

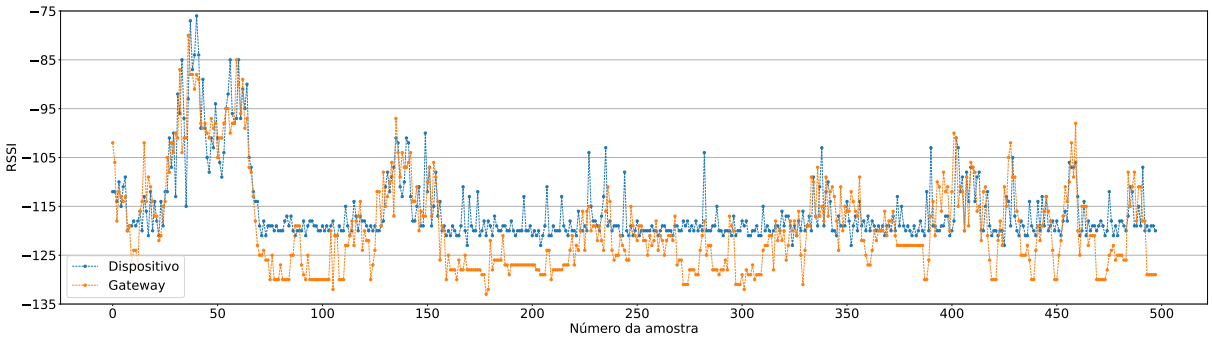


(c) Coleta 3

Figura 4.8: Medidas de RSSI das coletas estáticas do conjunto deste trabalho.

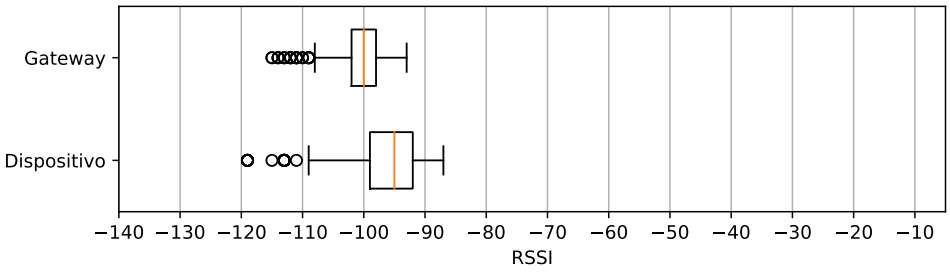


(a) Coleta 4

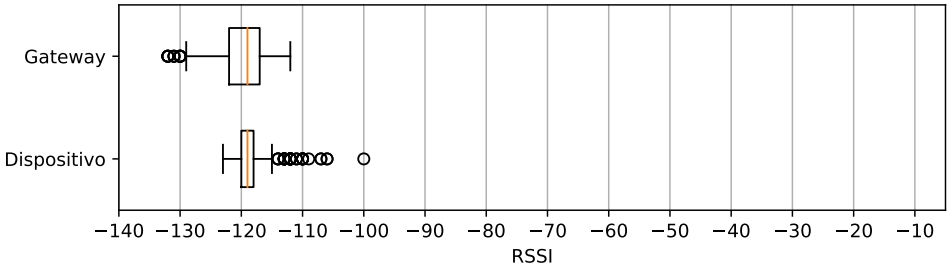


(b) Coleta 5

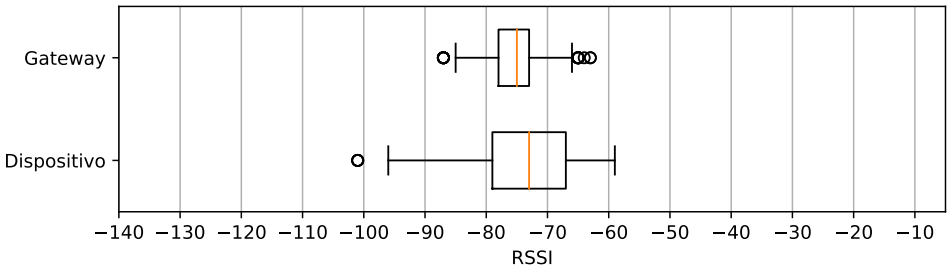
Figura 4.9: Medidas de RSSI das coletas dinâmicas do conjunto deste trabalho.



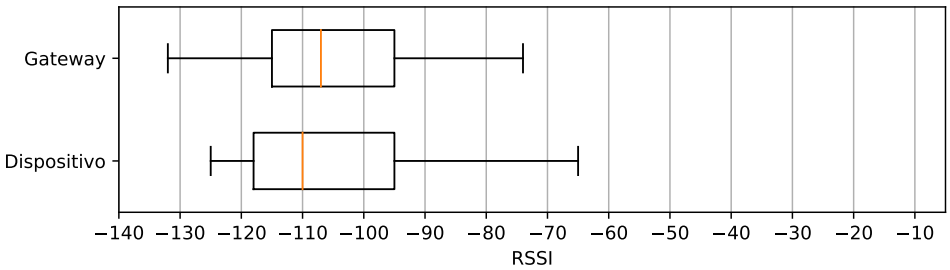
(a) Coleta 1



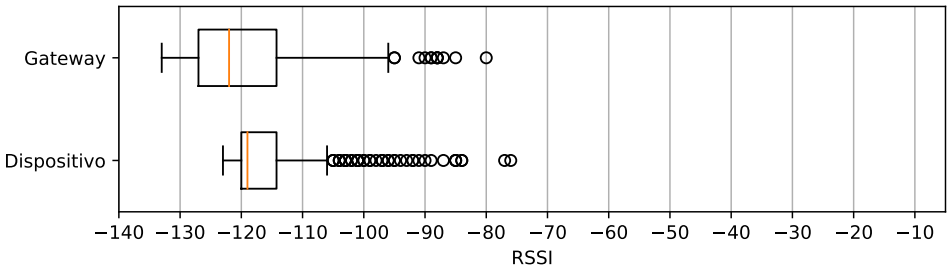
(b) Coleta 2



(c) Coleta 3



(d) Coleta 4



(e) Coleta 5

Figura 4.10: Variabilidade das medidas de RSSI do conjunto deste trabalho.

5 O Arcabouço RSSignal

Considerando a relevância do tema envolvendo a geração e distribuição de chaves em redes LoRaWAN, e também a importância da reprodutibilidade dos resultados de pesquisa, este capítulo apresenta o RSSignal: um arcabouço de código aberto que implementa, de forma modular, as etapas de geração e validação de chaves que utilizam medidas de RSSI como fonte de dados randômicos.

A implementação atual da geração de chaves no RSSignal se baseia na arquitetura proposta por (DA CRUZ; SUYAMA; LOIOLA, 2021). A Figura 5.1 ilustra esta arquitetura, que está dividida nas seguintes etapas que serão detalhadas na sequência: coleta de dados (Seção 5.1); pré-processamento dos dados coletados (Seção 5.2); quantização (Seção 5.3); troca de índices de descarte (Seção 5.4); reconciliação das chaves (Seção 5.5); e amplificação de privacidade (Seção 5.6). Ao final, acontece a geração da chave propriamente dita. O código e a documentação para utilização do RSSignal estão disponíveis em seu repositório público no GitHub[7].

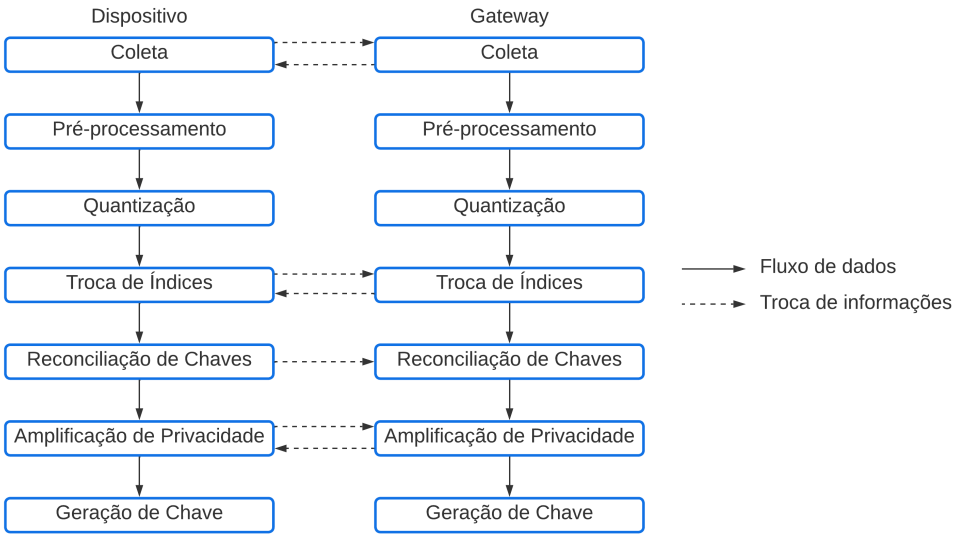


Figura 5.1: Arquitetura para geração de chaves implementada no RSSignal.

[7] ⟨https://github.com/oliveiraleo/RSSignal-LoRa⟩

5.1 Coleta de Dados

A etapa de coleta de dados consiste na troca de pacotes de controle entre o dispositivo e o *gateway*, de forma que a medida de RSSI possa ser extraída diretamente do cabeçalho dos pacotes LoRaWAN e armazenada de maneira independente por ambas as partes. No RSSignal, a troca de pacotes não ocorre de fato, sendo substituída por valores de RSSI previamente coletados simultaneamente no dispositivo e no *gateway*.

Devido ao grande número de modelos de dispositivos, escolheu-se desenvolver como forma de uma prova de conceito o LoRa RSSI Grabber (Seção 4.1), que foi utilizado para construir um dos conjuntos de dados utilizados neste trabalho.

5.2 Pré-processamento dos Dados Coletados

Num ambiente real, o processo de coleta de dados está sujeito às interferências do meio sem fio que podem resultar em perdas de pacotes ou pacotes mal formados. Desta forma, a etapa de pré-processamento é a responsável por identificar os valores de RSSI que serão, de fato, utilizados nas próximas etapas da geração das chaves. O arcabouço RSSignal implementa esta etapa através de um filtro com expressões regulares que extrai unicamente os números válidos das medidas de RSSI armazenadas, desconsiderando outras informações ou mesmo dados inválidos.

5.3 Quantização

A etapa de quantização é a responsável por transformar os valores de RSSI previamente coletados em sequências de *bits*. Em (DA CRUZ; SUYAMA; LOIOLA, 2021), os autores propõem duas abordagens: a quantização baseada na média e no desvio padrão (*Mean and Standard Deviation* (MSD)) e a quantização baseada na função de distribuição cumulativa com perdas (*Lossy Cumulative Distribution Function* (LCDF)). A implementação atual do RSSignal suporta apenas a quantização MSD que, como mostra a Equação 5.1, faz a diferenciação D de uma medida de índice l, de modo que M represente a distância entre l e a medida $l + M$ que será utilizada na diferenciação.

$$D_l = X_l - X_{(l+M)} \tag{5.1}$$

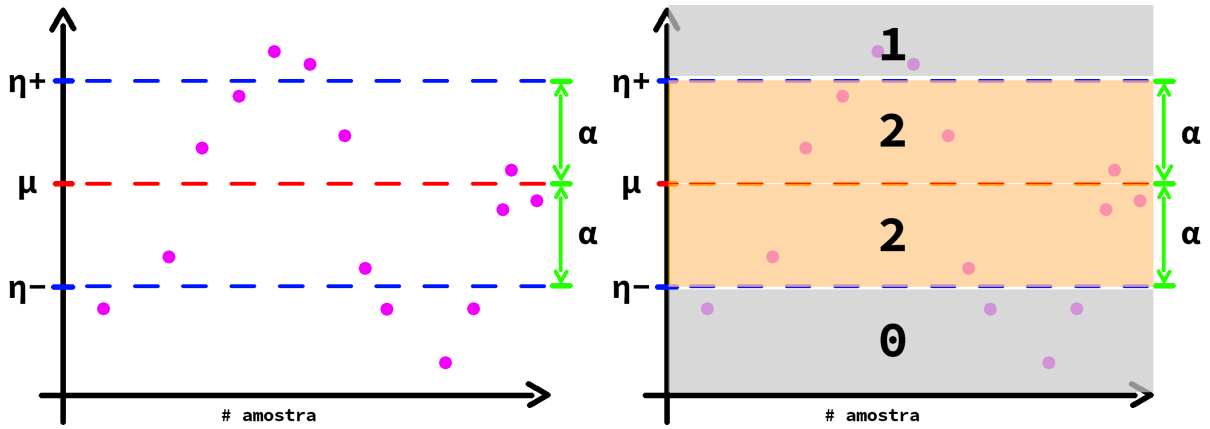
Como mostra a Equação 5.2, a média μ e o desvio padrão σ são usados para definir dois limiares, um superior (η^+) e outro inferior (η^-), sendo α um fator de ajuste da distância entre estes.

$$\begin{cases} \eta^+ = \mu_D + \alpha\sigma_D \\ \eta^- = \mu_D - \alpha\sigma_D \end{cases} \tag{5.2}$$

Então, como mostra a Equação 5.3, os D valores acima do limiar superior são marcados com o *bit* 1, os valores abaixo do limiar inferior são marcados com o *bit* 0 e, por fim, os valores entre os limiares são marcados com o valor 2 para que sejam descartados na etapa seguinte. A marcação de valores como 2 tem como objetivo evitar o uso de medidas agrupadas (medidas próximas à média), já que isso criaria vários blocos com sequências de 0s e 1s na entrada, o que desfavoreceria a randomização da chave gerada.

$$\begin{cases} K_i = 1,\ D_i > \eta^+ \\ K_i = 0,\ D_i < \eta^- \\ K_i = 2, \text{ caso contrário} \end{cases} \tag{5.3}$$

A Figura 5.2a representa um cenário hipotético onde as medidas de RSSI obtidas são representadas pelos pontos na cor rosa. Os parâmetros da Equação 5.1 estão



(a) Antes da marcação dos *bits* (b) Após a marcação dos *bits*

Figura 5.2: Gráficos de exemplo dos parâmetros da etapa de quantização.

representados na imagem: os limiares superior η^+ e inferior η^- (cor azul), a média μ (cor vermelha) e o fator de ajuste α (cor verde). Neste exemplo, a marcação feita pela Equação 5.3, resultaria nos bits mostrados pela Figura 5.2b.

5.4 Troca de Índices

Depois da etapa de quantização, os nós envolvidos no processo devem enviar um para o outro os índices das medidas que serão descartadas (que foram aqueles marcados com *bit* 2 na etapa anterior). Aqui vale destacar que os valores das medidas não são enviados, mas sim os índices que representam as posições delas dentro do conjunto de dados. Isso é importante, pois neste momento o canal de transmissão ainda é considerado inseguro e enviar diretamente os dados coletados poderia acarretar em uma vulnerabilidade de segurança. De fato, o envio em texto plano dos índices de descarte pode fazer com que eles estejam vulneráveis à captura e, então, poderiam ser utilizados para amplificar um ataque de força bruta contra o sistema. Porém, levando em consideração que o atacante não tem acesso físico aos dispositivos envolvidos, ele não seria capaz de determinar qual o número de medidas utilizadas como entrada para a etapa de quantização, nem quais os parâmetros α e M utilizados, nem mesmo quais foram os efeitos destes sobre a entrada.

Após a troca de índices, os nós executam uma operação de concatenação dos índices que eles mesmos já descartariam com aqueles recebidos do outro nó, reduzindo a disparidade entre os *bits* que serão usados nas etapas seguintes do processo.

5.5 Reconciliação de Chaves

Mesmo após a coleta simultânea das medidas de RSSI na etapa de coleta de dados (Seção 5.1) e do descarte seletivo das medidas agrupadas na etapa de troca de índices (Seção 5.4), ainda podem existir *bits* díspares nas sequências de *bits* geradas no dispositivo e no *gateway*. Assim, conforme sugerido em (DA CRUZ; SUYAMA; LOIOLA, 2021), o arcabouço RSSignal implementa um codificador *Reed-Solomon* para diminuir esta disparidade.

Como mostra a Figura 5.3, este codificador é executado de maneira independente em ambos os nós, tendo como entrada a sequência de *bits* da etapa anterior. Ao fazer a

codificação, são gerados símbolos (novos *bits*) de correção. O codificador foi implementado com a taxa de 1 para 2 (1 *byte* de correção para cada 2 *bytes* de dados).

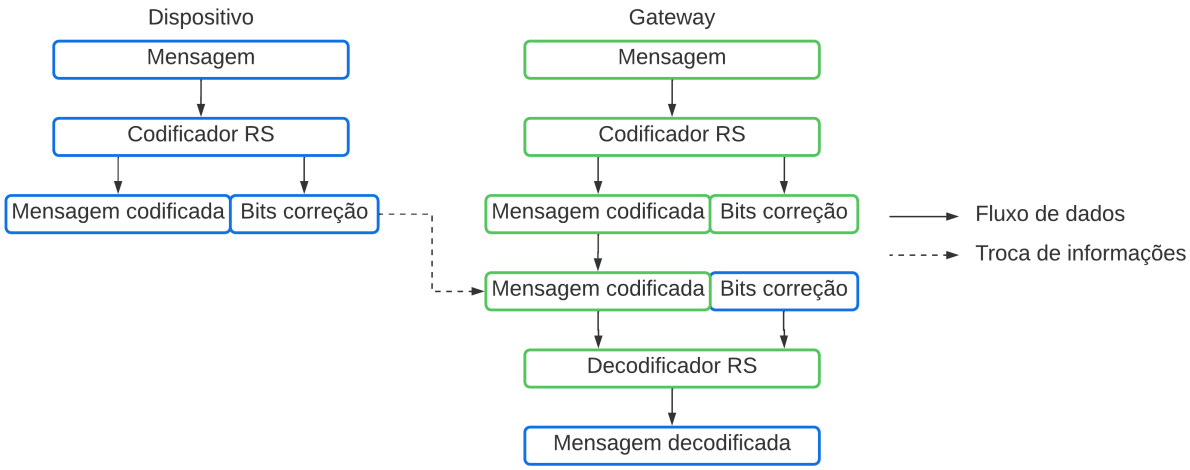


Figura 5.3: Etapa de reconciliação de chaves.

O poder de correção t é dado pela Equação 5.4, onde t é o número máximo de *bits* que podem ser corrigidos por este codificador, n representa a quantidade de *bits* de correção, e k é o comprimento da entrada (FERNANDO et al., 2017).

$$t = \frac{n-k}{2} \tag{5.4}$$

Os *bits* de correção obtidos pelo dispositivo ao executar o codificador são enviados ao *gateway* que, por sua vez, fará uma operação de decodificação e correção de seus *bits* usando as informações recebidas do dispositivo. É importante notar que somente o dispositivo envia seus símbolos de correção para o *gateway*. Como definido por (FERNANDO et al., 2017), não é possível se obter uma mensagem a partir do conhecimento de seus *bits* de código de correção. Logo, mesmo que o atacante intercepte estes símbolos, já não seria possível recuperar as medidas de RSSI da coleta, nem os valores resultantes da etapa de quantização (Seção 5.3).

É importante mencionar que a etapa de pré-processamento de dados coletados (Seção 5.2) pode gerar como resultado um conjunto de dados que possui comprimentos diferentes quando compara-se o que foi aferido no *gateway* e no dispositivo. Por conta do funcionamento do algoritmo de reconciliação de *bits* presente no codificador *Reed-Solomon* que é usado nesta etapa de reconciliação de chaves, é necessário que o número de medidas seja exatamente igual em ambos os lados.

5.6 Amplificação de Privacidade

A etapa de amplificação de privacidade serve para garantir a igualdade entre as sequências de *bits*, geradas de maneira independente pelos nós, antes que elas sejam usadas na geração da chave. Para isso, um algoritmo de *hash* é aplicado às sequências de modo a obter seus resumos. O dispositivo envia então seu resumo para o *gateway* que, por sua vez, confere a igualdade de seu resumo com aquele gerado pelo dispositivo. Em caso positivo, o *gateway* deve enviar uma mensagem de confirmação ao dispositivo.

Esta etapa é implementada no RSSignal com auxílio do algoritmo SHA3-512. Os algoritmos da família *Secure Hash Algorithm* (SHA) foram projetados com a propriedade de que a entrada pode ser facilmente transformada em um resumo, mas existe um nível de complexidade adequadamente alto para encontrar a entrada a partir do resumo (PRENEEL, 2010; DWORKIN et al., 2015). Para subsidiar a escolha da variante adequada, foram avaliados diferentes algoritmos SHA em três dispositivos distintos: um computador pessoal com processador Intel Core i7 (arquitetura *x86*) e $32GB$ de memória; um Raspberry Pi 3B com processador BCM2837 (arquitetura ARM) e $1GB$ de memória; e um Raspberry Pi 3B+ com processador BCM2837B0 (arquitetura ARM) e $1GB$ de memória. As Figuras 5.4 e 5.5 mostram os resultados das avaliações experimentais.

Apesar do algoritmo SHA-1 ter obtido o menor tempo de execução dentre os avaliados, este foi descartado por ser vulnerável aos ataques de força bruta (BOŠNJAK; SREŠ; BRUMEN, 2018). Por sua vez, o SHA3-512 melhora consideravelmente a segurança do resumo se comparado aos demais algoritmos da família SHA3 (TCHÓRZEWSKI; JAKÓBIK, 2019). Por conta disso e da diferença observada entre o tempo de execução dos algoritmos da família SHA3 implementados pelo módulo OpenSSL[8], foi decidido utilizar o algoritmo SHA3-512 no RSSignal. Analisando os resultados, é possível concluir que, na sua pior média, o SHA3-512 foi 16.55% mais lento que o SHA3-224. Entretanto, como demonstrado por (TCHÓRZEWSKI; JAKÓBIK, 2019), o SHA3-512 é 128% mais resistente que o SHA3-224, e 100% mais resistente que o SHA3-256 aos ataques por colisão de *hash* e ataques de força bruta por pré-imagem.

[8] A implementação do módulo da etapa de amplificação de privacidade permite que com poucas mudanças no código seja possível alternar entre os algoritmos SHA e, inclusive, eliminar a dependência do módulo OpenSSL.

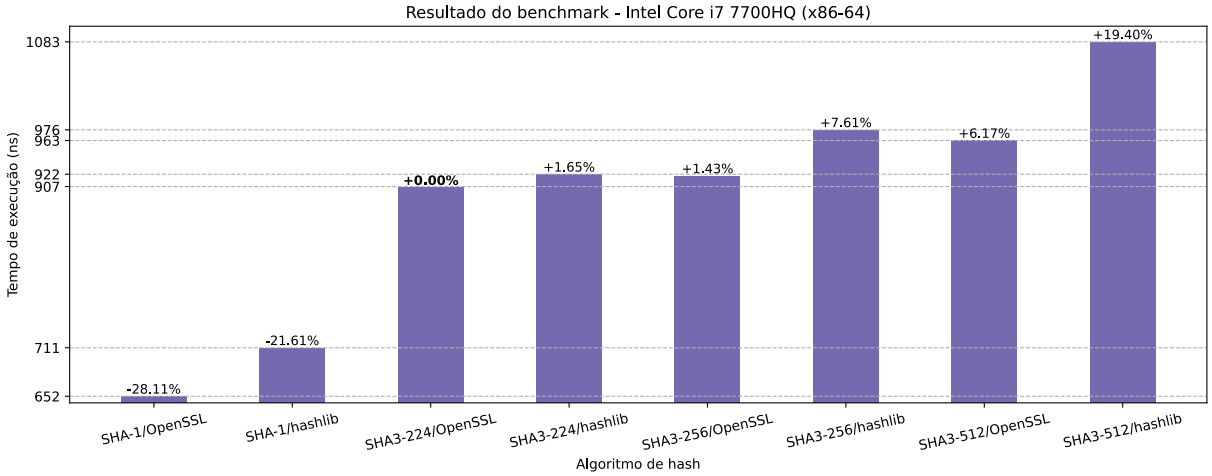


Figura 5.4: Tempo de execução médio na plataforma x86.

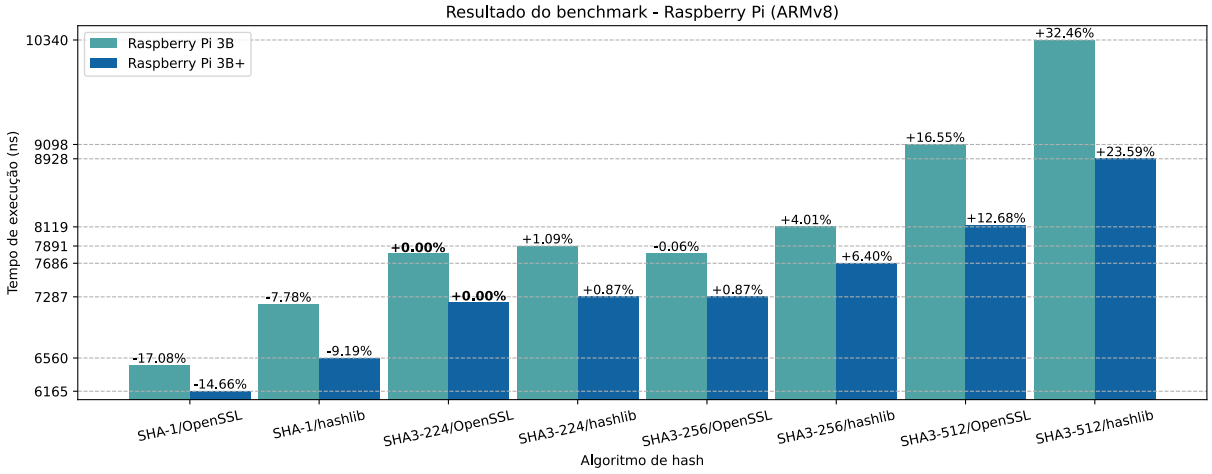


Figura 5.5: Tempo de execução médio na plataforma ARM.

6 Validação de Chaves

O arcabouço RSSignal gera como resultado uma chave. A ele foram adicionados *scripts* que automatizam os testes para validar a segurança das chaves geradas, de acordo com a suíte de testes do NIST 800-22 (Seção 6.1). Os resultados obtidos a partir dos conjuntos de dados apresentados na Seção 4.3 são mostrados e discutidos na sequência (Seção 6.2).

6.1 Suíte de Testes do NIST 800-22

Para validar as chaves geradas, o RSSignal submete as sequências de *bits* para a suíte de testes NIST 800-22 (BASSHAM et al., 2010). O NIST é conhecido por seus trabalhos de padronização, e sua suíte de testes estatísticos 800-22 realiza diversas análises sobre a entropia de uma sequência de *bits*. Os resultados são expressos através do chamado *p-valor*, e são considerados como bem sucedidos aqueles que obtiverem *p-valor* acima de 0.01 (BASSHAM et al., 2010). Como destacado por (MARTON; SUCIU, 2015), uma chave é considerada suficientemente randômica caso seja aprovada em pelo menos 7 dos 15 grupos de testes disponíveis na suíte. Isso não significa que uma chave que fosse reprovada não possa ser utilizada, porém ela não seria tão resistente à ataques de força bruta.

Neste trabalho, foram escolhidos os mesmos oito testes realizados por (DA CRUZ; SUYAMA; LOIOLA, 2021), além do teste de entropia da entrada para tornar o tamanho dela um fator determinante para sua aprovação ou não. Estes testes foram cuidadosamente escolhidos, visto que os demais não trariam resultados estatisticamente relevantes por conta do comprimento das chaves geradas (BASSHAM et al., 2010).

6.2 Resultados Obtidos

As Tabelas de 6.1 até 6.9 apresentam os resultados retornados pela suíte NIST 800-22 para diferentes parâmetros de quantização α e M das coletas dos conjuntos de dados descritos na Seção 4.3. Os valores dos testes reprovados encontram-se marcados em vermelho.

Tabela 6.1: Resultados coleta 1 do conjunto de (DA CRUZ; SUYAMA; LOIOLA, 2021).

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M = 1$	Frequency	0.015	0.818	0.251	0.251	0.479	0.917	0.917	0.705	1.000	1.000	0.577
	Block Frequency	0.220	0.071	0.479	0.479	0.479	0.917	0.917	0.705	1.000	1.000	0.577
	Run	**0.000**	**0.000**	**0.002**	**0.002**	0.046	0.029	0.029	0.016	**0.003**	**0.003**	0.081
	Run (Longest run of ones)	**0.010**	0.140	**0.060**	0.060	0.107	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	0.247 0.314	**0.000** **0.009**	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498	**0.000** **0.498**	**0.000** **0.498**	0.499 0.498
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.026	0.269	0.444	0.444	0.737	0.691	0.691	0.513	0.601	0.601	0.529
	Cum. Sums (Backward)	0.030	0.411	0.302	0.302	0.223	0.596	0.596	0.853	0.601	0.601	0.976
	Input length	375	302	194	194	128	**93**	**93**	**63**	**46**	**46**	**29**
$M = 2$	Frequency	0.030	0.527	0.382	0.429	0.429	0.446	0.292	0.446	0.500	0.446	0.869
	Block Frequency	0.368	0.182	0.052	0.111	0.111	0.446	0.292	0.446	0.500	0.446	0.869
	Run	**0.000**	0.019	0.409	0.222	0.222	0.528	0.990	0.399	0.458	0.708	0.413
	Run (Longest run of ones)	0.985	0.340	0.181	0.161	0.161	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	0.086 0.685	0.046 0.498	**0.000** **0.051**	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.052	0.169	0.213	0.266	0.266	0.364	0.320	0.408	0.355	**0.000**	0.278
	Cum. Sums (Backward)	0.060	0.548	0.683	0.604	0.604	0.762	0.483	0.733	0.807	0.711	1.000
	Input length	374	303	221	160	160	110	**73**	**62**	**55**	**43**	**37**
$M = 3$	Frequency	**0.006**	0.687	0.841	0.323	0.867	0.792	0.770	0.662	0.622	0.599	0.655
	Block Frequency	0.265	0.458	0.479	0.052	1.000	0.724	0.770	0.662	0.622	0.599	0.655
	Run	**0.000**	**0.000**	**0.001**	**0.002**	0.012	0.043	**0.008**	0.084	0.228	0.122	0.027
	Run (Longest run of ones)	**0.006**	0.138	0.169	0.334	0.687	0.213	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	**0.000** **0.073**	0.046 0.724	0.872 0.789	0.931 0.852	0.965 0.899	0.977 0.920	0.993 0.999	0.499 0.498	0.499 0.498	0.499 0.498	0.499 0.498
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	**0.007**	0.704	0.691	0.080	0.307	0.318	0.286	0.203	0.129	1.000	0.272
	Cum. Sums (Backward)	0.012	0.373	0.513	0.507	0.416	0.503	0.482	0.459	0.351	0.297	1.000
	Input length	373	303	225	173	142	129	105	**84**	**66**	**58**	**45**
$M = 4$	Frequency	0.213	0.365	0.127	0.376	0.678	0.510	0.841	0.518	0.907	0.796	0.376
	Block Frequency	1.000	0.032	**0.003**	0.021	0.596	0.510	0.841	0.518	0.907	0.796	0.376
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.004**	**0.009**	0.011	0.026	0.020	0.022
	Run (Longest run of ones)	0.297	0.017	0.056	0.524	**0.003**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	**0.000** **0.000**	**0.000** **0.000**	**0.000** **0.000**	**0.000** **0.162**	**0.000** **0.106**	**0.000** **0.946**	0.499 0.999	0.499 0.999	0.999 0.994	0.499 0.498	0.499 0.498
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.323	0.054	**0.006**	0.037	0.112	0.061	0.178	0.322	0.203	0.141	1.000
	Cum. Sums (Backward)	0.174	0.385	0.222	0.280	0.270	0.264	0.115	0.081	0.158	0.243	0.476
	Input length	372	312	227	184	145	113	100	**86**	**73**	**60**	**46**

Tabela 6.2: Resultados coleta 2 do conjunto de (DA CRUZ; SUYAMA; LOIOLA, 2021).

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M = 1$	Frequency	**0.000**	0.812	0.880	0.738	0.890	0.419	0.931	0.365	0.560	0.732	0.903
	Block Frequency	**0.000**	0.996	0.786	0.596	0.860	0.596	0.724	0.365	0.560	0.732	0.903
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.002**	**0.003**	0.029	0.271
	Run (Longest run of ones)	0.025	0.015	0.091	0.214	0.088	**0.003**	0.089	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	0.647 0.393	0.876 0.658	0.499 0.676	0.499 0.499	0.499 0.499	0.917 0.499	0.499 0.914	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	**0.000**	1.000	0.894	0.983	1.000	0.807	0.955	0.717	0.912	0.909	0.953
	Cum. Sums (Backward)	**0.000**	0.971	0.977	0.995	0.999	0.739	0.987	0.349	0.487	0.972	0.872
	Input length	675	443	395	223	210	185	133	122	106	**77**	**67**
$M = 2$	Frequency	**0.000**	0.184	0.650	0.681	0.398	0.883	0.875	0.051	0.703	0.686	0.655
	Block Frequency	**0.002**	0.647	0.958	0.732	0.596	0.860	1.000	0.022	0.703	0.686	0.655
	Run	**0.000**	0.007	**0.001**	**0.002**	0.035	0.556	0.639	0.530	0.333	0.533	0.358
	Run (Longest run of ones)	**0.000**	0.571	0.146	0.013	0.050	0.119	0.043	0.098	**0.000**	**0.000**	**0.000**
	Serial	0.029 0.054	0.985 1.000	0.742 0.821	0.499 0.106	0.806 0.937	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	**0.000**	0.312	0.956	0.794	0.774	0.963	0.978	0.044	0.847	0.531	0.728
	Cum. Sums (Backward)	**0.000**	0.199	0.762	0.964	0.537	0.998	0.995	0.084	0.971	0.892	0.975
	Input length	674	477	393	289	237	184	162	139	110	**98**	**80**
$M = 3$	Frequency	**0.005**	0.216	0.215	0.606	0.213	0.528	0.374	0.936	0.069	0.521	0.028
	Block Frequency	0.031	0.701	0.527	0.925	0.386	0.377	0.596	0.724	0.052	0.521	0.028
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.002**	0.090	0.054	0.180	0.014
	Run (Longest run of ones)	**0.000**	0.016	0.026	0.031	**0.001**	0.133	0.012	0.308	**0.002**	**0.000**	**0.000**
	Serial	0.647 0.704	0.691 0.856	0.499 0.685	**0.006** **0.038**	**0.002** **0.081**	0.499 0.186	0.499 0.499	0.953 0.991	0.953 0.991	0.985 0.999	0.998 0.977
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	**0.003**	0.400	0.242	0.943	0.239	0.839	0.415	0.973	0.075	0.622	1.000
	Cum. Sums (Backward)	**0.009**	0.370	0.429	0.813	0.270	0.839	0.595	0.993	0.137	0.707	1.000
	Input length	673	512	374	305	258	203	182	153	133	119	**91**
$M = 4$	Frequency	0.105	0.067	0.651	0.743	0.419	0.480	0.562	0.562	0.674	1.000	0.424
	Block Frequency	0.115	0.321	0.337	0.883	0.816	0.860	0.596	0.596	0.596	1.000	0.424
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.003**	**0.001**
	Run (Longest run of ones)	**0.000**	**0.000**	**0.000**	**0.002**	**0.008**	0.016	0.034	0.034	0.097	0.169	**0.000**
	Serial	**0.000** **0.016**	**0.000** **0.000**	0.098 0.676	**0.000** **0.294**	**0.025** **0.003**	0.854 0.228	**0.499** **0.000**	**0.499** **0.000**	0.499 0.100	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.128	0.065	0.578	0.980	0.635	0.724	0.682	0.682	0.916	0.655	0.629
	Cum. Sums (Backward)	0.090	0.121	0.670	0.928	0.751	0.724	0.817	0.817	0.545	0.655	0.387
	Input length	672	524	395	336	259	243	190	190	141	128	100

Tabela 6.3: Resultados coleta 3 do conjunto de (DA CRUZ; SUYAMA; LOIOLA, 2021).

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M = 1$	Frequency	**0.002**	0.601	0.636	0.636	0.815	0.631	0.686	0.762	0.762	0.573	0.530
	Block Frequency	0.753	0.992	0.972	0.972	0.986	0.638	0.960	0.824	0.824	0.596	0.377
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Run (Longest run of ones)	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	0.012	0.012	0.197	0.801
	Serial	**0.001** **0.083**	0.057 0.093	0.038 0.200	0.038 0.200	0.126 0.418	0.018 0.688	0.798 0.981	0.026 0.322	0.026 0.322	0.978 0.999	0.499 0.499
	Entropy	0.039	0.814	0.999	0.999	0.999	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	**0.004**	0.906	0.833	0.833	0.991	0.700	0.694	0.763	0.763	0.571	0.586
	Cum. Sums (Backward)	**0.003**	0.937	0.953	0.953	0.999	0.896	0.906	0.977	0.977	0.857	0.898
	Input length	2087	1774	1291	1291	893	733	612	394	394	255	205
$M = 2$	Frequency	**0.007**	0.437	0.625	0.544	0.594	0.394	0.832	1.000	0.874	0.903	0.898
	Block Frequency	0.299	0.869	0.959	0.932	0.751	0.271	0.365	0.880	0.969	0.984	0.860
	Run	**0.000**	0.011	0.962	0.326	0.217	0.039	0.082	0.251	0.791	0.902	0.897
	Run (Longest run of ones)	**0.000**	**0.000**	**0.003**	0.011	0.034	0.075	0.426	0.418	0.588	0.757	0.289
	Serial	0.089 0.271	0.100 0.157	0.223 0.824	0.922 0.629	0.498 0.038	0.240 0.894	0.322 0.165	0.691 0.760	0.500 0.306	0.499 0.499	0.499 0.499
	Entropy	0.142	0.462	0.972	0.999	0.999	0.999	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	**0.010**	0.514	0.947	0.851	0.855	0.499	0.978	0.923	0.995	0.919	0.968
	Cum. Sums (Backward)	**0.008**	0.834	0.894	0.769	0.828	0.414	0.847	0.923	0.999	0.979	0.997
	Input length	2086	1799	1360	1086	1015	727	557	512	359	270	242
$M = 3$	Frequency	**0.001**	0.284	0.578	0.902	0.902	0.772	0.965	0.965	0.715	0.522	0.403
	Block Frequency	0.224	0.883	0.967	0.410	0.410	0.952	0.997	0.997	0.820	0.860	0.860
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	0.171	0.692	0.692	0.953	0.681	0.663
	Run (Longest run of ones)	**0.000**	**0.000**	**0.003**	0.023	0.023	0.060	0.720	0.720	0.273	0.660	0.356
	Serial	**0.000** **0.000**	0.835 0.837	0.024 0.081	**0.000** **0.043**	**0.000** **0.043**	0.500 0.405	0.840 0.961	0.840 0.961	0.760 0.500	0.500 0.498	0.500 0.498
	Entropy	0.136	0.292	0.659	0.999	0.999	0.999	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	**0.001**	0.505	0.796	0.992	0.992	0.907	0.985	0.985	0.783	0.894	0.507
	Cum. Sums (Backward)	**0.001**	0.383	0.697	0.950	0.950	0.931	0.993	0.993	0.874	0.842	0.640
	Input length	2085	1840	1425	1048	1048	766	517	517	367	244	173
$M = 4$	Frequency	**0.004**	0.778	0.810	0.443	0.443	0.254	0.240	0.402	0.402	0.640	0.679
	Block Frequency	0.132	0.998	0.996	0.809	0.809	0.304	0.248	0.158	0.158	0.969	0.724
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.005**	**0.005**	**0.002**	0.055
	Run (Longest run of ones)	**0.000**	**0.000**	**0.000**	0.052	0.052	0.015	0.349	0.076	0.076	0.383	0.017
	Serial	**0.000** **0.217**	0.992 0.999	**0.000** **0.000**	**0.027** **0.003**	**0.027** **0.003**	**0.000** **0.000**	0.673 0.973	0.499 0.329	0.499 0.329	0.190 0.498	0.499 0.498
	Entropy	0.026	0.135	0.982	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	**0.007**	0.837	0.998	0.731	0.731	0.351	0.386	0.641	0.641	0.849	0.948
	Cum. Sums (Backward)	**0.005**	0.974	0.975	0.438	0.438	0.351	0.284	0.252	0.252	0.743	0.948
	Input length	2084	1816	1409	1061	1061	788	568	411	411	292	210

Tabela 6.4: Resultados coleta 1 do conjunto de (SIMKA; POLAK, 2022).

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M=1$	Frequency	0.000	1.000	1.000	1.000	1.000	0.180	0.180	0.180	0.564	1.000	1.000
	Block Frequency	0.000	1.000	1.000	1.000	1.000	0.180	0.180	0.180	0.564	1.000	1.000
	Run	0.000	0.018	0.018	0.018	0.018	0.050	0.050	0.050	0.387	0.157	0.157
	Run (Longest run of ones)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.000 0.000	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.000 0.000	0.000 0.000	0.000 0.000	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	1.000	0.909	0.909	0.909	0.909	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Backward)	1.000	0.909	0.909	0.909	0.909	1.000	1.000	1.000	1.000	1.000	1.000
	Input length	199	18	18	18	18	5	5	5	3	2	2
$M=2$	Frequency	0.000	1.000	1.000	1.000	0.366	0.366	1.000	1.000	1.000	1.000	1.000
	Block Frequency	0.000	1.000	1.000	1.000	0.366	0.366	1.000	1.000	1.000	1.000	1.000
	Run	0.000	0.450	0.450	0.450	0.554	0.554	0.480	1.000	1.000	1.000	1.000
	Run (Longest run of ones)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.000 0.000	0.499 0.499	0.499 0.499	0.499 0.499	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	1.000	0.513	0.513	0.513	1.000	1.000	0.925	1.000	1.000	1.000	1.000
	Cum. Sums (Backward)	1.000	0.513	0.513	0.513	1.000	1.000	0.925	1.000	1.000	1.000	1.000
	Input length	198	28	28	28	11	11	8	4	4	4	4
$M=3$	Frequency	0.000	0.868	0.868	0.868	0.197	1.000	1.000	1.000	1.000	1.000	1.000
	Block Frequency	0.000	0.868	0.868	0.868	0.197	1.000	1.000	1.000	1.000	1.000	1.000
	Run	0.000	0.615	0.615	0.615	0.847	1.000	1.000	1.000	1.000	1.000	0.414
	Run (Longest run of ones)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.000 0.000	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	1.000	0.779	0.779	0.779	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Backward)	1.000	0.618	0.618	0.618	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Input length	197	35	35	35	15	10	10	8	8	8	6
$M=4$	Frequency	0.000	0.763	0.763	0.763	0.617	0.617	0.439	0.763	0.763	1.000	0.480
	Block Frequency	0.000	0.763	0.763	0.763	0.617	0.617	0.439	0.763	0.763	1.000	0.480
	Run	0.000	0.036	0.036	0.036	0.341	0.341	0.519	0.376	0.376	0.527	0.187
	Run (Longest run of ones)	0.002	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.000 0.000	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	1.000	0.580	0.580	0.580	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Backward)	1.000	0.855	0.855	0.855	0.632	0.632	1.000	1.000	1.000	1.000	1.000
	Input length	196	44	44	44	16	16	15	11	11	10	8

Tabela 6.5: Resultados coleta 1 do conjunto deste trabalho.

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M = 1$	Frequency	0.016	0.731	0.831	0.690	0.553	0.928	0.849	0.829	0.642	1.000	0.466
	Block Frequency	0.142	0.668	0.320	0.860	1.000	0.928	0.849	0.829	0.642	1.000	0.466
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.002**	**0.000**	**0.001**	**0.000**	0.034	0.018	0.046
	Run (Longest run of ones)	**0.001**	**0.005**	0.028	0.550	0.574	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	0.847 0.927	0.891 0.960	0.072 0.020	0.499 0.499	0.921 0.840	0.499 0.068	0.499 0.499	0.499 0.018	**0.000** **0.499**	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.028	0.907	0.901	0.996	0.962	0.997	0.994	0.854	0.899	0.985	0.875
	Cum. Sums (Backward)	0.028	0.869	0.901	0.922	0.471	0.980	0.994	0.982	0.996	0.985	0.750
	Input length	500	415	350	226	182	121	110	**86**	**74**	**58**	**47**
$M = 2$	Frequency	0.028	0.764	0.498	0.498	0.225	0.225	0.069	0.069	0.241	0.241	0.096
	Block Frequency	0.167	0.984	0.731	0.732	0.157	0.157	0.069	0.069	0.241	0.241	0.096
	Run	0.236	0.314	**0.005**	**0.005**	0.237	0.237	0.308	0.308	0.396	0.396	0.616
	Run (Longest run of ones)	0.182	0.229	0.088	0.088	0.538	0.538	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	0.848 0.765	0.739 0.498	0.499 0.916	0.499 0.916	**0.001** **0.150**	**0.002** **0.149**	0.499 0.049	0.499 0.049	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.035	0.978	0.532	0.532	0.259	0.259	0.055	0.055	0.304	0.304	1.000
	Cum. Sums (Backward)	0.050	0.997	0.913	0.913	0.450	0.450	0.138	0.138	0.386	0.386	1.000
	Input length	499	398	263	263	174	174	109	109	**59**	**59**	**36**
$M = 3$	Frequency	0.016	0.881	0.725	0.949	0.940	0.622	0.778	0.499	0.497	0.628	0.366
	Block Frequency	0.230	0.553	0.588	0.724	0.724	0.377	0.778	0.499	0.497	0.628	0.366
	Run	**0.000**	**0.006**	0.994	0.652	0.153	0.727	0.931	0.525	0.861	0.606	0.049
	Run (Longest run of ones)	0.081	**0.002**	0.578	**0.009**	0.605	0.981	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	**0.001** **0.138**	**0.001** **0.183**	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.021	0.859	0.847	0.968	0.997	0.642	0.856	0.572	0.821	0.956	0.721
	Cum. Sums (Backward)	0.021	0.959	0.999	0.935	1.000	0.927	0.995	0.838	0.821	0.876	0.580
	Input length	498	401	290	241	177	148	113	107	**78**	**68**	**44**
$M = 4$	Frequency	0.243	0.299	0.373	0.373	0.555	0.737	0.525	0.756	0.359	0.768	0.369
	Block Frequency	0.847	0.824	0.636	0.636	0.112	0.480	0.525	0.756	0.359	0.768	0.369
	Run	**0.001**	0.029	0.055	0.055	0.389	0.859	0.160	0.249	0.574	0.777	0.739
	Run (Longest run of ones)	0.146	0.565	0.618	0.618	0.665	0.515	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	**0.000** **0.882**	0.895 0.499	0.183 0.499	0.183 0.499	0.082 0.499	0.499 0.102	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.415	0.510	0.468	0.468	0.210	0.359	0.345	0.691	0.414	0.868	0.728
	Cum. Sums (Backward)	0.415	0.510	0.516	0.516	0.600	0.623	0.798	0.947	0.502	0.868	0.561
	Input length	459	409	283	283	184	142	121	**93**	**76**	**46**	**31**

Tabela 6.6: Resultados coleta 2 do conjunto deste trabalho.

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M = 1$	Frequency	0.000	0.601	0.601	0.560	0.560	0.627	0.829	0.633	0.633	0.869	0.869
	Block Frequency	0.000	0.816	0.816	0.724	0.724	0.724	0.829	0.633	0.633	0.869	0.869
	Run	0.000	0.000	0.000	0.000	0.000	0.000	0.001	0.015	0.015	0.625	0.625
	Run (Longest run of ones)	0.032	0.003	0.003	0.016	0.016	0.048	0.000	0.000	0.000	0.000	0.000
	Serial	0.126 0.208	0.757 0.309	0.757 0.310	0.997 0.998	0.997 0.998	0.000 0.117	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.000	0.829	0.829	0.966	0.966	0.993	0.998	0.960	0.960	1.000	1.000
	Cum. Sums (Backward)	0.000	0.912	0.912	0.813	0.813	0.874	0.933	0.670	0.670	0.992	0.992
	Input length	446	366	366	188	188	152	86	70	70	37	37
$M = 2$	Frequency	0.000	0.792	0.444	0.706	0.929	0.929	0.276	0.276	0.248	0.724	0.532
	Block Frequency	0.001	0.855	0.535	0.596	0.929	0.929	0.276	0.276	0.248	0.724	0.532
	Run	0.000	0.000	0.000	0.000	0.003	0.003	0.120	0.120	0.048	0.031	0.897
	Run (Longest run of ones)	0.001	0.006	0.088	0.420	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.001 0.077	0.239 0.158	0.812 0.499	0.499 0.499	0.499 0.078	0.499 0.078	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.000	0.995	0.478	0.786	0.984	0.984	0.347	0.347	0.388	0.892	0.592
	Cum. Sums (Backward)	0.000	0.995	0.794	0.997	0.984	0.984	0.441	0.441	0.388	0.984	0.592
	Input length	506	361	289	175	127	127	54	54	48	32	23
$M = 3$	Frequency	0.000	0.712	0.559	0.592	0.741	0.741	1.000	1.000	0.258	1.000	0.732
	Block Frequency	0.005	0.925	0.869	0.289	0.724	0.724	1.000	1.000	0.258	1.000	0.732
	Run	0.830	0.152	0.283	0.017	0.020	0.020	0.020	0.020	0.178	0.217	0.037
	Run (Longest run of ones)	0.000	0.006	0.056	0.413	0.016	0.016	0.000	0.000	0.000	0.000	0.000
	Serial	0.499 0.037	0.017 0.157	0.810 0.731	0.933 0.983	0.499 0.499	0.499 0.499	0.499 0.008	0.499 0.008	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.000	0.995	0.965	0.566	0.790	0.790	0.967	0.967	0.315	0.950	0.604
	Cum. Sums (Backward)	0.000	0.999	0.849	0.906	0.924	0.924	0.967	0.967	0.406	0.950	0.908
	Input length	505	359	292	171	146	146	74	74	50	42	34
$M = 4$	Frequency	0.000	0.793	0.906	1.000	0.505	0.505	0.232	0.232	0.116	0.237	0.083
	Block Frequency	0.000	0.883	0.855	1.000	0.289	0.289	0.232	0.232	0.116	0.237	0.083
	Run	0.000	0.497	0.556	0.130	0.123	0.123	0.034	0.034	0.084	0.004	0.194
	Run (Longest run of ones)	0.000	0.265	0.220	0.227	0.012	0.012	0.000	0.000	0.000	0.000	0.000
	Serial	0.000 0.000	0.499 0.024	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.000	0.499 0.000	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.000	1.000	0.995	0.984	0.629	0.629	0.303	0.303	1.000	1.000	1.000
	Cum. Sums (Backward)	0.000	0.969	0.999	0.984	0.858	0.858	0.303	0.303	1.000	0.353	1.000
	Input length	504	363	288	174	144	144	70	70	49	35	27

Tabela 6.7: Resultados coleta 3 do conjunto deste trabalho.

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M = 1$	Frequency	0.008	0.436	0.525	0.657	0.799	0.859	0.850	0.225	0.691	0.674	0.257
	Block Frequency	0.100	0.855	0.677	0.860	0.724	0.859	0.850	0.225	0.691	0.674	0.257
	Run	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.025
	Run (Longest run of ones)	0.000	0.000	0.000	0.000	0.251	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.000 0.000	0.000 0.000	0.000 0.000	0.000 0.000	0.033 0.499	0.499 0.499	0.499 0.499	0.499 0.004	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.014	0.690	0.857	0.900	0.913	1.000	0.973	0.364	0.984	0.975	0.372
	Cum. Sums (Backward)	0.014	0.690	0.494	0.734	0.989	0.983	0.853	0.291	0.697	0.778	0.372
	Input length	495	371	299	249	139	126	112	68	57	51	28
$M = 2$	Frequency	0.654	0.509	0.291	0.694	0.593	0.593	0.399	0.399	0.216	0.139	0.157
	Block Frequency	0.675	0.732	0.495	0.860	0.593	0.593	0.399	0.399	0.216	0.139	0.157
	Run	0.209	0.216	0.060	0.131	0.070	0.070	0.154	0.154	0.228	0.577	1.000
	Run (Longest run of ones)	0.000	0.050	0.002	0.818	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.972 0.965	0.010 0.137	0.499 0.499	0.499 0.499	0.979 0.998	0.979 0.998	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.817	0.740	0.428	0.943	0.947	0.947	0.776	0.776	0.432	0.278	0.315
	Cum. Sums (Backward)	0.679	0.540	0.579	0.607	0.493	0.493	0.297	0.297	1.000	1.000	1.000
	Input length	403	330	259	161	126	126	69	69	53	37	32
$M = 3$	Frequency	0.163	0.442	0.222	0.706	0.686	0.930	0.393	0.393	0.691	1.000	0.835
	Block Frequency	0.553	0.570	0.368	0.480	0.724	0.860	0.393	0.393	0.691	1.000	0.835
	Run	0.000	0.000	0.000	0.320	0.121	0.134	0.007	0.007	0.044	0.144	0.292
	Run (Longest run of ones)	0.000	0.024	0.710	0.456	0.510	0.782	0.000	0.000	0.000	0.000	0.000
	Serial	0.000 0.000	0.000 0.000	0.943 0.998	0.499 0.151	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.325	0.702	0.330	0.786	0.933	0.998	0.764	0.764	0.820	0.713	1.000
	Cum. Sums (Backward)	0.191	0.609	0.330	0.997	0.993	1.000	0.358	0.358	0.466	0.713	0.592
	Input length	493	381	324	175	153	129	67	67	57	30	23
$M = 4$	Frequency	0.003	0.915	1.000	0.521	0.263	0.482	1.000	0.606	1.000	0.746	0.853
	Block Frequency	0.015	0.325	0.969	1.000	0.289	0.482	1.000	0.606	1.000	0.746	0.853
	Run	0.969	0.915	0.904	0.166	0.745	0.289	0.663	0.628	0.064	0.108	0.356
	Run (Longest run of ones)	0.031	0.556	0.455	0.308	0.471	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.499 0.968	0.499 0.499	0.499 0.499	0.903 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.004	0.901	0.957	0.829	0.243	0.383	0.646	0.837	0.434	0.289	0.877
	Cum. Sums (Backward)	0.003	0.813	0.957	0.352	0.393	0.895	0.646	0.393	0.434	0.511	0.698
	Input length	492	350	274	197	135	99	84	60	42	38	29

Tabela 6.8: Resultados coleta 4 do conjunto deste trabalho.

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M = 1$	Frequency	0.157	0.662	0.647	0.807	0.780	0.307	0.140	0.574	0.831	0.910	0.662
	Block Frequency	0.313	0.697	0.677	0.882	0.596	0.480	0.216	0.574	0.831	0.910	0.662
	Run	**0.000**	**0.000**	**0.000**	**0.000**	**0.003**	0.015	0.010	**0.000**	**0.003**	0.018	0.861
	Run (Longest run of ones)	0.076	**0.005**	**0.005**	**0.002**	0.132	0.035	0.099	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	**0.000** **0.000**	**0.000** **0.000**	**0.000** **0.119**	0.170 0.249	0.893 0.961	0.499 0.499	0.973 0.997	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.185	0.912	0.944	0.953	0.782	0.610	0.281	0.974	0.983	0.915	0.289
	Cum. Sums (Backward)	0.288	0.793	0.655	0.764	0.976	0.378	0.199	0.688	0.861	0.974	0.611
	Input length	510	425	306	268	206	188	133	114	**88**	**79**	**47**
$M = 2$	Frequency	0.084	0.388	0.474	0.399	0.463	0.265	0.432	0.136	0.035	0.515	0.527
	Block Frequency	0.377	0.719	0.404	0.561	0.596	0.377	0.377	0.136	0.035	0.515	0.527
	Run	0.592	0.876	0.334	0.107	0.241	0.367	0.622	0.491	0.863	0.852	0.180
	Run (Longest run of ones)	**0.005**	**0.002**	**0.004**	0.048	0.128	0.548	0.889	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	0.843 0.857	0.499 0.019	0.781 0.865	0.823 0.906	0.499 0.499	0.499 0.499	0.499 0.084	0.995 1.000	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.125	0.622	0.539	0.663	0.754	0.406	0.665	0.147	1.000	0.712	0.823
	Cum. Sums (Backward)	0.092	0.622	0.790	0.663	0.629	0.465	0.665	0.271	0.070	0.593	0.535
	Input length	509	434	329	276	225	158	131	101	**90**	**59**	**40**
$M = 3$	Frequency	0.183	0.887	0.913	1.000	0.746	0.762	0.762	0.593	0.604	0.659	0.891
	Block Frequency	0.493	1.000	0.925	0.495	0.860	0.596	0.596	0.593	0.604	0.659	0.891
	Run	0.185	0.200	0.662	0.905	0.954	0.452	0.452	0.358	0.895	0.674	0.215
	Run (Longest run of ones)	**0.001**	0.539	**0.005**	0.110	0.245	0.595	0.595	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	**0.000** **0.017**	0.717 0.499	0.499 0.499	0.180 0.499	0.499 0.499	0.499 0.149	0.499 0.149	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.220	0.951	0.958	0.615	0.987	0.784	0.784	0.947	0.947	0.978	0.907
	Cum. Sums (Backward)	0.184	0.995	0.889	0.615	0.778	0.910	0.910	0.947	0.878	0.738	0.979
	Input length	508	445	334	280	239	174	174	126	**93**	**82**	**53**
$M = 4$	Frequency	0.100	1.000	1.000	0.757	0.404	0.826	0.861	0.851	0.833	1.000	0.706
	Block Frequency	0.064	0.704	0.767	0.527	0.112	0.377	0.724	0.851	0.833	1.000	0.706
	Run	**0.000**	**0.000**	**0.006**	**0.004**	**0.009**	0.049	0.294	0.135	0.035	0.099	0.105
	Run (Longest run of ones)	**0.000**	0.171	0.424	0.132	**0.004**	0.457	0.178	**0.000**	**0.000**	**0.000**	**0.000**
	Serial	0.844 0.499	0.876 0.890	0.499 0.841	0.499 0.755	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.082	0.888	0.825	0.754	0.191	0.608	0.377	0.320	0.412	0.477	0.415
	Cum. Sums (Backward)	0.091	0.888	0.825	0.478	0.605	0.427	0.507	0.446	0.280	0.477	0.513
	Input length	507	444	362	261	243	187	130	114	**90**	**72**	**63**

Tabela 6.9: Resultados coleta 5 do conjunto deste trabalho.

	Test / α	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$M = 1$	Frequency	0.005	0.865	0.890	0.942	0.856	0.856	0.486	0.486	0.889	0.889	0.724
	Block Frequency	0.045	0.939	1.000	0.724	0.856	0.856	0.486	0.486	0.889	0.889	0.724
	Run	0.000	0.000	0.000	0.001	0.011	0.011	0.321	0.321	0.482	0.482	0.149
	Run (Longest run of ones)	0.000	0.017	0.690	0.082	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.696 0.999	0.207 0.877	0.891 0.960	0.499 0.172	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.008	0.989	1.000	0.998	0.879	0.879	0.489	0.490	0.897	0.897	0.984
	Cum. Sums (Backward)	0.008	1.000	0.993	1.000	0.981	0.981	0.802	0.802	0.975	0.975	0.742
	Input length	497	313	208	191	122	122	74	74	51	51	32
$M = 2$	Frequency	0.001	0.915	0.272	0.272	0.866	0.860	0.920	0.651	0.651	0.896	0.492
	Block Frequency	0.007	0.985	0.289	0.289	0.860	0.860	0.920	0.651	0.651	0.896	0.492
	Run	0.654	0.831	0.109	0.109	0.397	0.594	0.762	0.667	0.667	0.898	0.838
	Run (Longest run of ones)	0.000	0.007	0.207	0.207	0.452	0.929	0.000	0.000	0.000	0.000	0.000
	Serial	0.499 0.986	0.499 0.153	0.499 0.196	0.499 0.196	0.499 0.098	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.001	0.984	0.432	0.432	0.914	0.819	0.999	0.912	0.912	0.987	0.667
	Cum. Sums (Backward)	0.001	0.999	0.432	0.432	0.990	0.655	0.999	0.717	0.717	0.931	0.793
	Input length	496	354	212	212	140	128	99	78	78	59	53
$M = 3$	Frequency	0.001	0.674	0.583	0.570	0.672	0.626	0.758	0.522	0.251	0.109	0.297
	Block Frequency	0.023	0.495	0.596	0.596	0.860	0.626	0.758	0.522	0.251	0.109	0.297
	Run	0.497	0.841	0.799	0.869	0.454	0.293	0.614	0.304	0.311	0.631	0.770
	Run (Longest run of ones)	0.281	0.800	0.530	0.320	0.790	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.697 0.642	0.239 0.308	0.499 0.196	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.003	0.968	0.729	0.767	0.613	0.651	0.606	0.570	0.502	0.165	0.359
	Cum. Sums (Backward)	0.003	0.778	0.602	0.570	0.913	0.832	0.884	0.861	0.337	0.123	0.359
	Input length	495	362	212	198	139	105	95	88	76	56	45
$M = 4$	Frequency	0.000	0.832	0.946	0.831	0.622	0.201	0.297	0.518	0.819	0.900	0.593
	Block Frequency	0.002	0.755	0.860	0.596	0.860	0.201	0.297	0.518	0.819	0.900	0.593
	Run	0.021	0.168	0.026	0.013	0.144	0.015	0.013	0.034	0.109	0.258	0.192
	Run (Longest run of ones)	0.019	0.368	0.725	0.215	0.187	0.000	0.000	0.000	0.000	0.000	0.000
	Serial	0.697 0.642	0.926 0.938	0.879 0.795	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.499	0.499 0.009	0.499 0.499	0.499 0.499
	Entropy	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
	Cum. Sums (Forward)	0.000	0.904	0.915	0.829	0.795	0.342	0.434	0.757	0.812	0.853	0.813
	Cum. Sums (Backward)	0.000	0.904	0.864	0.632	0.377	0.136	0.213	0.391	0.906	0.739	0.568
	Input length	494	354	219	197	148	120	111	86	76	63	56

Como é possível visualizar nas Tabelas de 6.1 até 6.9, a maioria das configurações rejeitadas concentram-se nos testes *Input length*, que avalia o comprimento da chave, e nos testes *Run* e *Run (longest run of ones)*, que apuram a quantidade de sequências de *bits* 1 na entrada. Sequências com menos de 128 *bits* de comprimento total, possuem altas chances de falhar (BASSHAM et al., 2010). Ao observar os gráficos de variabilidade estatística do RSSI apresentados nas Figuras 4.5, 4.7 e 4.10 e os resultados desta seção, é possível inferir que medidas de RSSI agrupadas e próximas à mediana, sem a presença de um grande número de *outliers*, resultam numa maior taxa de reprovação das chaves nos testes. O agrupamento das medidas também leva a uma maior velocidade na queda do comprimento das chaves à medida que os parâmetros α e M vão aumentando, como pode ser observado nos resultados da coleta do conjunto de dados de (SIMKA; POLAK, 2022) (Figuras 4.6 e 4.7 e Tabela 6.4). Outra característica observada é a influência negativa das medidas consecutivas concentradas abaixo ou acima dos limiares η, o que leva a uma sequência de *bits* repetidos na chave gerada.

Também é possível observar que a primeira coluna de cada tabela (resultados para o parâmetro $\alpha = 0.0$), foi reprovada na grande maioria dos casos. Este valor de α representa as configurações onde, após a etapa de quantização, não haveria descarte de medidas de RSSI. Esse comportamento demonstra a importância da etapa de descarte de medidas para a geração de sequências suficientemente randômicas. Há também uma relação direta entre o parâmetro α e o comprimento da chave gerada, pois quanto maior o valor de α, menor a chave. Esse comportamento ocorre por conta do ajuste que este parâmetro provoca na fase de descarte de medidas, controlando a distância com que os limiares η^+ e η^- ficam em relação à média μ.

Ao comparar os gráficos de variabilidade estatística do RSSI (Figuras 4.5, 4.7 e 4.10) com as características das coletas, é possível notar que quanto menor a movimentação dos dispositivos LoRa, mais compacta é a distribuição das medidas de RSSI. Isso afeta diretamente a velocidade com que o comprimento das chaves geradas decresce a medida que o parâmetro α da quantização aumenta, levando a um menor número de configurações que são aprovadas nos testes.

7 Conclusão

Este capítulo resume as contribuições do trabalho (Seção 7.1), discute em torno do tema abordado (Seção 7.2), e lista possíveis trabalhos futuros (Seção 7.3).

7.1 Principais Contribuições

No presente trabalho foram apresentados o LoRa RSSI Grabber: um arcabouço para coleta e armazenamento de medidas de RSSI em dispositivos LoRa; e também o RSSignal: um arcabouço modular para geração de chaves a partir de medidas de RSSI já coletadas. A arquitetura das soluções e os testes realizados foram descritos com riqueza de detalhes. Todo o código fonte e documentação dos arcabouços, juntamente com o conjunto de dados coletados neste trabalho, estão publicados de forma aberta na Internet, favorecendo a reutilização, extensão e reprodução dos experimentos realizados.

A construção e disponibilização de conjuntos de dados de medidas de RSSI abertos, viabilizada pelo LoRa RSSI Grabber, favorece outros trabalhos que podem utilizar destes como parte de seu processo de teste e/ou validação. Além disso, a partir da análise dos resultados obtidos no processo de validação das chaves geradas pelo arcabouço RSSignal, foi possível concluir que o método implementado é efetivo, visto que houveram testes aprovados em diversas das configurações avaliadas.

7.2 Discussão

A utilização da camada física de dispositivos IoT como entropia para arcabouços de geração distribuída de chaves simétricas se mostra uma forte candidata para aumentar a segurança dos dados trafegados em meios sem fio. Isso se dá, principalmente, por conta da ausência da necessidade de estabelecimento prévio de um canal seguro para distribuição de chaves. Ainda sim, seria possível atender os requisitos de desempenho e eficiência energética impostos pelo ambiente de IoT.

A presença de um eventual atacante que escute passivamente o meio e tente derivar a chave dos participantes legítimos não seria um problema na solução proposta. Isso porque ele não conseguiria obter a coesão de canal se estivesse distante dos nós, resultando em medidas de RSSI diferentes daquelas usadas na geração da chave. Mesmo que o atacante conseguisse localizar um dos nós legítimos e se aproximasse consideravelmente dele (ficando a uma distância menor que meio comprimento de onda), ainda sim teria que conhecer o algoritmo de geração de chaves e seus parâmetros, além de saber exatamente em que pontos começaram e terminaram a troca dos pacotes de controle. As chances desta conjunção de eventos pode ser considerada baixa em ambientes reais, o que viabiliza o uso dos arcabouços nestes cenários.

7.3 Trabalhos Futuros

Como trabalhos futuros, pretende-se realizar uma análise estatística mais aprofundada para explorar a relação entre o tamanho da amostra e a variância do RSSI com os resultados obtidos a partir da suíte de testes do NIST.

Outro trabalho futuro compreende a implementação e o teste de algoritmos de quantização alternativos no RSSignal, buscando melhorar características como a taxa de geração de *bits* e o comprimento da chave gerada.

Também pretende-se validar o arcabouço RSSignal em outra suíte de testes (por exemplo, a Diehard[9]) para obter mais uma fonte de resultados estatisticamente relevantes. Assim, será possível comparar os resultados obtidos por cada um dos conjuntos de dados coletados pelo LoRa RSSI Grabber, já avaliados na suíte de testes do NIST, com o resultado de uma outra suíte, de forma a aprimorar o processo de validação da técnica de geração de chave implementada.

Por fim, vislumbra-se implementar um protocolo completo de acordo de chaves em duas fases: uma primeira fase de geração de chave rápida, para viabilizar o início ágil da comunicação segura na rede a partir de uma quantidade pequena de medidas de RSSI; e uma segunda fase de geração de chave padrão, onde a etapa de coleta pode acumular uma quantidade maior de medidas para aumentar a entropia da chave.

[9] ⟨https://en.wikipedia.org/wiki/Diehard_tests⟩

Bibliografia

AERNOUTS, M.; BERKVENS, R.; VLAENDEREN, K. V.; WEYN, M. Sigfox and lorawan datasets for fingerprint localization in large urban and rural areas. *Data*, MDPI, v. 3, n. 2, p. 13, 2018.

BADAWY, A.; ELFOULY, T.; KHATTAB, T.; MOHAMED, A.; GUIZANI, M. Unleashing the secure potential of the wireless physical layer: Secret key generation methods. *Physical Communication*, Elsevier, v. 19, p. 1–10, 2016.

BASSHAM, L. E.; RUKHIN, A. L.; SOTO, J.; NECHVATAL, J. R.; SMID, M. E.; BARKER, E.; LEIGH, S.; LEVENSON, M.; VANGEL, M.; BANKS, D. et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications.* National Institute of Standards and Technology, 2010. National Institute of Standards and Technology - NIST. Disponível em: ⟨https://doi.org/10.6028/nist.sp.800-22r1a⟩.

BENKIC, K.; MALAJNER, M.; PLANINSIC, P.; CUCEJ, Z. Using RSSI value for distance estimation in wireless sensor networks based on ZigBee. In: IEEE. *15th international conference on systems, signals and image processing*. [S.l.], 2008. p. 303–306.

BOŠNJAK, L.; SREŠ, J.; BRUMEN, B. Brute-force and dictionary attack on hashed real-world passwords. In: *41st International Convention on Information and Communication Technology, Electronics and Microelectronics*. [S.l.: s.n.], 2018. p. 1161–1166.

CALLEBAUT, G.; LEENDERS, G.; BUYLE, C.; CRUL, S.; PERRE, L. Van der. LoRa physical layer evaluation for point-to-point links and coverage measurements in diverse environments. *arXiv preprint arXiv:1909.08300*, 2019.

CODELUPPI, G.; CILFONE, A.; DAVOLI, L.; FERRARI, G. LoRaFarM: A LoRaWAN-Based Smart Farming Modular IoT Architecture. *Sensors*, v. 20, n. 7, 2020.

COMMITTEE, I. C. S. L. S. et al. *IEEE standards 802.15. 4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)*. [S.l.]: New York: IEEE, 2003: 55-139, 2003.

DA CRUZ, P. I.; SUYAMA, R.; LOIOLA, M. B. Increasing key randomness in physical layer key generation based on RSSI in LoRaWAN devices. *Physical Communication*, v. 49, p. 101480, 2021. ISSN 1874-4907.

DE OLIVEIRA, L.; CHAVES, L.; SILVA, E. Rssignal: um arcabouço para evolução de técnicas de geração de chaves baseadas em rssi. In: *Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. Porto Alegre, RS, Brasil: SBC, 2022. p. 111–124. Disponível em: ⟨https://sol.sbc.org.br/index.php/sbseg/article/view/21662⟩.

DEKKERS, P. *LoRa, the Internet of Things*. 2022. Disponível em: ⟨https://communities.surf.nl/artikel/lora-the-internet-of-things⟩.

DWORKIN, M. J. et al. SHA-3 standard: Permutation-based hash and extendable-output functions. 2015. Disponível em: ⟨https://doi.org/10.6028/NIST.FIPS.202⟩.

FERNANDO, M.; JAYALATH, D.; CAMTEPE, S.; FOO, E. Reed Solomon codes for the reconciliation of wireless PHY layer based secret keys. In: *Proceedings of the 86th Vehicular Technology Conference*. [S.l.: s.n.], 2017. p. 1–6.

FINLEY, M. *SNR Calculation*. 2017. 6–7 p. Disponível em: ⟨https://uavrt.nau.edu/wp-content/uploads/2017/06/SNR_Documentation.pdf⟩.

GARLISI, D.; MANGIONE, S.; GIULIANO, F.; CROCE, D.; GARBO, G.; TINNIRELLO, I. Interference cancellation for lora gateways and impact on network capacity. *IEEE Access*, IEEE, v. 9, p. 128133–128146, 2021.

GOLDONI, E.; SAVAZZI, P.; FAVALLI, L.; VIZZIELLO, A. Correlation between weather and signal strength in LoRaWAN networks: An extensive dataset. *Computer Networks*, Elsevier, v. 202, p. 108627, 2022.

HAN, B.; LI, Y.; WANG, X.; LI, H.; HUANG, J. Flora: Sequential fuzzy extractor based physical layer key generation for lpwan. *Future Generation Computer Systems*, 2022. ISSN 0167-739X.

HAN, B.; PENG, S.; WU, C.; WANG, X.; WANG, B. LoRa-based physical layer key generation for secure V2V/V2I communications. *Sensors*, Multidisciplinary Digital Publishing Institute, v. 20, n. 3, p. 682, 2020.

HERSHEY, J.; HASSAN, A.; YARLAGADDA, R. Unconventional cryptographic keying variable management. *IEEE Transactions on Communications*, v. 43, n. 1, p. 3–6, 1995.

HIDAYAT, M.; NUGROHO, A.; SUTIARSO, L.; OKAYASU, T. Development of environmental monitoring systems based on lora with cloud integration for rural area. In: IOP PUBLISHING. *IOP Conference Series: Earth and Environmental Science*. [S.l.], 2019. v. 355, n. 1, p. 012010.

JAYASURIYA, E. N. *ECDH Based Key Management for LoRaWAN Considering Sensor Node Limitations*. Tese (Doutorado) — University of Colombo, 2021. Disponível em: ⟨https://dl.ucsc.cmb.ac.lk/jspui/handle/123456789/4392⟩.

KITAURA, A.; IWAI, H.; SASAOKA, H. A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio. In: *Proceedins of the 9th International Conference on Advanced Communication Technology*. [S.l.: s.n.], 2007. v. 3, p. 1763–1767.

LINKA, H.; RADEMACHER, M.; ALIU, O. G.; JONAS, K. Path loss models for low-power wide-area networks: Experimental results using LoRa. Hochschule Bonn-Rhein-Sieg, 2018.

LIU, L.; YAO, Y.; CAO, Z.; ZHANG, M. DeepLoRa: Learning accurate path loss model for long distance links in LPWAN. In: *INFOCOM*. [S.l.: s.n.], 2021.

MACHINA; GARTNER. *Global Internet of Things market to grow to 27 billion devices, generating USD3 trillion revenue in 2025*. 2016. Disponível em: ⟨https://machinaresearch.com/news/press-release-global-internet-of-things-market-to-grow-to-27-billion-devices-generating-usd3-trillion-revenue-in-2025/⟩.

MARTON, K.; SUCIU, A. On the interpretation of results from the NIST statistical test suite. *Science and Technology*, v. 18, n. 1, p. 18–32, 2015. Disponível em: ⟨https://www.romjist.ro/content/pdf/02-msys.pdf⟩.

NETWORK, T. T. *LoRaWAN Architecture*. 2022. Disponível em: ⟨https://www.thethingsnetwork.org/docs/lorawan/architecture/⟩.

NETWORK, T. T. *LoRaWAN Security*. 2022. Disponível em: ⟨https://www.thethingsnetwork.org/docs/lorawan/security/⟩.

NETWORK, T. T. *What are LoRa and LoRaWAN?* 2022. Disponível em: ⟨https://www.thethingsnetwork.org/docs/lorawan/end-device-activation/⟩.

PASOLINI, G.; BURATTI, C.; FELTRIN, L.; ZABINI, F.; CASTRO, C. D.; VERDONE, R.; ANDRISANO, O. Smart city pilot projects using LoRa and IEEE802.15.4 technologies. *Sensors*, Multidisciplinary Digital Publishing Institute, v. 18, n. 4, p. 1118, 2018.

PRENEEL, B. Cryptographic hash functions: theory and practice. In: *Proceedings of the 11th International Conference on Cryptology in India*. [S.l.: s.n.], 2010. p. 115–117.

SANCHEZ, C.; ARPI, B.; VAZQUEZ-RODAS, A.; ASTUDILLO-SALINAS, F.; MINCHALA, L. I. Performance evaluation of rssi-based positioning system with low-cost lora devices. In: *Proceedings of the 16th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks*. [S.l.: s.n.], 2019. p. 37–44.

SEMTECH. *LoRa® Modulation Basics*. 2. ed. [S.l.], 2015. AN1200.22.

SEMTECH. *Predicting LoRaWAN Capacity*. 2022. Disponível em: ⟨https://lora-developers.semtech.com/documentation/tech-papers-and-guides/predicting-lorawan-capacity⟩.

SEYE, M. R.; NGOM, B.; GUEYE, B.; DIALLO, M. A study of LoRa coverage: range evaluation and channel attenuation model. In: IEEE. *2018 1st International Conference on Smart Cities and Communities (SCCIC)*. [S.l.], 2018. p. 1–4.

SIMKA, M.; POLAK, L. On the RSSI-based indoor localization employing LoRa in the 2.4 GHz ISM band. *Radioengineering*, v. 31, n. 1, p. 135–143, 2022.

SINHA, R. S.; WEI, Y.; HWANG, S.-H. A survey on LPWA technology: LoRa and NB-IoT. *ICT Express*, Elsevier, v. 3, n. 1, p. 14–21, 2017.

STATISTA. *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)*. 2016. Disponível em: ⟨https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/⟩.

TCHÓRZEWSKI, J.; JAKÓBIK, A. Theoretical and experimental analysis of cryptographic hash functions. *Journal of Telecommunications and Information Technology*, Instytut Łączności - Państwowy Instytut Badawczy, v. 1, n. 11, p. 125–133, 2019.

VALACH, A.; MACKO, D. Exploration of the lora technology utilization possibilities in healthcare iot devices. In: IEEE. *2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA)*. [S.l.], 2018. p. 623–628.

WANG, H.; FAPOJUWO, A. O. A Survey of Enabling Technologies of Low Power and Long Range Machine-to-Machine Communications. *IEEE Communications Surveys Tutorials*, v. 19, n. 4, p. 2621–2639, 2017.

YEGIN, A.; SORNIN, N. et al. *LoRaWAN™1.1 Specification*. 2017. Disponível em: ⟨https://lora-aliance.org/resource_hub/lorawan-specification-v1-1/⟩.