Explorando o RSSI na Geração de Chaves para LoRaWAN

Leonardo Azalim de Oliveira[1], **Luciano Jerez Chaves**[1], **Edelberto Franco Silva**[1]

[1] Departamento de Ciência da Computação – Universidade Federal de Juiz de Fora
{leonardo.azalim, luciano.chaves, edelberto}@ice.ufjf.br

Abstract. *Criptography is critical to the security of wireless networks. In the context of LoRa for the Internet of Things, the symmetric key distribution is a challenge. As an alternative, it is possible to generate keys in a distributed manner, based on characteristics of the physical medium, such as the RSSI indicator. This work advances the study of this approach in the context of the RSSignal framework for LoRaWAN networks. The results suggest that, even in scenarios without mobility, the RSSI variance is sufficient for the key generation process. This work also presents the LoRa RSSI Grabber for collecting and storing the RSSI indicator, besides making a new dataset with real measurements publicly available to the community.*

Resumo. *A criptografia é fundamental para a segurança das redes sem fio. No contexto de LoRa para a Internet das Coisas, a distribuição de chaves simétricas é um desafio. Como alternativa, é possível gerar as chaves de maneira distribuída, a partir de características do meio físico, como o indicador RSSI. Este trabalho aprofunda o estudo dessa abordagem no contexto do arcabouço RSSignal para redes LoRaWAN. Os resultados sugerem que, mesmo em cenários sem mobilidade, a variância do RSSI é suficiente para o processo de geração de chaves. De maneira transversal, este trabalho apresenta o LoRa RSSI Grabber para coleta e armazenamento do indicador RSSI, assim como disponibiliza publicamente um novo conjunto de dados com medidas reais para a comunidade.*

1. Introdução

A natureza de um meio não guiado faz com que os sinais sejam transmitidos em *broadcast*, o que significa que todos os dispositivos dentro do raio de alcance do sinal podem capturar uma cópia da informação. Dessa forma, é importante tratar da segurança das comunicações sem fio, principalmente, ao empregar tecnologias como *Long Range* (LoRa) cujo sinal pode atingir longas distâncias. Assim, técnicas de criptografia que cifram os dados transmitidos são regularmente utilizadas, sendo esta questão abordada pelas camadas superiores dos protocolos de comunicação sem fio [Badawy et al. 2016].

Dentre as dificuldades impostas pela criptografia das comunicações sem fio destaca-se a geração e distribuição das chaves criptográficas. Considerando as limitações nos recursos computacionais dos dispositivos que compõem a *Internet of Things* (IoT), a geração distribuída de chaves simétricas com base em características aleatórias inerentes ao canal de comunicação sem fio se apresenta como uma possível solução para este desafio [Ruotsalainen et al. 2020]. Especificamente, a utilização da entropia do indicador *Received Signal Strength Indication* (RSSI) como entrada para algoritmos de geração de chaves tem sido explorada por diversos autores [da Cruz et al. 2021, Han et al. 2023].

Com foco na reprodutibilidade de pesquisas, [de Oliveira et al. 2022] apresentaram o RSSignal: um arcabouço de código aberto para geração e validação de chaves simétricas a partir do indicador RSSI em redes sem fio *Long Range Wide Area Network* (LoRaWAN)[1]. O RSSignal foi inicialmente validado a partir de dois conjuntos de dados de terceiros, sendo um deles público e o outro privado. Entretanto, os ambientes experimentais utilizados para a construção desses conjuntos de dados não exploram exaustivamente as características de mobilidade dos dispositivos, o que dificultou conclusões mais precisas sobre a aplicabilidade da técnica utilizada, principalmente em cenários estáticos.

Neste sentido, o presente trabalho continua a investigar sobre a utilização do indicador RSSI na geração de chaves criptográficas para redes LoRaWAN. Para viabilizar este estudo, primeiramente é apresentado o LoRa RSSI Grabber: um conjunto de *scripts* que automatiza a coleta e o armazenamento do indicador RSSI em conexões LoRa. Com auxílio do LoRa RSSI Grabber, um novo conjunto de dados foi gerado a partir de experimentos reais em ambientes com características diversas dos já estudados. Os dados coletados estão disponíveis publicamente, e foram utilizados como novas entradas para o arcabouço RSSignal. Os resultados obtidos são analisados quantitativamente do ponto de vista de segurança e, quando comparados com os resultados previamente apresentados em [de Oliveira et al. 2022], contrariam as hipóteses anteriores ao mostrar que, para além dos cenários com mobilidade, a técnica empregada no arcabouço RSSignal também pode ser capaz de gerar chaves criptográficas seguras mesmo nos ambientes com ausência de mobilidade dos dispositivos.

Em síntese, este trabalho avança o estado da arte na área de segurança de redes sem fio com as seguintes contribuições tecnológicas e científicas:

1. Apresentação do LoRa RSSI Grabber: uma ferramenta para automatizar a coleta e o armazenamento do indicador RSSI em conexões LoRa;
2. Disponibilização de um conjunto de dados com medidas de RSSI obtidas pelo LoRa RSSI Grabber em ambientes experimentais com características diversas;
3. Discussões sobre os resultados obtidos a partir do arcabouço RSSignal, tendo como entrada o novo conjunto de dados aqui disponibilizado.

As demais seções deste artigo se organizam da seguinte forma: a Seção 2 sumariza os principais trabalhos relacionados ao tema; a Seção 3 apresenta o LoRa RSSI Grabber e o novo conjunto de dados; a Seção 4 discute sobre os resultados obtidos a partir do RSSignal para o novo conjunto de dados; e, por fim, a Seção 5 conclui este trabalho.

2. Trabalhos Relacionados

O conceito de usar características da camada física para geração distribuída de chaves criptográficas foi apresentado inicialmente por [Hershey et al. 1995] e, desde então, tem recebido contribuições significativas em diferentes sistemas e cenários. Especificamente, a utilização do indicador RSSI como entrada para a geração distribuída de chaves simétricas em redes LoRaWAN se mostra uma opção atraente para driblar os desafios da distribuição de chaves entre as partes, já que o indicador RSSI é facilmente obtido nestas redes, apresenta considerável variabilidade e possui alta correlação quando medido nos dois extremos do enlace de comunicação [Badawy et al. 2016, Han et al. 2023].

[1] `https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/`

Conforme discutido por [Ruotsalainen et al. 2020], os métodos de geração de chave baseados em características de camada física são resistentes à computação quântica, desde que não seja possível obter as medidas originais a partir da sequência de *bits* da chave, e que essa tenha um comprimento suficientemente adequado. Além disso, conforme abordado por [Mathur et al. 2008] e por [Xu et al. 2019], a presença de um atacante que passivamente escuta o meio para capturar e medir o RSSI dos pacotes e tentar um ataque de força bruta contra o sistema não representa uma ameaça, visto que a coesão de canal do atacante é baixa quando comparada com as partes legítimas da comunicação.

Em [da Cruz et al. 2021], os autores descrevem um processo em seis etapas para a geração de chaves criptográficas simétricas a partir de medidas de RSSI em redes LoRaWAN. As etapas compreendem: (1) a coleta dos valores de RSSI, realizada através da troca de pacotes entre as partes; (2) o pré-processamento dos dados coletados, removendo eventuais inconsistências; (3) a quantização, responsável por transformar os valores de RSSI em sequências de *bits*; (4) a troca de índices, onde as partes entram em acordo sobre quais medidas serão seletivamente descartadas; (5) a reconciliação de chaves, para corrigir as disparidades nas sequências de *bits* geradas separadamente por cada uma das partes; e (6) a amplificação de privacidade, para garantir a igualdade entre as chaves finais. Os autores descrevem detalhadamente a metodologia adotada e os algoritmos escolhidos para cada etapa do processo. A proposta é avaliada através de experimentos com dados coletados em ambientes reais que envolvem baixa e alta mobilidade do dispositivo LoRa. Para validar as chaves geradas, os autores utilizam a suíte de testes 800-22 do *National Institute of Standards and Technology* (NIST), e confirmam que é possível obter chaves criptograficamente seguras em ambientes em que os nós se movimentam.

Com foco na reprodutibilidade de trabalhos científicos, [de Oliveira et al. 2022] apresentam o RSSignal[2]: um arcabouço de código aberto para geração e validação de chaves criptográficas simétricas a partir do indicador de sinal RSSI em redes LoRaWAN. Para a etapa de geração das chaves, a implementação atual do arcabouço se baseia na técnica proposta por [da Cruz et al. 2021], recebendo como entrada um conjunto de dados com medidas de RSSI previamente coletadas e executando as etapas seguintes do processo. Entretanto, cabe destacar que o arcabouço pode ser instanciado com técnicas de geração alternativas para atender às especificidades de outros tipos de redes. Para a etapa de validação das chaves, o RSSignal submete a sequência de *bits* gerada para a suíte de testes estatísticos NIST 800-22, que analisa o quão estatisticamente aleatória esta é para dizer se ela pode ou não ser considerada suficientemente segura.

Com o objetivo de validar a implementação do arcabouço RSSignal e também a técnica proposta por [da Cruz et al. 2021] para a geração distribuída de chaves simétricas, [de Oliveira et al. 2022] utilizaram dois conjuntos de dados com valores de RSSI coletados em ambientes reais. O primeiro conjunto foi gentilmente cedido por [da Cruz et al. 2021], compreendendo três coletas com medições de RSSI em ambientes com mobilidade. Já o segundo conjunto foi disponibilizado publicamente por [Simka e Polak 2022], compreendendo uma única coleta em um ambiente sem mobilidade. Com base nos experimentos realizados, os autores concluem que o método implementado no arcabouço é capaz de gerar chaves seguras para cenários com mobilidade, corroborando os resultados de [da Cruz et al. 2021]. Entretanto, com base nos resultados

[2]`https://github.com/oliveiraleo/RSSignal-LoRa`

obtidos a partir do conjunto de dados de [Simka e Polak 2022], os autores levantaram a hipótese de que o método não funcionaria para ambientes sem mobilidade, dada a baixa variabilidade do RSSI que implicou num tempo longo para obter uma chave, posteriormente considerada insegura.

O presente trabalho tem por objetivo investigar com mais detalhes a aplicabilidade do método de geração de chave adotado no RSSignal em ambientes estáticos. Para que isso seja possível, é necessário avaliar novos conjuntos de dados no arcabouço. Entretanto, um dos requisitos para a escolha destes conjuntos de dados é a de que as medidas de RSSI sejam coletadas de maneira sequencial e simultânea em ambos os lados da conexão LoRa (dispositivo e *gateway*), de modo a explorar a coesão do canal. Exceto por aqueles disponibilizados em [Simka e Polak 2022], não foram encontrados em domínio público outros conjuntos de dados com esta característica. Dessa forma, fez-se necessário criar um novo conjunto de dados, sendo o LoRa RSSI Grabber um facilitador para esta tarefa, conforme descrito na Seção 3. Este novo conjunto de dados foi então usado como entrada para o RSSignal, e os resultados obtidos são discutidos na Seção 4.

A Tabela 1 resume as características dos trabalhos relacionados. A coluna *arcabouço de geração de chaves* destaca os trabalhos que apresentam mecanismos para gerar chaves a partir do RSSI. As colunas de *acesso aberto* indicam se o código fonte ou o conjunto de dados utilizados estão disponíveis publicamente. Por fim, as colunas do *ambiente de testes LoRa* descrevem as características do ambientes avaliados, como a utilização de comunicação entre dispositivo e *gateway* (em contraste com cenários *ad-hoc*); a presença (LOS) ou ausência (NLOS) de visada direta entre o transmissor e o receptor; e o tipo de movimentação dos dispositivos (E: estática, L: lenta e R: rápida).

Tabela 1. Comparativo das principais características dos trabalhos relacionados.

		Acesso Aberto		**Ambiente de Testes LoRa**			
Autores / Trabalhos	**Arcabouço de Geração de Chaves**	**Código Fonte**	**Conjunto de Dados**	**Utiliza *Gateway***	**LOS**	**NLOS**	**Movimentação Dispositivo**
[Hershey et al. 1995]							
[Badawy et al. 2016]	✓				✓		Não informado
[Ruotsalainen et al. 2020]	✓			✓	✓	✓	E
[Han et al. 2023]	✓	✓*		✓	✓		E / L
[Mathur et al. 2008]	✓	✓*					
[Xu et al. 2019]	✓			✓			E / L
[da Cruz et al. 2021]	✓			✓		✓	L / R
[de Oliveira et al. 2022]	✓	✓					
[Simka e Polak 2022]			✓		✓		E
Este trabalho		✓	✓	✓	✓	✓	E / L / R

* Somente pseudocódigo

3. Conjunto de Dados com Medidas de RSSI

Conjuntos de dados com medidas de RSSI possuem diversas aplicações, servindo de base, por exemplo, para o planejamento da instalação de redes de sensores, a construção de *heatmaps* para análise da cobertura de sinal, ou mesmo para alimentar arcabouços que utilizam essas medidas como entrada. Na Subseção 3.1 é apresentada a ferramenta LoRa RSSI Grabber, bem como o ambiente utilizado na coleta de dados. Na Subseção 3.2 é descrito o novo conjunto de dados com medidas reais disponibilizado publicamente.

3.1. O LoRa RSSI Grabber e o Ambiente de Coleta

A ferramenta LoRa RSSI Grabber permite coletar medidas de RSSI em ambos os lados de uma conexão LoRa (dispositivo e *gateway*), acompanhadas dos dados de geolocalização do dispositivo. A implementação de uma ferramenta como essa varia de acordo com o protocolo de comunicação e o modelo dos equipamentos. O código fonte, disponível publicamente no GitHub[3], suporta atualmente o dispositivo LoRa Multitech mDot.

A arquitetura do LoRa RSSI Grabber está retratada na Figura 1, que compreende também o ambiente de coleta utilizado neste trabalho. O computador, que é o responsável por executar os *scripts* da ferramenta, está conectado através de cabos *Universal Serial Bus* (USB) com um celular e com a placa programadora do dispositivo LoRa e através de uma conexão de rede (cujo primeiro salto é via Wi-Fi) aos servidores da *The Things Network* (TTN) na Internet. Com auxílio do módulo *Android Debug Bridge* (ADB), o computador configura o celular para capturar o sinal *Global Positioning System* (GPS), calcular as coordenadas de geolocalização do dispositivo e enviá-las de volta ao computador. Por sua vez, a conexão entre o computador e o dispositivo LoRa é intermediada pela placa programadora, responsável também por fornecer energia ao dispositivo. O computador configura o dispositivo LoRa para enviar pacotes de controle periódicos ao *gateway* (*uplink*), que serão individualmente confirmados (*downlink*), viabilizando a coleta das medidas de RSSI em ambos os lados da conexão LoRa (destacada em amarelo na figura). Do lado do *gateway* LoRaWAN, existe uma antena gerenciada por um controlador de baixo custo que executa um sistema operacional Linux. Este controlador também está conectado, via rede cabeada, aos servidores da TTN na Internet. É através desta conexão que os valores de RSSI medidos no *gateway* são disponibilizados ao LoRa RSSI Grabber. Os dados coletados no *gateway* são enviados ao servidor de aplicação sendo, posteriormente, acessados pelo computador através de uma *Application Programming Interface* (API) que utiliza o protocolo *Message Queue Telemetry Transport* (MQTT).

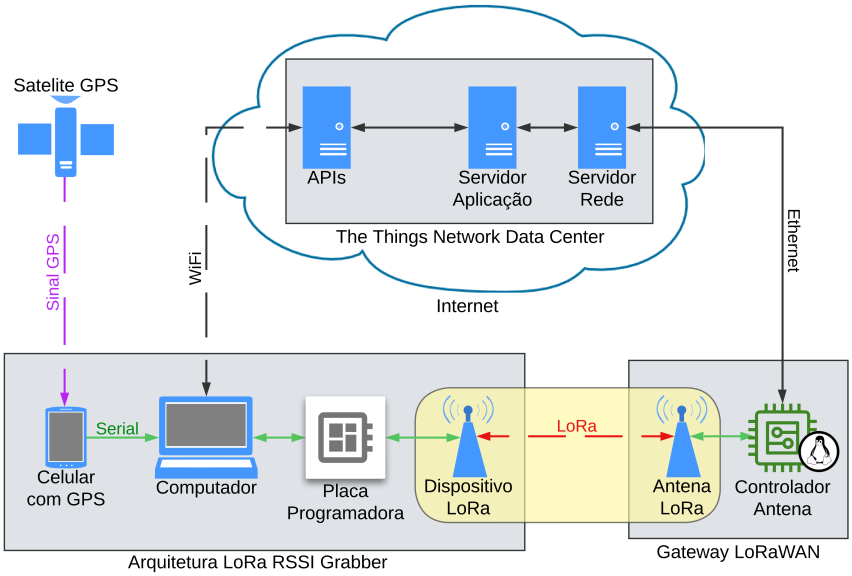


Figura 1. Arquitetura do LoRa RSSI Grabber e o ambiente de coleta.

[3]https://github.com/oliveiraleo/LoRa-RSSI-Grabber

A Figura 2 ilustra o fluxo de execução dos *scripts* que compõem a ferramenta LoRa RSSI Grabber. Para atender aos requisitos do paradigma *publish-subscribe* utilizado pelo protocolo MQTT, o *script* `get-mqtt-data.sh` deve ser executado primeiro, ficando responsável pela conexão com a API da TTN para recuperar em tempo real os pacotes recebidos pelo *gateway*. Na sequência, o *script* `send_control_packets.py` instruirá o dispositivo LoRa a enviar os pacotes de controle periodicamente ao *gateway*. Cada novo pacote enviado é identificado por um número sequencial único, sendo este identificador recuperado pelo *gateway* e armazenado junto ao valor de RSSI aferido. Ao obter a confirmação de recebimento do pacote enviado ao *gateway*, o dispositivo armazena o valor do RSSI aferido no momento do recebimento da confirmação. Após a conclusão desta etapa, o *script* `process_api_data.py` processa os pacotes recebidos para extrair os identificadores e os valores de RSSI. Por fim, o *script* `join_GW_ED_data.py` concatena os resultados locais com aqueles coletados no *gateway*, sincronizando os valores de RSSI a partir dos identificadores dos pacotes para então gerar o arquivo final da coleta que será salvo localmente.

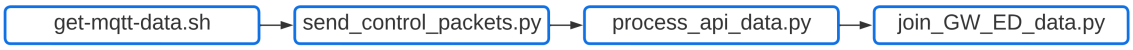


Figura 2. Fluxo de execução dos scripts do LoRa RSSI Grabber.

A Tabela 2 exemplifica o formato do arquivo final com os seguintes campos sendo armazenados: *Time* (horário local do computador); *GPS Time* (horário UTC reportado pelos satélites GPS); *ID* (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* (precisão do sinal de GPS – quanto menor, melhor); *# Satellites* (quantidade de satélites que estão na vista do aparelho); *ED RSSI* (medida do RSSI no dispositivo LoRa); e *GW RSSI* (medida do RSSI no *gateway* LoRa).

Tabela 2. 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
18:40:45	21:40:37	5	−21.77802725	−43.37142227	905.6	1	14	−114	−111
18:40:53	21:40:45	6	−21.77780865	−43.37138255	905.6	1	14	−113	−109
18:41:01	21:40:53	7	−21.77749243	−43.37134171	902.3	1	14	−120	−120
18:41:09	21:41:01	8	−21.77710902	−43.37141932	898.2	1	14	−119	−119
18:41:17	21:41:09	9	−21.77670287	−43.37149252	891.1	1	14	−127	−119

3.2. Um Novo Conjunto de Dados

Neste trabalho, o LoRa RSSI Grabber foi utilizado para criar um novo conjunto de dados com medidas reais de RSSI. Este novo conjunto, que compreende cinco coletas distintas, está publicamente disponível através de um repositório no GitHub[4].

O ambiente utilizado na criação deste conjunto de dados compreende um dispositivo LoRa Multitech mDot conectado a um *gateway* que é controlado por um Raspberry Pi e possui uma antena externa instalada no topo do prédio da Faculdade de Engenharia da Universidade Federal de Juiz de Fora (UFJF) ($\approx$ 932 m de altitude em relação ao

[4] `https://github.com/oliveiraleo/LoRa-RSSI-dataset-outdoor`

nível do mar). Tanto o *gateway* quanto o dispositivo LoRa foram configurados para operar na faixa de frequência de 915 MHz. O mDot foi configurado para utilizar sempre o *Spreading Factor* (SF) 12 com a *Bandwidth* (BW) de 125 KHz. Conforme discutido por [Ruotsalainen et al. 2020], desativar a adaptação automática destes parâmetros é necessário para não impactar nas medições de RSSI.

A Tabela 3 descreve as principais características de cada coleta: o total de medidas de RSSI obtidas; os valores mínimo, médio e máximo de RSSI observados durante a coleta; o desvio padrão das medidas coletadas; o tipo de movimentação do dispositivo em relação ao *gateway*; a velocidade média de deslocamento do dispositivo durante a coleta; a distância em linha reta entre o local onde a medição foi feita e o local onde a antena do *gateway* está instalada (para coletas com mobilidade são apresentados a menor e a maior distância); a elevação do dispositivo em relação ao nível do mar; a existência de visada limpa e direta entre o dispositivo e a antena do *gateway*; as médias de temperatura e pressão atmosférica durante as coletas; e as variações no volume de chuva e na velocidade do vento no ambiente (medida inicial $\rightarrow$ medida final). Todas as coletas tiveram duração de 70 minutos, com troca de pacotes de controle a cada 8 segundos.

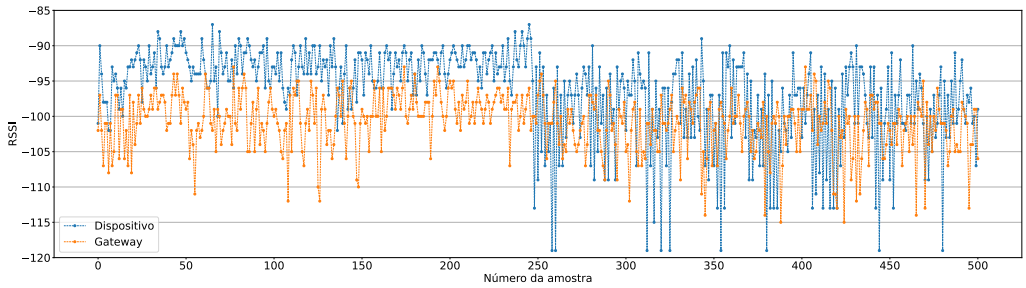
Tabela 3. Características das coletas do conjunto de dados deste trabalho,

Características	**Coleta 1**	**Coleta 2**	**Coleta 3**	**Coleta 4**	**Coleta 5**
Quantidade de Medidas	501	508	496	511	498
RSSI Mínimo (dBm)	-119	-132	-101	-132	-133
RSSI Médio (dBm)	-99	-119	-75	-105	-118
RSSI Máximo (dBm)	-87	-100	-59	-65	-76
RSSI Desvio Padrão	5,773	3,291	6,377	13,443	8,829
Movimentação Dispositivo	Estática	Estática	Estática	Lenta	Rápida
Velocidade Média (Km/h)	0,0	0,0	0,0	5,5	24,0
Distância da Antena (m)	325	365	12	$[30, 1060]$	$[35, 2410]$
Elevação (m)	932	905	930	$[868, 946]$	$[835, 958]$
Visada Direta	Sim	Não	Sim	Não	Não
Temperatura Média ($^{\circ}C$)	24,6	23,3	24,7	21,8	19,3
Pressão Atmosférica (hPa)	900,9	904,6	902,9	907,6	909,1
Umidade Relativa do Ar ($\%$)	65,8	71,5	69,5	74,5	90,3
Volume de Chuva (mm)	$0{,}0 \rightarrow 0{,}0$	$0{,}0 \rightarrow 0{,}0$	$3{,}6 \rightarrow 0{,}4$	$0{,}0 \rightarrow 0{,}0$	$0{,}4 \rightarrow 0{,}8 \rightarrow 2{,}8$
Velocidade do Vento (m/s)	$4{,}9 \rightarrow 5{,}0$	$2{,}7 \rightarrow 3{,}0$	$5{,}5 \rightarrow 1{,}6$	$7{,}4 \rightarrow 5{,}6$	$3{,}8 \rightarrow 7{,}4 \rightarrow 6{,}2$

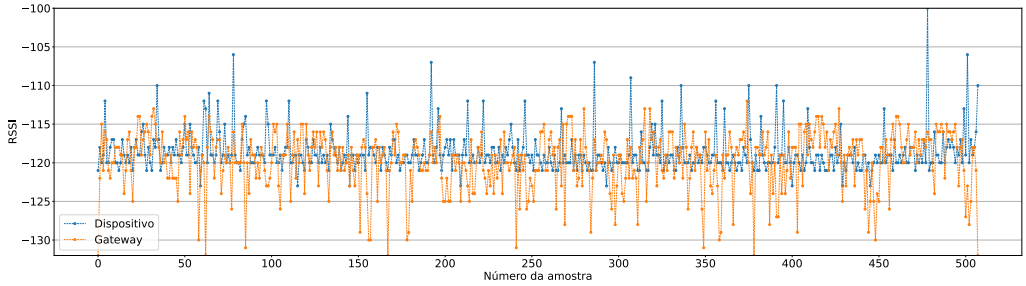
Os dados sobre o clima apresentados foram obtidos da estação meteorológica instalada no *campus*, através do site do Instituto Nacional de Meteorologia (INMET)[5]. Conforme discutido por [Goldoni et al. 2022], existe relação entre os valores de RSSI medidos e as características meteorológicas do ambiente de testes. Logo, disponibilizar estas informações juntamente com os dados de RSSI pode ser útil para trabalhos desta natureza.

A Figura 3 mostra as medidas de RSSI para as cinco coletas do novo conjunto de dados. Em todos os gráficos existem sempre duas linhas, indicando os valores de RSSI medidos no dispositivo e também no *gateway*. Conforme esperado, a distância entre o dispositivo e o *gateway* tem influência significativa no valor absoluto do RSSI. Além disso, o padrão de mobilidade do dispositivo afetou a variabilidade dos valores coletados.

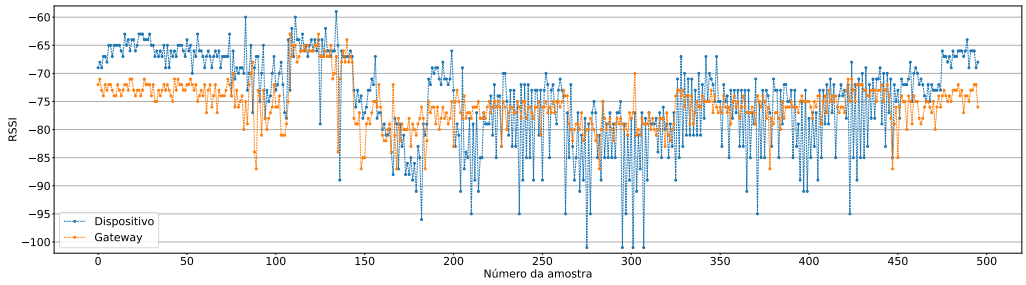
[5]`https://tempo.inmet.gov.br/TabelaEstacoes/A518`



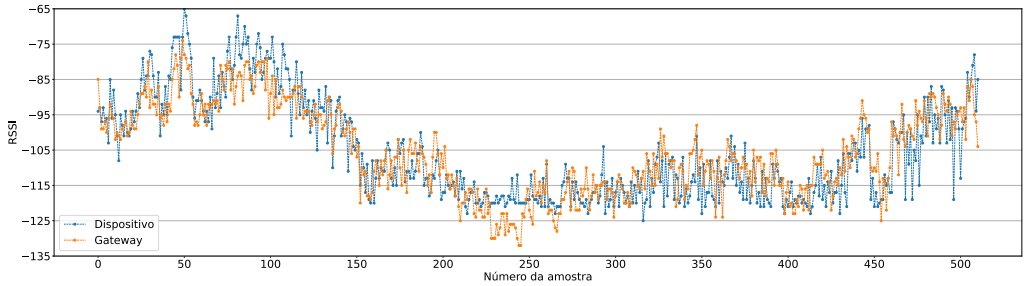
(a) Coleta 1



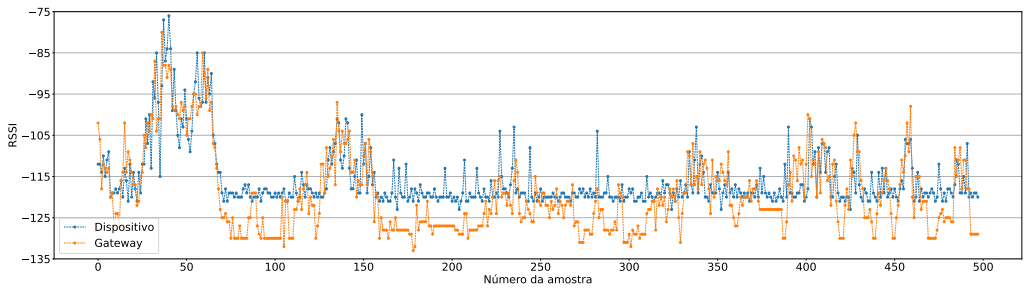
(b) Coleta 2



(c) Coleta 3



(d) Coleta 4



(e) Coleta 5

Figura 3. Medidas de RSSI das coletas do conjunto de dados deste trabalho (atenção para os diferentes intervalos de RSSI no eixo Y dos gráficos).

4. Geração e Validação de Chaves no RSSignal

Para explorar o uso do indicador RSSI na geração distribuída de chaves criptográficas simétricas em redes LoRaWAN, o novo conjunto de dados foi utilizado como entrada para o arcabouço RSSignal. A Subseção 4.1 resume o funcionamento do RSSignal enquanto a Subseção 4.2 apresenta e discute os resultados obtidos.

4.1. O Arcabouço RSSignal

Conforme detalhado em [de Oliveira et al. 2022], o RSSignal é um arcabouço de código aberto para a geração distribuída e validação de chaves criptográficas simétricas a partir do indicador de intensidade do sinal RSSI. A implementação do arcabouço é baseada no método para a geração de chaves proposto por [da Cruz et al. 2021], seguido da validação das chaves geradas através da suíte de testes estatísticos 800-22 do NIST.

Na proposta de [da Cruz et al. 2021], o processo de geração das chaves acontece em 6 etapas. A primeira etapa (coleta de dados) consiste na troca de pacotes para aferição simultânea do RSSI nos dois extremos de uma conexão LoRa. No RSSignal, esta etapa é substituída pela entrada de medidas de RSSI previamente coletadas, sendo o LoRa RSSI Grabber visto como uma prova de conceito para essa etapa inicial. Na segunda etapa (pré-processamento dos dados), o RSSignal implementa filtros com expressões regulares para extrair apenas os valores numéricos válidos para as medidas de RSSI, desconsiderando outras informações ou mesmo dados inválidos. A terceira etapa (quantização) é a responsável por transformar os valores de RSSI em sequências de *bits*. A implementação do RSSignal suporta a quantização baseada na média e no desvio padrão. Primeiro, faz-se a diferenciação $D_l = X_l - X_{l+M}$ entre medidas de RSSI que estão distantes M posições umas das outras, de modo a diminuir a correlação entre valores consecutivos. Posteriormente, a média μ_D e o desvio padrão σ_D são calculados. Por fim, valores D_l acima do intervalo $\mu_D \pm \alpha\,\sigma_D$ são convertidos em *bit* 1, enquanto valores abaixo deste intervalo são convertidos em *bit* 0. Valores D_l dentro do intervalo são marcados para descarte, de modo a evitar o uso de medidas agrupadas à média e favorecer a randomização da chave gerada. A quarta etapa (troca de índices) permite que as partes compartilhem os índices das medidas de RSSI que serão descartadas, conforme marcação da etapa anterior. Já na quinta etapa (reconciliação das chaves), o RSSignal utiliza um codificador *Reed-Solomon* para diminuir a disparidade entre os *bits* nas sequências geradas de maneira independente no dispositivo e no *gateway*. Por fim, a sexta etapa (amplificação de privacidade) utiliza o algoritmo de *hash* SHA3-512 para garantir a igualdade entre as sequências de *bits*, de modo que elas possam ser usadas como chaves simétricas de criptografia.

Para a validação das chaves, a suíte de testes 800-22 do NIST recebe como entrada a sequência de *bits* gerada após a reconciliação das chaves, executa uma série de testes estatísticos e retorna o chamado *p-valor* para cada um delas. Se *p-valor* $\geq 0{,}01$, o teste é considerado como aprovado [Bassham et al. 2010]. Segundo [Marton e Suciu 2015], se uma sequência consegue ser aprovada em pelo menos 7 dos 15 testes disponíveis, então ela pode ser considerada suficientemente randômica (o que, para os propósitos deste trabalho, significa que ela é segura para ser utilizada como uma chave criptográfica). Para esta fase, foram cuidadosamente selecionados os mesmos 8 testes realizados por [da Cruz et al. 2021], adicionando-se o teste de entropia e o cálculo do comprimento da entrada. Este último foi incluído como um fator determinante para aprovação ou não de uma sequência de *bits*, devendo essa ter pelo menos 100 *bits* [Bassham et al. 2010].

4.2. Resultados e Discussões

O conjunto de dados descrito na Seção 3 foi utilizado como entrada para o RSSignal, considerando diferentes configurações dos parâmetros M e α para a etapa de quantização. As tabelas com os *p-valores* obtidos para todos os testes estão disponíveis no repositório do RSSignal no GitHub[6]. Para auxiliar as discussões, os resultados foram compilados nas Tabelas de 4 a 8, que destacam com ✓ as configurações em que a chave foi aprovada. As demais configurações foram reprovadas, sendo destacadas com * apenas as reprovadas em decorrência do comprimento reduzido da chave (sequência inferior a 100 *bits*).

Existe uma relação direta de α com o tamanho da chave, pois quanto maior o valor de α, maior o intervalo de descarte definido na etapa de quantização. Logo, se o intervalo é maior, a quantidade de *bits* que são descartados aumenta e a chave final ficará mais curta, tornando mais difícil que esta seja suficientemente segura. Por outro lado, $\alpha = 0$ elimina o descarte de valores, resultando em muitas sequências de 0s ou 1s na chave,

Tabela 4. Resultados da coleta 1.

M / α	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
1			✓	✓	✓			*	*	*	*
2	✓	✓	✓	✓			✓	✓	*	*	*
3			✓	✓	✓	✓	✓	✓	*	*	*
4		✓	✓	✓	✓	✓	✓	*	*	*	*

Tabela 5. Resultados da coleta 2.

M / α	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
1				✓	✓		*	*	*	*	*
2			✓	✓			*	*	*	*	*
3		✓	✓	✓	✓	✓	*	*	*	*	*
4		✓	✓	✓	✓	✓	*	*	*	*	*

Tabela 6. Resultados da coleta 3.

M / α	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
1					✓			*	*	*	*
2	✓	✓	✓	✓	✓	✓	*	*	*	*	*
3			✓	✓	✓	✓	*	*	*	*	*
4		✓	✓	✓	✓	*	*	*	*	*	*

Tabela 7. Resultados da coleta 4.

M / α	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
1					✓	✓	✓		*	*	*
2	✓	✓	✓	✓	✓	✓	✓	✓	*	*	*
3		✓	✓	✓	✓	✓	✓	✓	*	*	*
4		✓	✓	✓		✓	✓	✓	*	*	*

[6] https://github.com/oliveiraleo/RSSignal-LoRa/tree/main/results/key-evaluation

Tabela 8. Resultados da coleta 5.

M / α	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
1		✓	✓	✓	✓	✓	*	*	*	*	*
2		✓	✓	✓	✓	✓	*	*	*	*	*
3		✓	✓	✓	✓	✓	*	*	*	*	*
4		✓	✓	✓	✓	✓	✓	*	*	*	*

Tabela 9. Resultados da coleta 1 do conjunto de [Simka e Polak 2022].

M / α	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
1		*	*	*	*	*	*	*	*	*	*
2		*	*	*	*	*	*	*	*	*	*
3		*	*	*	*	*	*	*	*	*	*
4		*	*	*	*	*	*	*	*	*	*

o que diminui a aleatoriedade da mesma e aumenta a taxa de reprovação. Com relação ao parâmetro M, observa-se um pequeno aumento nas aprovações para valores maiores deste parâmetro. Esse comportamento se explica pela menor correlação entre as medidas usadas na diferenciação quando M é maior.

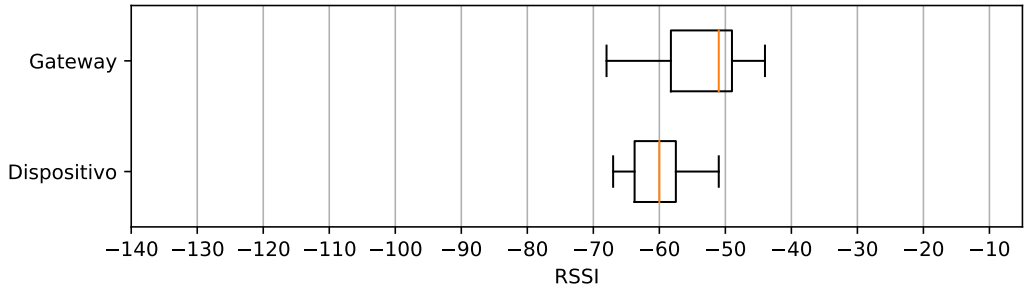
Com base nos experimentos desse trabalho em que há movimentação do dispositivo, supondo o melhor caso de um cenário controlado, isto é, sem perda de pacotes de controle, desconsiderando os eventuais descartes de medidas que podem ocorrer e sem restrições de *duty cycle* na rede LoRaWAN, é possível gerar uma chave de 128 bits de comprimento em 1024 segundos (≈18 min), logo, a uma taxa igual a 7,5 bits/min.

O trabalho de [da Cruz et al. 2021] havia confirmado a eficácia do método de geração de chaves para ambientes com mobilidade dos dispositivos. Os testes realizados por [de Oliveira et al. 2022], assim como os testes das coletas 4 e 5 do conjunto de dados deste trabalho (Tabelas 7 e 8, respectivamente), corroboram esta afirmação. Por outro lado, em [da Cruz et al. 2021] levantou-se a hipótese de que o método não seria propício para ambientes sem mobilidade, dado a baixa variabilidade entre as medidas de RSSI, o que resultaria num longo tempo de coleta que produziria chaves pequenas e pouco seguras. Um problema semelhante a este já havia sido levantado por [Ruotsalainen et al. 2020], que propuseram o uso de antenas ESPAR para causar variações no padrão de propagação do sinal e viabilizar a geração de chaves em cenários estáticos.

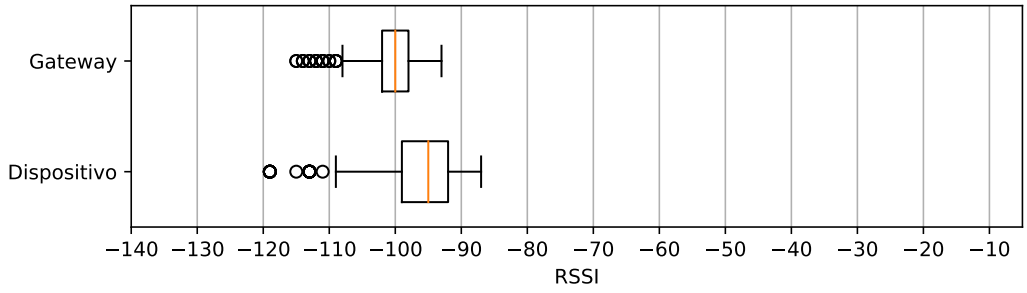
O trabalho [de Oliveira et al. 2022] introduziu os primeiros testes de geração de chaves a partir de medidas de RSSI coletadas em um ambiente estático (utilizando o conjunto de dados disponibilizado por [Simka e Polak 2022]) no RSSignal. A Tabela 9 compila os resultados apresentados naquele trabalho, confirmando a reprovação das chaves geradas em todas as configurações avaliadas. Entretanto, os resultados obtidos para as coletas 1, 2 e 3 do conjunto de dados deste trabalho (Tabelas 4, 5 e 6, respectivamente), onde não há mobilidade do dispositivo, contrariam o que foi afirmado até então.

Para auxiliar no entendimento deste comportamento, a Figura 4 apresenta a variabilidade estatística das medidas de RSSI das coletas estáticas dos conjuntos de dados de [Simka e Polak 2022] e deste trabalho. Ao comparar os gráficos da Figura 4, é possível

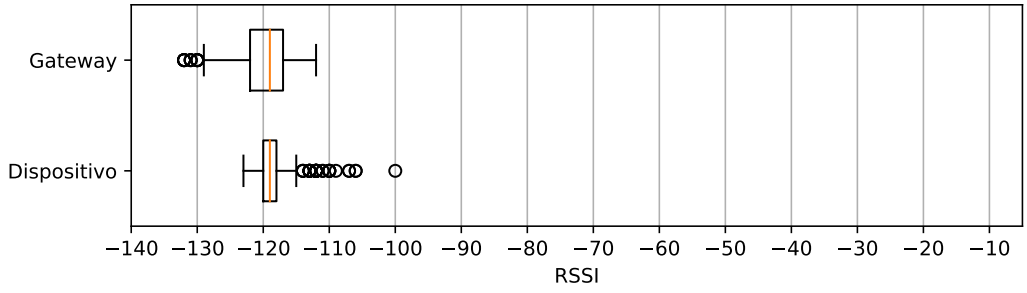
notar que, em todos os casos, as medidas de RSSI estão concentradas próximas à mediana (linha vermelha). Entretanto, as medidas das coletas do conjunto deste trabalho contém um número considerável de *outliers* (círculos pretos). Esse comportamento pode ajudar a explicar os resultados obtidos neste trabalho.



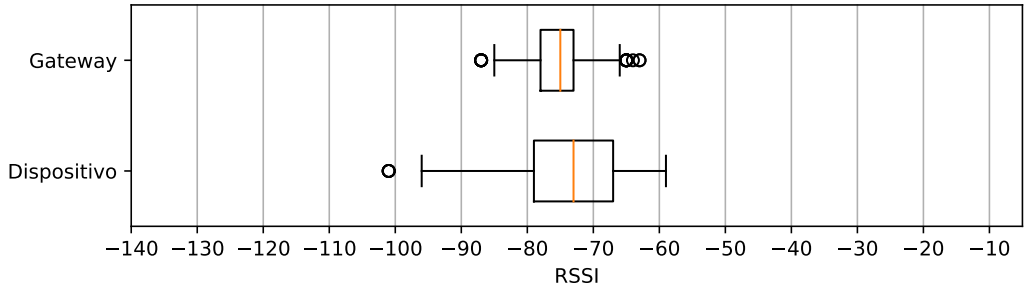
(a) Coleta 1 do conjunto de [Simka e Polak 2022]



(b) Coleta 1 do conjunto



(c) Coleta 2 do conjunto



(d) Coleta 3 do conjunto

Figura 4. Variabilidade das medidas de RSSI em ambientes estáticos.

Ao analisar as Tabelas de 3 a 9, os gráficos da Figura 4 e as discussões disponíveis em alguns trabalhos da literatura, é possível criar hipóteses que ajudem a explicar os resultados obtidos. A primeira delas está relacionada ao ambiente experimental. Diferente do trabalho de [Simka e Polak 2022], o ambiente das três coletas estáticas do presente trabalho era aberto, com a presença de movimentação de veículos, pessoas e massas de ar. Os trabalhos de [Goldoni et al. 2022] e [Ruotsalainen et al. 2020] já haviam evidenciado uma possível correlação entre essas características ambientais e uma maior variabilidade das medidas do indicador RSSI.

Outro ponto que merece destaque é que, como visto em [Ruotsalainen et al. 2020], o SF escolhido e o *payload* dos pacotes de controle influenciam na variabilidade das medidas. No contexto de LoRa, um SF $\geq$ 10 e *payloads* arbitrários tendem a aumentar essa variabilidade. Em [Goldoni et al. 2022], o SF escolhido foi o 7, já nos trabalhos de [Simka e Polak 2022] e neste, foi utilizado o SF 12. Ao longo das coletas, por conta do próprio algoritmo de comunicação LoRa e por conta de um contador ordinal que foi introduzido para este trabalho, o *payload* dos pacotes de controle era arbitrário e variável.

Considerando as discussões apresentadas por [Ruotsalainen et al. 2020], os resultados obtidos neste trabalho, e também a investigação dos resultados de [Goldoni et al. 2022], [Han et al. 2020] e [Han et al. 2023], foi possível observar que não é obrigatório movimentar ou customizar o formato da antena do dispositivo para alcançar variabilidade nas medidas de RSSI em coletas estáticas.

5. Conclusão

Este trabalho apresenta o LoRa RSSI Grabber: uma ferramenta para coleta de medidas de RSSI em dispositivos LoRa mDot. Esta ferramenta funciona como uma prova de conceito para a primeira etapa do arcabouço RSSignal, o que permitiu a criação de um conjunto de dados abertos com medidas de RSSI de uma rede LoRaWAN real. Este novo conjunto foi utilizado como entrada no arcabouço RSSignal para geração de chaves, que foram posteriormente validadas em uma instância da suíte de testes do NIST 800-22. Os resultados evidenciam que, para além dos cenários com alta mobilidade e alta variância de RSSI, o RSSignal pode ser capaz de fazer a geração de chaves criptográficas seguras mesmo nos cenários com ausência de mobilidade e menor variância de RSSI, sem necessidade de alterações físicas nos dispositivos já disponíveis no mercado. O LoRa RSSI Grabber, o conjunto de dados e os resultados obtidos neste trabalho estão disponíveis publicamente.

Como trabalhos futuros, pretende-se avaliar o comportamento do RSSignal sob outras configurações de SF e BW. Além disso, a partir do arcabouço e do LoRa RSSI Grabber, há a intenção de criar um protocolo completo de geração e atualização de chaves simétricas para redes LoRaWAN. Por fim, é interessante investigar formas para aumentar a taxa de geração de *bits* do método implementado no arcabouço, principalmente considerando o contexto onde há presença de regulações de *duty cycle* dos dispositivos LoRa. Dentre as alternativas, é possível considerar as seguintes estratégias: (1) utilizar uma chave pré-carregada no dispositivo que será atualizada posteriormente; (2) utilizar uma chave mais curta (menos segura) para acelerar o processo inicial e depois utilizar o protocolo para atualizar essa chave; ou (3) implementar outro algoritmo de quantização no arcabouço de forma que seja possível realizar uma extração *multi-bit*, assim como mostrado em [Han et al. 2023].

Agradecimentos

Os autores gostariam de agradecer ao Sr. Rogério Casagrande, ao Sr. Thiago Scher, e ao Professor Álvaro de Medeiros, membros do Laboratório de Telecomunicações Aplicadas (LTA) da Universidade Federal de Juiz de Fora (UFJF) pelo apoio na montagem do ambiente e pelo empréstimo dos equipamentos. Os autores também agradecem à UFJF, CAPES, FAPEMIG (APQ-00999-18) e FAPESP (2018/23062-5) pelo apoio financeiro.

Referências

Badawy, A., Elfouly, T., Khattab, T., Mohamed, A., e Guizani, M. (2016). Unleashing the secure potential of the wireless physical layer: secret key generation methods. *Physical Communication*, 19:1–10.

Bassham, L., Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., et al. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology - NIST.

da Cruz, P., Suyama, R., e Loiola, M. (2021). Increasing key randomness in physical layer key generation based on RSSI in LoRaWAN devices. *Physical Communication*, 49:101480.

de Oliveira, L., Chaves, L., e Silva, E. (2022). RSSignal: um arcabouço para evolução de técnicas de geração de chaves baseadas em RSSI. Em *Anais do XXII SBSeg*, páginas 111–124, Porto Alegre, RS, Brasil. SBC.

Goldoni, E., Savazzi, P., Favalli, L., e Vizziello, A. (2022). Correlation between weather and signal strength in LoRaWAN networks: An extensive dataset. *Computer Networks*, 202:108627.

Han, B., Li, Y., Wang, X., Li, H., e Huang, J. (2023). FLoRa: Sequential fuzzy extractor based physical layer key generation for LPWAN. *Future Generation Computer Systems*, 140:253–265.

Han, B., Peng, S., Wu, C., Wang, X., e Wang, B. (2020). LoRa-based physical layer key generation for secure V2V/V2I communications. *Sensors*, 20(3):682.

Hershey, J., Hassan, A., e Yarlagadda, R. (1995). Unconventional cryptographic keying variable management. *IEEE Transactions on Communications*, 43(1):3–6.

Marton, K. e Suciu, A. (2015). On the interpretation of results from the NIST statistical test suite. *Science and Technology*, 18(1):18–32.

Mathur, S., Trappe, W., Mandayam, N., Ye, C., e Reznik, A. (2008). Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. Em *Proc. of the 14th MobiCom*, páginas 128–139, USA. ACM.

Ruotsalainen, H., Zhang, J., e Grebeniuk, S. (2020). Experimental investigation on wireless key generation for Low-Power Wide-Area Networks. *IEEE Internet of Things Journal*, 7(3):1745–1755.

Simka, M. e Polak, L. (2022). On the RSSI-based indoor localization employing LoRa in the 2.4 GHz ISM band. *Radioengineering*, 31(1):135–143.

Xu, W., Jha, S., e Hu, W. (2019). LoRa-Key: Secure key generation system for LoRa-based network. *IEEE Internet of Things Journal*, 6(4):6404–6416.