



Pedido nacional de Invenção, Modelo de Utilidade, Certificado de Adição de Invenção e entrada na fase nacional do PCT

Número do Processo: BR 10 2024 002578 4

Dados do Depositante (71)

Depositante 1 de 2

Nome ou Razão Social: UNIVERSIDADE FEDERAL DE MINAS GERAIS

Tipo de Pessoa: Pessoa Jurídica

CPF/CNPJ: 17217985000104

Nacionalidade: Brasileira

Qualificação Jurídica: Instituição de Ensino e Pesquisa

Endereço: Av. Antônio Carlos, 6627 - Unidade Administrativa II - 2º andar- sala 2011

Cidade: Belo Horizonte

Estado: MG

CEP: 31270-901

País: Brasil

Telefone: (31) 3409-6430

Fax:

Email: patentes@ctit.ufmg.br

Depositante 2 de 2

Nome ou Razão Social: COMPANHIA DE SANEAMENTO DE MINAS GERAIS - COPASA
MG

Tipo de Pessoa: Pessoa Jurídica

CPF/CNPJ: 17281106000103

Nacionalidade: Brasileira

Qualificação Jurídica: Pessoa Jurídica

Endereço: Rua Mar de Espanha, 525 - Santo Antônio

Cidade: Belo Horizonte

Estado: MG

CEP:

País: BRASIL

Telefone: (31) 325 01140

Fax:

Email: usdt@copasa.com.br

Natureza Patente: 10 - Patente de Invenção (PI)

Título da Invenção ou Modelo de Utilidade (54): PROCESSOS DE COMUNICAÇÃO EM REDE DE TRANSCÉPTORES DE RÁDIO COM REDUÇÃO DE VULNERABILIDADES.

Resumo: Propõe-se um processo de comunicação entre transceptores de rádio controlados por plataformas de prototipação eletrônicas (PPE) baseadas em microcontroladores (PPE-MC) ou baseadas em computadores de placa única (PPE-CPU). Os transceptores são preferencialmente de modulação Chirp spread spectrum (CSS) (Ex.: LoRa: Long Range), operados num modelo de controle de comunicação assimétrico do tipo mestre e escravo com polling cíclico e tempo de serviço limitado para evitar colisões de mensagens. O transceptor mestre funciona como um hub de comunicação que controla e determina o envio de dados pelos transceptores escravos da rede de comunicação para o mestre (gateway). A tecnologia inclui uma camada de segurança para redução de vulnerabilidades e mitigação de riscos que utiliza um identificador unívoco (UID) de cada transceptor no processo de autenticação e verificação de integridade. A tecnologia propicia que a informação transmitida na rede de comunicação seja protegida por criptografia, por exemplo no padrão advanced encryption standard (AES). Utilizam-se também funcionalidades de segurança como software (firmware) de inicialização seguro ou secure boot (SB), criptografia do conteúdo da memória flash ou flash encryption (FE) e comunicação segura com protocolo Transport Layer Security (TLS). A tecnologia proposta se aplica em redes de comunicação, especialmente no contexto de Internet das Coisas (IoT).

Figura a publicar: 1

Dados do Inventor (72)

Inventor 1 de 6

Nome: ADRIANO BORGES DA CUNHA

CPF: 83457666687

Nacionalidade: Brasileira

Qualificação Física: Professor do ensino superior

Endereço: Av. Antônio Carlos, 6627 - Unidade Administrativa II - 2º andar- sala 2011

Cidade: Belo Horizonte

Estado: MG

CEP: 31270-901

País: BRASIL

Telefone: (31) 340 96430

Fax:

Email: patentes@ctit.ufmg.br

Inventor 2 de 6

Nome: GUILHERME LEAL FERNANDES

CPF: 07934363621

Nacionalidade: Brasileira

Qualificação Física: Pesquisador

Endereço: Av. Antônio Carlos, 6627 - Unidade Administrativa II - 2º andar- sala 2011

Cidade: Belo Horizonte

Estado: MG

CEP: 31270-901

País: BRASIL

Telefone: (31) 340 96430

Fax:

Email: patentes@ctit.ufmg.br

Inventor 3 de 6

Nome: CARLOS EDUARDO DA SILVA PINEL

CPF: 13134196646

Nacionalidade: Brasileira

Qualificação Física: Pesquisador

Endereço: Av. Antônio Carlos, 6627 - Unidade Administrativa II - 2º andar- sala 2011

Cidade: Belo Horizonte

Estado: MG

CEP: 31270-901

País: BRASIL

Telefone: (31) 340 96430

Fax:

Email: patentes@ctit.ufmg.br

Inventor 4 de 6

Nome: DANIEL HENRIQUE ALVES BICALHO DIAS

CPF: 13140489617

Nacionalidade: Brasileira

Qualificação Física: Pesquisador

Endereço: Av. Antônio Carlos, 6627 - Unidade Administrativa II - 2º andar- sala 2011

Cidade: Belo Horizonte

Estado: MG

CEP: 31270-901

País: BRASIL

Telefone: (31) 340 96430

Fax:

Email: patentes@ctit.ufmg.br

Inventor 5 de 6

Nome: ALEXANDRE DINIZ MARQUES

CPF: 09967810645

Nacionalidade: Brasileira

Qualificação Física: Pesquisador

Endereço: Av. Antônio Carlos, 6627 - Unidade Administrativa II - 2º andar- sala 2011

Cidade: Belo Horizonte

Estado: MG

CEP: 31270-901

País: BRASIL

Telefone: (31) 340 96430

Fax:

Email: patentes@ctit.ufmg.br

Inventor 6 de 6

Nome: SAMUEL RODRIGUES OLIVEIRA

CPF: 04778109694

Nacionalidade: Brasileira

Qualificação Física: Pesquisador

Endereço: Av. Antônio Carlos, 6627 - Unidade Administrativa II - 2º andar- sala 2011

Cidade: Belo Horizonte

Estado: MG

CEP: 31270-901

País: BRASIL

Telefone: (31) 340 96430

Fax:

Email: patentes@ctit.ufmg.br

Tipo Anexo	Nome
Comprovante de pagamento de GRU 200	1 - Comprovante de pagamento - 29409162312409450.pdf
Portaria	2 - Portaria 2195-2020 - Prof. Gilberto UFMG.pdf
Procuração	3 - Procuração Copasa.pdf
Comprovação de Poderes	4 - Comprovação de Poderes Copasa.pdf
Relatório Descritivo	5 - Relatório Descritivo.pdf
Reivindicação	6 - Reivindicações.pdf
Desenho	7 - Desenho.pdf
Resumo	8 - Resumo.pdf

Acesso ao Patrimônio Genético

- ☒ Declaração Negativa de Acesso - Declaro que o objeto do presente pedido de patente de invenção não foi obtido em decorrência de acesso à amostra de componente do Patrimônio Genético Brasileiro, o acesso foi realizado antes de 30 de junho de 2000, ou não se aplica.

Declaração de veracidade

- ☒ Declaro, sob as penas da lei, que todas as informações acima prestadas são completas e verdadeiras.

___ SIAFI2023-DOCUMENTO-CONSULTA-CONGRU (CONSULTA GUIA DE RECOLHIMENTO DA UNIAO
27/11/23 10:54 USUARIO : GABRIEL PASSOS
DATA EMISSAO : 27Nov23 TIPO : 1 - PAGAMENTO NUMERO : 2023GR800800
UG/GESTAO EMITENTE : 153254 / 15229 - ADMINISTRACAO GERAL/UFGM
UG/GESTAO FAVORECIDA : 183038 / 18801 - INSTITUTO NACIONAL DA PROPRIEDADE INDU
RECOLHEDOR : 153254 GESTAO : 15229
CODIGO RECOLHIMENTO : 72200 - 6 COMPETENCIA: NOV23 VENCIMENTO: 27Nov23
DOC. ORIGEM: 153254 / 15229 / 2023NP002327 PROCESSO : 23072.215546/2023
RECURSO : 1
(=) VALOR DOCUMENTO : 70,00
(-) DESCONTO/ABATIMENTO:
(-) OUTRAS DEDUCOES :
(+) MORA/MULTA :
(+) JUROS/ENCARGOS :
(+) OUTROS ACRESCIMOS :
(=) VALOR TOTAL : 70,00
NOSSO NUMERO/NUMERO REFERENCIA : 00029409162312409450
CODIGO DE BARRAS : 89610000000 0 70000001010 3 95523127220 9 00360640000 4
OBSERVACAO
Serviço: 200-Pedido nacional de Invenção, Modelo de Utilidade, Certificado de
Adição de Invenção e entrada na fase nacional do PCT
LANCADO POR : 05621286111 - GABRIEL PASSOS UG : 153254 27Nov2023 10:03
PF1=AJUDA PF3=SAI PF2=DADOS ORC/FIN PF4=ESPELHO PF12=RETORNA



UNIVERSIDADE FEDERAL DE MINAS GERAIS

PORTARIA Nº 2195, DE 06 DE ABRIL DE 2020

A REITORA DA UNIVERSIDADE FEDERAL DE MINAS GERAIS, no uso de suas atribuições legais e estatutárias, considerando o disposto nos artigos 11 e 12 do Decreto-Lei nº 200, de 25 de fevereiro de 1967,

RESOLVE:

Art. 1º Delegar competência ao Diretor da Coordenadoria de Transferência e Inovação Tecnológica (CTIT), Professor Gilberto Medeiros Ribeiro, Inscrição UFMG nº 247405 e SIAPE nº 1964486, e a seu substituto eventual para, no âmbito desse Órgão,

- a) assinar, por meio eletrônico ou físico, documentos ou instrumentos jurídicos, concernentes ao exercício das atividades de competência da CTIT, no âmbito da Lei 10.973/04 – Lei de Inovação Tecnológica, da Política de Inovação da UFMG e suas resoluções específicas, tais como Contrato de Transferência de *Know-How*, Contrato de Licenciamento de Tecnologia, Contrato de Partilhamento de Titularidade de Tecnologia, Acordos de Confidencialidade e Termos de Sigilo, Termos de Autorização de Teste e documentos afins;
- b) assinar, por meio eletrônico ou físico, documentação necessária para depósito, processamento, adição, retificação, substituição, modificação, ampliação e resposta de relatórios referentes a objeto de proteção de propriedade intelectual junto aos órgãos competentes, em âmbito nacional e internacional;
- c) autorizar a realização de despesas dentro dos limites orçamentários da CTIT;
- d) autorizar a concessão de suprimento de fundos a servidores da Unidade, bem como determinar a baixa de responsabilidade;
- e) requisitar passagens e transportes em geral, por quaisquer vias, nos limites da dotação orçamentária da CTIT;
- f) autorizar viagens de servidores, a serviço da Unidade, arbitrando-lhes as respectivas diárias, obedecidas as disposições legais pertinentes;
- g) assinar contratos, decorrentes de licitação, de dispensa de licitação ou inexigibilidade, no âmbito da CTIT;
- h) prover arrecadação de receitas em geral, no âmbito da CTIT; e
- i) apurar dívidas de terceiros para com a Universidade, oriundas de contratos de cotitularidade, licenciamento, transferência, dentre outros, adotando as medidas necessárias à regularização delas, no âmbito da CTIT.

Art. 2º Com base no disposto no Decreto nº 10.193, de 27 de dezembro de 2019, e no inciso II do art. 1º e art. 3º da Portaria nº 243, de 12 de fevereiro de 2020, do Ministério da Educação (MEC), subdelegar

competência ao supracitado Diretor e a seu substituto eventual para, no âmbito da CTIT,

I - celebrar novos contratos administrativos decorrentes de licitação, de dispensa de licitação e de inexigibilidade, ou prorrogar contratos em vigor relativos às atividades de custeio cujos valores sejam inferiores a R\$500.000,00 (quinhentos mil reais); e

II - autorizar a realização de despesas relativas às atividades de custeio cujos valores sejam inferiores a R\$500.000,00 (quinhentos mil reais).

Art. 3º Tornar sem efeito a Portaria nº 010, de 24 de janeiro de 2019.

Art. 4º A presente Portaria entra em vigor nesta data.

Belo Horizonte, 6 de abril de 2020.

Profa. Sandra Regina Goulart Almeida
Reitora



Documento assinado eletronicamente por **Sandra Regina Goulart Almeida, Reitora**, em 09/04/2020, às 17:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).

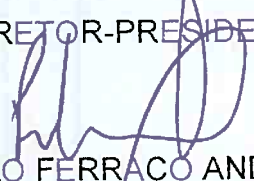
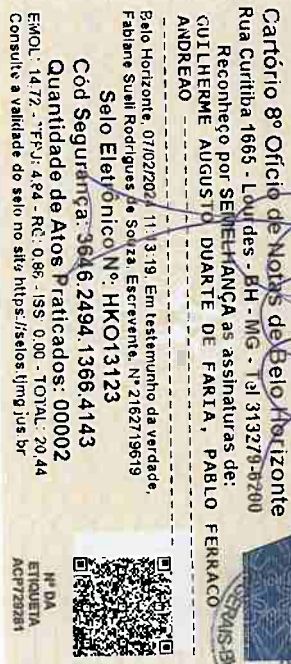


A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0096203** e o código CRC **04D898C8**.

DRJU n.º 05/2024

COMPANHIA DE SANEAMENTO DE MINAS GERAIS - COPASA MG, Sociedade de Economia Mista, com sede em Belo Horizonte/MG, na Rua Mar de Espanha, nº 525, inscrita no CNPJ/MF sob o nº 17.281.106/0001-03, neste ato, representada por seu Diretor-Presidente **GUILHERME AUGUSTO DUARTE DE FARIA**, brasileiro, casado, administrador público, Carteira de Identidade MG-7.644.881 SSP/MG, CPF nº 080.172.116-43; e por seu Diretor de Desenvolvimento Tecnológico, Meio Ambiente e Empreendimentos, **PABLO FERRAÇO ANDREÃO**, brasileiro, casado, engenheiro civil, Carteira de Identidade CONFEA n.º 0801223490, CPF n.º 002.073.317-82, por este instrumento particular de procuração, nomeia e constitui seus bastantes procuradores, pelo prazo de 1 (um) ano, a contar da data de assinatura deste instrumento, confere poderes especiais à **UNIVERSIDADE FEDERAL DE MINAS GERAIS - UFMG**, com sede na Avenida Antônio Carlos, nº 6.627, Belo Horizonte, Minas Gerais, inscrita no CNPJ sob o nº 17.217.985/0001-04, representada neste ato pelo **Professor Gilberto Medeiros Ribeiro**, Diretor da **Coordenadoria de Transferência e Inovação Tecnológica – CTIT**, para representá-la perante o Instituto Nacional da Propriedade Industrial – INPI, para o fim de requerer e processar direitos de propriedade intelectual face ao pedido de patente intitulado “**PROCESSOS DE COMUNICAÇÃO EM REDE DE TRANSCEPTORES DE RÁDIO COM REDUÇÃO DE VULNERABILIDADES**”, a ser depositado junto ao INPI, para mantê-lo em vigor com amplos poderes para assinar petições e documentos, pagar taxas, anotar transferências, fazer prova de uso da invenção patenteada, apresentar oposições, recursos, réplicas, anotar, elaborar notificações extrajudiciais, e praticar para os fins mencionados todos os atos necessários perante as autoridades administrativas competentes no Brasil e no exterior, em benefício da Outorgante, ratificando os atos já praticados. Vedado o substabelecimento, total ou parcial, do presente mandato.

Belo Horizonte, 05 de fevereiro de 2024.


GUILHERME AUGUSTO DUARTE DE FARIA
DIRETOR-PRESIDENTE
PABLO FERRAÇO ANDREÃO
DIRETOR DE DESENVOLVIMENTO TECNOLÓGICO,
MEIO AMBIENTE E EMPREENDIMENTOS

COMPANHIA DE SANEAMENTO DE MINAS GERAIS - COPASA MG

COMPANHIA ABERTA

NIRE 31.300.036.375

CNPJ nº 17.281.106/0001-03

ATA DE REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO

REALIZADA EM 25 DE MAIO DE 2023

1. Data, hora e local: realizada no dia vinte e cinco de maio do ano de dois mil e vinte e três, às dez horas e trinta minutos, na sede da Companhia, localizada na rua Mar de Espanha, 525, Santo Antônio, na cidade de Belo Horizonte, Estado de Minas Gerais. **2. Presença:** convocação realizada nos termos do Estatuto Social da Companhia, estando fisicamente presentes os Conselheiros Guilherme Augusto Duarte de Faria, Hamilton Amadeo, Helio Marcos Coutinho Beltrão, Jaime Leôncio Singer, Marcelo Souza Monteiro e Robson Guedes Campos, bem como a Secretária Executiva de Governança, Kátia Roque da Silva. **3. Mesa:** assumiu a presidência dos trabalhos, na forma estatutária, o Presidente do Conselho de Administração, Hamilton Amadeo, que convidou Kátia Roque da Silva para secretariá-lo. **4. Ordem do dia:** **4.1.** recondução dos membros da Diretoria Executiva; **4.2.** reporte do Diretor-Presidente; **4.3.** reporte dos assuntos discutidos pelo Comitê de Auditoria Estatutário - COAUDI; **4.4.** reporte do Comitê de Investimentos - CINV; **4.5.** Carta Anual de Políticas Públicas e de Governança Corporativa - Proposta de Resolução do Conselho de Administração - PCA nº 033/23; **4.6.** instituição da Política de Defesa da Concorrência - PCA nº 034/23; **4.7.** análise do atendimento das metas e resultados na execução do Plano de Negócios e da Estratégia de Longo Prazo no exercício de 2022; **4.8.** acompanhamento do Orçamento Empresarial 2023; **4.9.** acompanhamento do Orçamento Regulatório 2023; **4.10.** status do projeto de capitalização de despesas de manutenção como reposição de ativos; **4.11.** acompanhamento dos trabalhos de Auditoria Interna referentes ao 1º trimestre de 2023; **4.12.** reporte do Risco Tratamento de Esgoto; **4.13.** indicador e apetite ao risco R025 - Saúde e Segurança do Trabalho - PCA nº 035/23; **4.14.** acompanhamento dos trabalhos da Superintendência de Compliance relativos ao 1º trimestre de 2023; **4.15.** Métricas de Integridade; **4.16.** revisão da Política de Gestão de Riscos Corporativos - PCA nº 036/23; **4.17.** acompanhamento do Plano de Ação de Redução de Perdas de Água; **4.18.** formalização de instrumentos contratuais para permitir o pagamento de valores relativos ao reequilíbrio econômico-financeiro de contratos de empreitada - PCA nº 037/23; **4.19.** formalização dos seguintes aditamentos contratuais: **4.19.1.** IV termo aditivo de adequação de planilha, com alteração de valor, ao contrato nº 20.2023 para obras e serviços de ampliação e melhorias do sistema de esgotamento sanitário - SES na Sede do município de Ubá - PCA nº 038/23; **4.19.2.** I termo aditivo de valor e prazo ao contrato nº 22.2449 para prestação de serviços ambientais de cercamento de nascentes e matas ciliares - PCA nº 039/23; **4.19.3.** III termo aditivo de valor e prazo ao contrato nº 21.0344 para prestação de serviços de implantação do SAP S/4 HANA Utilities e seus módulos em nuvem do Success Factor e Asset Manager - PCA nº 040/23; **4.20.** reporte da homologação do processo administrativo licitatório CPLI nº 0520230103, referente à aquisição de energia elétrica no Ambiente de Contratação Livre - ACL. **5. Deliberações/Discussões:** os Conselheiros tomaram conhecimento e deliberaram sobre os seguintes assuntos: **5.1.** após análise de currículos e verificação dos requisitos e vedações, de acordo com a Política de Indicação e Elegibilidade de Membros Estatutários da Companhia, reconduzir, conforme inciso II do artigo 29 do Estatuto Social da Companhia, os seguintes membros da Diretoria Executiva da Companhia: **a) Diretor-Presidente:** Guilherme Augusto Duarte de Faria, brasileiro, casado, administrador público,

CPF nº 080.172.116-43, portador da Identidade nº MG-7.644.881 SSP/MG, residente e domiciliado em Belo Horizonte - MG, na rua Olga Dias de Castro, nº 288, apartamento 304, bairro Santa Rosa, CEP 31255-700; **b)** Diretor Financeiro e de Relações com Investidores: Carlos Augusto Botrel Berto, brasileiro, casado, economista, CPF nº 883.832.456-53, portador da Identidade nº M-5.237.154 SSP/MG, residente e domiciliado em Belo Horizonte - MG, na rua Alvarenga Peixoto, nº 876, apartamento 101, bairro Lourdes, CEP 30180-124; **c)** Diretor de Relacionamento com o Cliente e Regulação: Cleyson Jacomini de Sousa, brasileiro, casado, administrador de empresas, CPF nº 688.918.066-68, portador da Identidade M-3.948.461, residente e domiciliado em Belo Horizonte - MG, na rua Alvarenga Peixoto, nº 832, apartamento 201, bairro Lourdes, CEP 30180-124; **d)** Diretor de Operação: Guilherme Frasson Neto, brasileiro, casado, engenheiro eletricitista, CPF nº 447.555.386-53, portador da Identidade nº M-2.082.495 SSP/MG, residente e domiciliado em Lavras - MG, na rua José Augusto de Andrade, nº 56, bairro Centro - CEP 37200-128; e **e)** Diretora de Desenvolvimento Tecnológico, Meio Ambiente e Empreendimentos: Márcia Fragoso Soares, brasileira, casada, engenheira civil, CPF nº 863.363.477-53, portadora da Carteira de Identidade Profissional CREA-RJ nº 871074983, residente e domiciliada em Belo Horizonte - MG, na rua Carangola, nº 123, apartamento 401, bairro Santo Antônio, CEP 30330-240. O prazo de gestão dos Diretores será de 2 (dois) anos e terminará na data da primeira reunião do Conselho de Administração a ser realizada após a Assembleia Geral Ordinária do exercício de 2025, sendo a respectiva posse condicionada a: (i) assinatura do Termo de Posse e de compromisso de atingimento de metas e resultados; e (ii) assinatura da Declaração de Desimpedimento nos termos da legislação aplicável. Os Conselheiros registraram o reconhecimento pelos esforços envidados por parte dos Diretores e os parabenizaram pelos resultados alcançados pela Diretoria Executiva nesta gestão. O Conselheiro Guilherme Augusto Duarte de Faria não participou da discussão deste item, em conformidade com o inciso V do artigo 16 do Regimento Interno do Conselho de Administração; **5.2.** o Diretor-Presidente reportou ao Conselho de Administração sobre os atuais assuntos relevantes para a Companhia. Na sequência, apresentou a proposta de alteração do Regulamento do Plano de Carreiras, Cargos e Salários - PCCS. O Coordenador do Comitê de Gestão de Pessoas - CGP, Helio Marcos Coutinho Beltrão, informou que este assunto foi apreciado pelo CGP, o qual manifestou favoravelmente à proposta apresentada. Após discussão, o Conselho de Administração autorizou, conforme artigo 29 do Estatuto Social da Companhia, a alteração dos artigos 53, 56 e 60 do Regulamento do PCCS da COPASA MG. O Conselheiro Robson Guedes Campos não participou da discussão deste assunto, em conformidade com o inciso V do artigo 16 do Regimento Interno do Conselho de Administração; **5.3.** o membro do COAUDI, Marcelo Souza Monteiro, apresentou informações sobre os assuntos tratados na reunião de 22/05/2023 do COAUDI, destacando os principais pontos relevantes discutidos; **5.4.** o membro do CINV, Hamilton Amadeo, apresentou as informações sobre os assuntos tratados na reunião de 22/05/2023 deste Comitê; **5.5.** foi apresentada a proposta de aprovação da Carta Anual de Políticas Públicas e de Governança Corporativa, em atendimento à Lei nº 13.303/2016 e de acordo com o padrão aprovado em 07/02/2018. Após discussão e ajustes efetuados, o Conselho de Administração aprovou, conforme artigo 29 do Estatuto Social da Companhia, a Carta Anual de Políticas Públicas e de Governança Corporativa, a ser arquivada na Comissão de Valores Mobiliários - CVM e na Brasil, Bolsa, Balcão - B3, bem como disponibilizada no site da Companhia e enviada ao Tribunal de Contas do Estado de Minas Gerais - TCE-MG; **5.6.** foi apresentada a proposta de instituição da Política de Defesa da Concorrência, sendo destacado que essa proposta possui justificativas técnicas e atende aos aspectos legais. Após discussão, o Conselho de Administração autorizou, conforme artigo 29 do Estatuto Social da Companhia, a instituição da

Política de Defesa da Concorrência, nº POL CSMG-2023-003/0; **5.7.** em atendimento ao artigo 29 do Estatuto Social da Companhia, o Conselho de Administração autorizou a publicação das conclusões relativas ao atendimento das metas e resultados na execução do Plano de Negócios e da Estratégia de Longo Prazo no exercício de 2022, a serem informadas à Assembleia Legislativa do Estado de Minas Gerais e ao Tribunal de Contas do Estado de Minas Gerais; **5.8.** foram apresentadas informações sobre o acompanhamento do Orçamento Empresarial 2023, sendo demonstrados os resultados de abril, relativos ao faturamento, aos custos e despesas e ao Programa de Investimentos - PI; **5.9.** foram apresentados os resultados de abril do Orçamento Regulatório 2023; **5.10.** foi apresentado o status do projeto de capitalização de despesas de manutenção como reposição de ativos; **5.11.** foi apresentado o acompanhamento dos trabalhos de Auditoria Interna, referente ao 1º trimestre de 2023, sendo destacado os trabalhos de auditoria concluídos, bem como o acompanhamento das recomendações emitidas da Auditoria em 2022 e 2023 e o posicionamento sobre as denúncias do Canal de Linha Ética; **5.12.** foram repassadas informações relativas ao Risco Corporativo Tratamento de Esgoto; **5.13.** aprovar, conforme artigo 29 do Estatuto Social da Companhia, os indicadores e o apetite ao Risco Corporativo R025 - Saúde e Segurança do Trabalho; **5.14.** foi apresentado o acompanhamento dos trabalhos da Superintendência de Compliance referente ao 1º trimestre de 2023; **5.15.** foi apresentado o acompanhamento do Plano de Integridade relativo ao 1º trimestre de 2023; **5.16.** foi apresentada a proposta de revisão da Política de Gestão de Riscos Corporativos, sendo destacado que essa proposta possui justificativas técnicas e atende aos aspectos legais. Após discussão, o Conselho de Administração autorizou, conforme artigo 29 do Estatuto Social da Companhia, a revisão da referida Política; **5.17.** foi apresentado o acompanhamento do Plano de Ação de Redução de Perdas de Água; **5.18.** após análise do material disponibilizado previamente e considerando as justificativas técnicas e os aspectos legais, o Conselho de Administração autorizou, conforme artigo 30 da NP nº 2018-006/5 e observando as regras dos artigos 340, 341 e 342 do Regulamento de Contratações da COPASA MG nº 2018-001/7, a formalização de instrumentos contratuais, visando permitir o pagamento de valores de reequilíbrio econômico-financeiro aos contratos de empreitada nº 21.0592, 21.1284, 21.0990, 22.1452 e 21.0277 devidamente reconhecidos pela Companhia. Esta aprovação está condicionada à aquiescência das empresas contratadas, referente aos valores acordados para o reequilíbrio econômico-financeiro contratual; **5.19.** após análise do material disponibilizado previamente e considerando as justificativas técnicas e os aspectos legais, o Conselho de Administração autorizou, conforme artigo 30 da NP nº 2018-006/5, a formalização dos seguintes aditivos contratuais: **5.19.1.** IV termo aditivo de adequação de planilha, com alteração de valor, ao contrato nº 20.2023, referente às obras e serviços de ampliação e melhorias do sistema de esgotamento sanitário na Sede do município de Ubá, acrescendo-o em R\$3.462.049,50 (três milhões, quatrocentos e sessenta e dois mil, quarenta e nove reais e cinquenta centavos), correspondente a 5,60% (cinco vírgula sessenta por cento) do valor original do contrato, totalizando com esse aditamento o montante de R\$76.484.773,29 (setenta e seis milhões, quatrocentos e oitenta e quatro mil, setecentos e setenta e três reais e vinte e nove centavos); **5.19.2.** I termo aditivo de valor e prazo ao contrato nº 22.2449, referente à prestação de serviços ambientais de cercamento de nascentes e matas ciliares, por meio da construção de cerca de arame farpado e cerca de arame liso, acrescendo-o em R\$2.848.350,00 (dois milhões, oitocentos e quarenta e oito mil, trezentos e cinquenta reais), correspondente a 25% (vinte e cinco por cento) do valor original do contrato, prorrogando o prazo por mais 8 (oito) meses, totalizando com esse aditamento o montante de R\$14.241.750,00 (quatorze milhões, duzentos e quarenta e um mil, setecentos e cinquenta reais) e passando seu vencimento para 03/02/2024;

5.19.3. o assunto relativo ao item 4.19.3 da Ordem do Dia foi retirado de pauta, a pedido do Diretor Financeiro e de Relações com Investidores; **5.20.** em atendimento à solicitação do Conselho de Administração, foram disponibilizadas informações relativas à homologação do processo administrativo licitatório CPLI nº 0520230103, referente à aquisição de energia elétrica no ACL.

6. Participantes: Alessandra Guimarães Rocha, Superintendente de Compliance; Bruno Vieira Andrade, Superintendente de Gestão de Ativos; Carlos Augusto Botrel Berto, Diretor Financeiro e de Relações com Investidores; Cláudio César Dotti, Superintendente de Desenvolvimento de Empreendimentos; Fabrícia Matos Alves Penna, Gerente da Unidade de Serviço de Assuntos Regulatórios; Ítalo José Cabral Guerra, Superintendente da Controladoria; Glenda Lúcia Pessoa Arthuzo, Superintendente de Pessoas; Guilherme Frasson Neto, Diretor de Operação; Márcia Fragoso Soares, Diretora de Desenvolvimento, Tecnológico, Meio Ambiente e Empreendimentos; Marcus Tullius Reis, Superintendente de Desenvolvimento Tecnológico, Inovação e Engenharia; Mario Lúcio da Silva, Gerente da Unidade de Serviço de Gestão de Riscos; Mauro Lúcio Henrique de Carvalho, Gerente da Unidade de Serviço de Saúde e Segurança do Trabalho; Michelle Gomes de Resende, Superintendente de Gestão Estratégica; Osvaldo Raimundo Rodrigues, Gerente da Unidade de Serviços de Relações Com Investidores; Renata Gomes Ubaldo Machado Vasconcelos, Auditora Geral; e Valter de Souza Lucas Júnior, Gerente da Unidade de Serviço de Hidrometria. **7. Encerramento:** nada mais havendo a se tratar, foram encerrados os trabalhos e concluída a Ata, depois lida, aprovada e assinada pela secretária Kátia Roque da Silva e pelos Conselheiros. Belo Horizonte, 25 de maio de 2023. Confere com a original.

Guilherme Augusto Duarte de Faria
Conselheiro

Hamilton Amadeo
Presidente do Conselho

Helio Marcos Coutinho Beltrão
Vice-Presidente do Conselho

Jaime Leôncio Singer
Conselheiro

Marcelo Souza Monteiro
Conselheiro

Robson Guedes Campos
Conselheiro

Kátia Roque da Silva
Secretária

COMPANHIA DE SANEAMENTO DE MINAS GERAIS - COPASA MG

COMPANHIA ABERTA

NIRE 31.300.036.375

CNPJ nº 17.281.106/0001-03

ATA DE REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO

REALIZADA EM 29 DE NOVEMBRO DE 2023

1. Data, hora e local: realizada no dia vinte e nove de novembro do ano de dois mil e vinte e três, às quatorze horas, na sede da Companhia, localizada na rua Mar de Espanha, 525, Santo Antônio, na cidade de Belo Horizonte, Estado de Minas Gerais. **2. Presença:** convocação realizada nos termos do Estatuto Social da Companhia, estando presentes os Conselheiros Guilherme Augusto Duarte de Faria, Hamilton Amadeo, Jaime Leôncio Singer, Marcelo Souza Monteiro, Márcia Fragoso Soares e Robson Guedes Campos, bem como a Secretária Executiva de Governança, Kátia Roque da Silva. O Conselheiro Helio Marcos Coutinho Beltrão, participou virtualmente da reunião, conforme artigo 24 do Estatuto Social da Companhia. **3. Mesa:** assumiu a presidência dos trabalhos, na forma estatutária, o Presidente do Conselho de Administração, Hamilton Amadeo, que convidou Kátia Roque da Silva para secretariá-lo. **4. Ordem do dia:** **4.1.** reporte do Comitê de Gestão de Pessoas - CGP; **4.1.1.** plano de ação de redução de horas extras; **4.2.** reporte do Diretor-Presidente; **4.3.** reporte dos assuntos discutidos pelo Comitê de Auditoria Estatutário - COAUDI; **4.4.** reporte do Comitê de Investimentos - CINV; **4.5.** acompanhamento do Orçamento Empresarial 2023; **4.6.** premissas do Orçamento Empresarial 2024; **4.7.** acompanhamento do Orçamento Regulatório 2023; **4.8.** status do projeto de capitalização de despesas de manutenção como reposição de ativos; **4.9.** acompanhamento do Plano de Ação de Redução de Perdas de Água; **4.10.** indicadores e apetite aos riscos corporativos "R005 - Proteção de Receita" e "R015 - Relacionamento com Clientes" - Proposta de Resolução do Conselho de Administração - PCA nº 080/23; **4.11.** acompanhamento dos trabalhos da Superintendência de Compliance relativos ao 3º trimestre de 2023; **4.12.** acompanhamento das métricas do Plano de Integridade; **4.13.** acompanhamento dos trabalhos de Auditoria Interna - AUDI, do Canal de Denúncias e do *follow-up* de recomendações, referentes aos meses de agosto, setembro e outubro de 2023; **4.14.** equacionamento do déficit do Plano de Previdência Complementar Copasa Saldado, administrado pela Fundação Libertas - PCA nº 081/23; **4.15.** calendário de reuniões para 2024 - PCA nº 082/23; **4.16.** instauração de processo administrativo licitatório para obras e serviços de ampliação e melhorias do sistema de abastecimento de água - SAA da Sede do município de Pouso Alegre - PCA nº 083/23; **4.17.** formalização do I termo aditivo de adequação de planilha, com alteração de valor, ao contrato nº 22.2070 para obras e serviços de crescimento vegetativo, manutenção e melhorias operacionais de água e de esgoto, na área de abrangência da Gerência Regional Metropolitana Oeste - PCA nº 084/23; **4.18.** formalização do IV termo aditivo de valor e prazo ao contrato nº 20.0274, referente à prestação de serviços de distribuição de créditos de vales alimentação e refeição para os empregados da COPASA MG - PCA nº 085/23. **5. Deliberações/Discussões:** os Conselheiros tomaram conhecimento e deliberaram sobre os seguintes assuntos: **5.1. e 5.1.1.** o Coordenador do CGP, Helio Marcos Coutinho Beltrão, apresentou as informações sobre a reunião do CGP de 14/11/2023, destacando as discussões e recomendações efetuadas pelo Comitê à Superintendência de Pessoas, referentes ao plano de ação para redução de horas extras. O Conselho de Administração solicitou que o CGP e o

COAUDI, nas suas respectivas áreas de competência, acompanhem a implementação das medidas recomendadas pela Diretoria Executiva que visam a solucionar os problemas identificados. O Conselheiro Robson Guedes Campos não participou da discussão deste assunto, em conformidade com o inciso V do artigo 16 do Regimento Interno do Conselho de Administração; **5.2.** o Diretor-Presidente, Guilherme Augusto Duarte de Faria, reportou ao Conselho de Administração informações sobre os atuais assuntos relevantes para a Companhia; **5.3.** o Coordenador do COAUDI, Marcelo Souza Monteiro, apresentou as informações sobre os assuntos tratados na reunião de 27/11/2023 do COAUDI, destacando os principais pontos discutidos; **5.4.** o Coordenador do CINV, Hamilton Amadeo, reportou informações sobre os assuntos apresentados na reunião de 27/11/2023, destacando as manifestações deste Comitê; **5.5.** foram apresentadas informações sobre o acompanhamento do Orçamento Empresarial 2023, sendo demonstrados os resultados de outubro, relativos ao faturamento, aos custos e despesas e ao Programa de Investimentos - PI; **5.6.** foram apresentadas informações relativas ao cronograma e às premissas do Orçamento Empresarial 2024; **5.7** foram apresentados os resultados de outubro de 2023 relativos ao Orçamento Regulatório; **5.8.** foi apresentado o status do projeto de capitalização de despesas de manutenção como reposição de ativos; **5.9.** foi apresentado o acompanhamento do Plano de Ação de Redução de Perdas de Água; **5.10.** foi apresentada a proposta para definição dos indicadores e apetite aos riscos corporativos “R005 - Proteção de Receita” e “R015 - Relacionamento com Clientes”. Após análise e discussão, considerando a manifestação favorável do COAUDI na reunião de 23/10/2023, o Conselho de Administração aprovou, conforme artigo 29 do Estatuto Social da Companhia, os indicadores e apetite dos referidos riscos corporativos; **5.11.** foi apresentado o acompanhamento do Plano Anual da Superintendência de Compliance relativo ao 3º trimestre de 2023, as informações sobre as ações referentes à Lei Geral de Proteção de Dados Pessoais - LGPD, bem como o acompanhamento do Plano Anual da Gestão de Riscos, sendo demonstrado os níveis de criticidade dos riscos corporativos; **5.12.** foi apresentado o acompanhamento das métricas do Plano de Integridade da Companhia; **5.13.** foi apresentado o acompanhamento dos trabalhos de Auditoria Interna, do Canal de Denúncias, bem como o *follow-up* de recomendações e outras atividades pertinentes da AUDI, referentes aos meses de agosto, setembro e outubro de 2023; **5.14.** após análise do material disponibilizado previamente e considerando as justificativas técnicas e os aspectos legais, bem como a manifestação favorável do COAUDI na reunião de 23/10/2023, o Conselho de Administração autorizou o equacionamento do valor de R\$25.012.918,00 (vinte e cinco milhões, doze mil, novecentos e dezoito reais) para o restabelecimento do equilíbrio econômico-financeiro e atuarial do Plano de Previdência Complementar Copasa Saldado, autorizando o aporte da parte da COPASA MG correspondente à R\$12.113.981,30 (doze milhões, cento e treze mil, novecentos e oitenta e um reais e trinta centavos) a ser pago em parcela única até abril de 2024; **5.15.** foi apresentado e aprovado o calendário das reuniões do Conselho de Administração para o exercício de 2024; **5.16.** após análise do material disponibilizado previamente e considerando as justificativas técnicas e os aspectos legais, bem como a manifestação favorável do CINV na reunião de 27/11/2023, o Conselho de Administração autorizou, conforme artigo 29 do Estatuto Social da Companhia, a instauração de processo administrativo licitatório, referente à execução, com aquisição de materiais a cargo da COPASA MG, das obras e serviços de ampliação e melhorias do sistema de abastecimento de água da Sede do município de Pouso Alegre, no

montante de até R\$63.000.000,00 (sessenta e três milhões de reais), com prazo de execução previsto de 36 (trinta e seis) meses; **5.17.** após análise do material disponibilizado previamente e considerando as justificativas técnicas e legais, bem como a manifestação favorável do CINV na reunião de 27/11/2023, o Conselho de Administração autorizou, conforme artigo 30 da NP nº 2018-006/7, a formalização do I termo aditivo de adequação de planilha, com alteração de valor, ao contrato nº 22.2070, referente às obras e serviços de manutenção, melhorias operacionais e crescimento vegetativo de água e esgoto, na área de abrangência da Gerência Regional Metropolitana Oeste, acrescendo-o em R\$8.680.061,18 (oito milhões, seiscentos e oitenta mil, sessenta e um reais e dezoito centavos), correspondente a 15,43% (quinze vírgula quarenta e três por cento) do valor original do contrato, totalizando com esse aditamento o montante de R\$64.925.871,64 (sessenta e quatro milhões, novecentos e vinte e cinco mil, oitocentos e setenta e um reais e sessenta e quatro centavos); **5.18.** foi apresentada a proposta de formalização do IV termo aditivo de valor e prazo ao contrato nº 20.0274, sendo destacado que essa proposta possui justificativas técnicas e atende aos aspectos legais. Após discussão, o Conselho de Administração autorizou, conforme artigo 29 do Estatuto Social da Companhia, a formalização do IV termo aditivo de valor e prazo ao contrato nº 20.0274, referente à prestação de serviços de distribuição de créditos para vale alimentação e refeição, por meio de cartões eletrônicos e/ou magnéticos, destinados aos empregados da COPASA MG, no valor de R\$175.891.276,22 (cento e setenta e cinco milhões, oitocentos e noventa e um mil, duzentos e setenta e seis reais e vinte e dois centavos), prorrogando o prazo por mais 12 (doze) meses, passando seu vencimento para 27/02/2025. **6. Assuntos Gerais: 6.1.** após análise do currículo e verificação dos requisitos, de acordo com a Política de Indicação e Elegibilidade de Membros Estatutários da Companhia, considerando manifestação favorável do COAUDI na reunião de 27/11/2023, em substituição a Guilherme Augusto Duarte de Faria, que respondia interinamente pela Diretoria de Desenvolvimento Tecnológico, Meio Ambiente e Empreendimentos, o Conselho de Administração elegeu, por maioria de votos, conforme inciso II do artigo 29 do Estatuto Social da Companhia, para o cargo de Diretor de Desenvolvimento Tecnológico, Meio Ambiente e Empreendimentos, a partir de 01/12/2023, Pablo Ferraço Andreão, brasileiro, casado, engenheiro civil, CPF nº 002.073.317-82, carteira de identidade CONFEA 0801223490, residente e domiciliado em Vitória - Espírito Santo, na rua Izaltino Arão Marques, nº 191, apartamento 1.201, bairro Mata da Praia, CEP 29065-450. O prazo de gestão do Diretor, ora eleito, será de 2 (dois) anos, e terminará na data da primeira reunião do Conselho de Administração, a ser realizada após a Assembleia Geral Ordinária do exercício de 2025, sendo a sua posse condicionada a: (i) assinatura do Termo de Posse e de compromisso de atingimento de metas e resultados; e (ii) assinatura da Declaração de Desimpedimento nos termos da legislação aplicável. O Conselheiro Robson Guedes Campos absteve-se da votação. **7. Participantes:** Alessandra Guimarães Rocha, Superintendente de Compliance; Bruno Vieira Andrade, Superintendente de Gestão de Ativos; Carlos Augusto Botrel Berto, Diretor Financeiro e de Relações com Investidores; Cláudio César Dotti, Superintendente de Desenvolvimento de Empreendimentos; Cleyson Jacomini de Sousa, Diretor de Relacionamento com o Cliente e Regulação; Elisângela Martins de Oliveira, Gerente da Unidade de Serviços de Informações e Estudos Econômicos; Glenda Lúcia Pessoa Arthuzo, Superintendente de Pessoas; Ítalo José Cabral Guerra; Superintendente da Controladoria; Marcus Tullius de Paula Reis, Superintendente de Desenvolvimento Tecnológico, Inovação e Engenharia; Mário Lúcio da Silva,

Gerente da Unidade de Serviço de Gestão de Riscos; Michelle Gomes de Resende, Superintendente de Gestão Estratégica; Pablo Duarte Lima, Gerente da Unidade de Serviço de Administração de Pessoal; Renata Gomes Ubaldo Machado Vasconcelos, Auditora Geral; Thimóteo Cezar Lima, Gerente da Unidade de Serviço de Assuntos Regulatórios; Valter de Souza Lucas Júnior, Gerente da Unidade de Serviço de Hidrometria; e Wallace Lúcio Silva, Superintendente de Relacionamento com o Cliente. **8. Encerramento:** nada mais havendo a se tratar, foram encerrados os trabalhos e concluída a Ata, depois lida, aprovada e assinada pela secretária Kátia Roque da Silva e pelos Conselheiros Guilherme Augusto Duarte de Faria, Hamilton Amadeo, Helio Marcos Coutinho Beltrão, Jaime Leôncio Singer, Marcelo Souza Monteiro, Márcia Fragoso Soares e Robson Guedes Campos. Belo Horizonte, 29 de novembro de 2023. Confere com a original.

Guilherme Augusto Duarte de Faria
Conselheiro

Hamilton Amadeo
Presidente do Conselho

Helio Marcos Coutinho Beltrão
Vice-Presidente do Conselho

Jaime Leôncio Singer
Conselheiro

Marcelo Souza Monteiro
Conselheiro

Márcia Fragoso Soares
Conselheira

Robson Guedes Campos
Conselheiro

Kátia Roque da Silva
Secretária

“PROCESSOS DE COMUNICAÇÃO EM REDE DE TRANSCEPTORES DE RÁDIO COM REDUÇÃO DE VULNERABILIDADES”

[01] Propõe-se um processo de comunicação entre transceptores de rádio controlados por plataformas de prototipação eletrônicas (PPE) baseadas em microcontroladores (PPE-MC) ou baseadas em computadores de placa única (PPE-CPU). Os transceptores são preferencialmente de modulação *Chirp spread spectrum* (CSS) (Ex.: *LoRa: Long Range*), operados num modelo de controle de comunicação assimétrico do tipo mestre e escravo com *polling* cíclico e tempo de serviço limitado para evitar colisões de mensagens. O transceptor mestre funciona como um *hub* de comunicação que controla e determina o envio de dados pelos transceptores escravos da rede de comunicação para o mestre (*gateway*). A tecnologia inclui uma camada de segurança para redução de vulnerabilidades e mitigação de riscos que utiliza um identificador unívoco (UID) de cada transceptor no processo de autenticação e verificação de integridade. A tecnologia propicia que a informação transmitida na rede de comunicação seja protegida por criptografia, por exemplo no padrão *advanced encryption standard* (AES). Utilizam-se também funcionalidades de segurança como *software* (*firmware*) de inicialização seguro ou *secure boot* (SB), criptografia do conteúdo da memória *flash* ou *flash encryption* (FE) e comunicação segura com protocolo *Transport Layer Security* (TLS). A tecnologia proposta se aplica em redes de comunicação, especialmente no contexto de Internet das Coisas (IoT).

[02] Há no estado da técnica algumas tecnologias dedicadas a possibilitar a comunicação entre transceptores de rádio, sendo que algumas têm meios de redução de vulnerabilidades e mitigação a ataques cibernéticos e de riscos, como as apresentadas a seguir.

[03] O documento CN115022739, com data de prioridade de 18/04/2022, intitulado "Data acquisition system and method based on LoRa communication", propõe uma rede de comunicação baseada em transceptores com tecnologia LoRa (*Long Range*) com configuração do tipo mestre e escravo. Entretanto, não propõe nenhuma medida de redução de vulnerabilidades em relação a riscos de ataques que possam ameaçar a cibersegurança.

[04] O documento CN109688555, com data de prioridade de 28/12/2018, intitulado "Real-time acquisition and communication system and method of signal data", propõe uma rede de comunicação baseada em transceptores com tecnologia LoRa (*Long Range*). O sistema de comunicação apresentado utiliza a tecnologia *Bluetooth* para abrir e encerrar as sessões de comunicação dos módulos LoRa. Dessa forma, cada nó da rede (mestres e escravos) deve necessariamente conter um módulo *Bluetooth* juntamente com um módulo LoRa. O processo de autenticação baseia-se na verificação de correspondência de um código de autenticação entre nós comunicantes. A comparação ocorre depois de reverter a criptografia simétrica que é aplicada somente no código de autenticação e não em toda a mensagem que foi trocada entre os nós.

[05] O mecanismo de autenticação descrito na tecnologia CN109688555 tem uma desvantagem grave que consiste no fato de que, uma vez descoberto o código de autenticação, o cibercriminoso poderá usá-lo para se autenticar perante a todos os nós da rede.

[06] Na tecnologia ora proposta, cada nó da rede tem um identificador unívoco que, caso seja descoberto pelo cibercriminoso, permitirá apenas a autenticação indevida de um nó da rede, que é aquele que teve o identificador unívoco revelado. Dessa forma, o impacto será menor se comparado ao impacto causado com o uso da autenticação proposta na tecnologia CN109688555.

[07] No estado da técnica há um padrão de comunicação em rede baseado na técnica de modulação CSS muito conhecido e utilizado, trata-se da especificação *LoRaWAN* que inclui um protocolo de rede de baixo consumo denominado *Low Power Wide Area* (LPWA) projetado para conexão sem fio no contexto de Internet das Coisas (IoT).

[08] A tecnologia *LoRa* inclui a modulação *LoRa* e os *chipsets* (conjuntos de *chips*) proprietários, que implementam transceptores de rádio, além da pilha de protocolos *LoRaWAN* (por exemplo as séries de chips SX12xx e SX13xx que servem de base para fabricação de transceptores e “gateways”, respectivamente), cuja titularidade patentária pertence à empresa fabricante de tais dispositivos, a *SEMTECH Corporation*.

[09] Os chips da SEMTECH são utilizados por outros fabricantes do ecossistema *LoRa* para fabricar os diversos dispositivos de rede *LoRaWan* como *endpoints* ou *end-devices*, *gateways*, servidores de rede etc. Os *end-devices* (transceptores) podem custar até cem vezes menos que os *gateways* ou servidores de rede, ou seja, em uma rede *LoRaWan* típica o *end-device* costuma ser o dispositivo mais barato.

[10] Na tecnologia ora proposta apresenta-se uma rede de comunicação com uma especificação distinta da *LoRaWan* formada apenas por dispositivos do tipo *end-devices* baseados em transceptores de rádio em que o papel de *gateway* é desempenhado pelo transceptor mestre que, de forma complementar, encaminha as mensagens enviadas pelos escravos para um servidor via comunicação Ethernet, Modem-3G, Wi-Fi ou outros.

[11] A tecnologia proposta neste pedido de patente propõe um processo de comunicação entre transceptores de rádio controlados por plataformas de prototipação eletrônicas (PPE) baseadas em microcontroladores (PPE-MC) ou baseadas em computadores de placa única (PPE-CPU). Os transceptores podem ser de modulação *Chirp*

spread spectrum (CSS) (Ex.: *LoRa: Long Range*), operados num modelo de controle de comunicação assimétrico do tipo mestre e escravo com *polling* cíclico e tempo de serviço limitado para evitar colisões de mensagens. O transceptor mestre funciona como um *hub* de comunicação que controla e determina o envio de dados pelos transceptores escravos da rede de comunicação para o mestre (*gateway*). A tecnologia inclui uma camada de segurança para redução de vulnerabilidades e mitigação de riscos que utiliza um identificador unívoco (UID) de cada transceptor no processo de autenticação e verificação de integridade. Propicia que a informação transmitida na rede de comunicação seja protegida por criptografia, por exemplo no padrão *advanced encryption standard* (AES). A tecnologia utiliza também funcionalidades de segurança como *software (firmware)* de inicialização seguro ou *secure boot* (SB), criptografia do conteúdo da memória *flash* ou *flash encryption* (FE) e comunicação segura com protocolo *Transport Layer Security* (TLS).

[12] As medidas de segurança adotadas visam garantir confidencialidade, integridade e disponibilidade das informações, recursos e serviços relacionados à rede de comunicação apresentada na tecnologia ora proposta.

BREVE DESCRIÇÃO DAS FIGURAS

[13] A **figura 1** exibe, de forma não limitante, um exemplo de rede de comunicação (3) implementada conforme o processo proposto, formada por um mestre e três escravos. Os instantes T1, T2 e T3 representam o início dos períodos delimitados pelo tempo de serviço em que há comunicação dos escravos com o mestre. A seta em linha contínua representa a solicitação de envio de mensagem do mestre ao escravo, já a seta tracejada representa a mensagem de resposta do escravo ao mestre.

[14] A **figura 2** exibe, de forma não limitante, o fluxograma que descreve de forma resumida as ações do mestre no processo de comunicação ora proposto.

[15] A **figura 3** exibe, de forma não limitante, o fluxograma que descreve de forma resumida as ações do escravo no processo de comunicação ora proposto.

[16] A **figura 4** exibe, de forma não limitante, um exemplo de plataforma de prototipação eletrônica (PPE) baseada em microcontroladores (PPE-MC) com um microcontrolador ESP32 (kit de desenvolvimento) como recurso computacional (1) e um módulo LoRa E220-400T22D como transceptor de rádio (2).

[17] A **figura 5** exibe, de forma não limitante, um exemplo de plataforma de prototipação eletrônica (PPE) baseadas computadores de placa única (PPE-CPU) com um *Raspberry pi* como recurso computacional (1) e um módulo LoRa E220-400T22D como transceptor de rádio (2).

DESCRIÇÃO DETALHADA DA TECNOLOGIA

[18] A tecnologia proposta neste pedido de patente propõe um processo de comunicação entre transceptores de rádio controlados por plataformas de prototipação eletrônicas (PPE) baseadas em microcontroladores (PPE-MC) ou baseadas em computadores de placa única (PPE-CPU). Os transceptores são preferencialmente de modulação *Chirp spread spectrum* (CSS) (Ex.: *LoRa: Long Range*), operados num modelo de controle de comunicação assimétrico do tipo mestre e escravo com *polling* cíclico e tempo de serviço limitado para evitar colisões de mensagens. O transceptor mestre funciona como um *hub* de comunicação que controla e determina o envio de dados pelos transceptores escravos da rede de comunicação para o mestre (*gateway*). A tecnologia inclui uma camada de segurança para redução de vulnerabilidades e mitigação de riscos que utiliza um identificador

unívoco (UID) de cada transceptor no processo de autenticação e verificação de integridade. A tecnologia propicia que a informação transmitida na rede de comunicação seja protegida por criptografia, por exemplo no padrão *advanced encryption standard* (AES). Utilizam-se também funcionalidades de segurança como *software (firmware)* de inicialização seguro ou *secure boot* (SB), criptografia do conteúdo da memória *flash* ou *flash encryption* (FE) e comunicação segura com protocolo *Transport Layer Security* (TLS).

[19] Adiante apresenta-se o processo de comunicação entre transceptores de rádio, contendo meios de redução de vulnerabilidades e mitigação a ataques cibernéticos e de riscos. O processo se divide em dois, sendo um para implementação do escravo e outro do mestre, que são as duas possibilidades de configuração para os nós na rede de comunicação proposta. O processo aplicado ao mestre está representado no fluxograma da figura 3 e o processo aplicado ao escravo está representado no fluxograma da figura 4.

[20] O processo de comunicação em rede de transceptores de rádio com redução de vulnerabilidades caracterizado por aplicar-se aos nós da rede definidos como mestres compreende as seguintes etapas:

- a) incluir, no código-fonte do programa, juntamente como as instruções do processo de comunicação ora pleiteado, como variáveis declaradas, os valores de cada identificador unívoco dos transceptores configurados como escravos que estão autorizados a enviar mensagem para o transceptor mestre escravo e também as chaves simétricas privadas exclusivas para criptografar e descriptografar as mensagens recebidas;
- b) utilizar um protocolo de assinatura digital para verificar a autenticidade do agente que está enviando o novo programa a ser armazenado e executado no PPE bem como verificar a integridade do

arquivo que contém o programa e somente prosseguir se houver autenticação e integridade do programa verificados;

c) criptografar o programa a ser armazenado e executado no PPE e armazená-lo em uma memória sem possibilidades de leitura ou escrita via meios externos físicos ou via *software* e com criptografia;

d) atualizar a frequência de comunicação e configurar e iniciar a comunicação de rádio do transceptor no modo de transmissão (Tx);

e) criptografar e enviar mensagem ao escravo atual contendo a frequência atualizada do canal de comunicação a ser estabelecido na próxima comunicação, o identificador unívoco do mestre juntamente com o segundo identificador unívoco que define e identifica o escravo de destino da mensagem e solicita ao escravo atual que envie a mensagem;

f) após envio, configurar e iniciar a comunicação de rádio modo recepção (Rx) e tentar obter a mensagem enviada pelo escravo atual, e, se a resposta não chegar dentro do tempo estabelecido T_s , retornar à etapa “d” de modo que o próximo escravo seja solicitado;

g) se receber a mensagem, o mestre descriptografa a mensagem com sua chave criptográfica de uso exclusivo com aquele escravo atual;

h) em seguida, o mestre verifica se a mensagem é uma mensagem de alerta ou verifica se o identificador unívoco contido na mensagem corresponde ao de um escravo autorizado:

h.1) caso não haja correspondência, o mestre gera um alerta de segurança “escravo não autorizado tentou estabelecer comunicação” e descarta mensagem considerada inválida;

h.2) se for uma mensagem de alerta enviada pelo escravo ou uma mensagem inválida, o mestre troca a frequência do canal de comunicação com os escravos e retorna à etapa “d”;

h.3) caso o identificador unívoco contido na mensagem corresponda ao de um escravo autorizado, o mestre encaminha a mensagem para o

destino (servidor de dados, de arquivos etc.) com segurança utilizando protocolo *Transport Layer Security* (SSL);

i) em seguida o processo continua de forma iterativa a partir da etapa “d”.

[21] O processo de comunicação em rede de transceptores de rádio com redução de vulnerabilidades caracterizado por aplicar-se aos nós da rede definidos como escravos compreende as seguintes etapas:

- a) incluir, no código-fonte do programa, juntamente como as instruções do processo de comunicação ora pleiteado, como variáveis declaradas, os valores de cada identificador unívoco dos transceptores configurados como mestres que estão autorizados a solicitar e a receber mensagens em relação ao transceptor escravo e também as chaves simétricas privadas exclusivas para criptografar e descriptografar as mensagens recebidas dos mestres autorizados ou enviadas aos mestres autorizados;
- b) utilizar um protocolo de assinatura digital para verificar a autenticidade do agente que está enviando o novo programa a ser armazenado e executado no PPE bem como verificar a integridade do arquivo que contém o programa e somente prosseguir se houver autenticação e integridade do programa verificados;
- c) criptografar o programa a ser armazenado e executado no PPE e armazená-lo em uma memória sem possibilidades de leitura ou escrita via meios externos físicos ou via *software* e com criptografia;
- d) configurar e iniciar a comunicação de rádio modo Rx na última frequência atualizada do canal de comunicação que foi definida anteriormente pelo mestre enviada na última mensagem;
- e) tentar detectar a mensagem de solicitação de algum mestre;
- f) caso a mensagem de solicitação não seja detectada, retornar à etapa “e”;

g) caso a mensagem de solicitação seja detectada, o escravo irá receber a mensagem e descriptografar a mensagem com sua chave criptográfica de uso exclusivo com aquele mestre e em seguida o escravo verifica se o identificador unívoco contido na mensagem corresponde ao de um mestre autorizado a solicitar mensagens e verifica se o segundo identificador unívoco contido na mensagem que define e identifica o escravo de destino da mensagem corresponde ao seu próprio identificador unívoco:

g.1) caso o identificador unívoco contido na mensagem não corresponda ao de um mestre autorizado, o escravo gera um alerta de segurança, descarta a mensagem inválida e envia ao mestre uma mensagem de alerta ao mestre (“Mestre não autorizado e/ou falta de Integridade da mensagem”);

g.2) caso o segundo identificador unívoco contido na mensagem que define o escravo de destino da mensagem não corresponda ao seu próprio identificador unívoco, o escravo retorna à etapa “d”;

g.3) caso o identificador unívoco contido na mensagem corresponda ao de um mestre autorizado e o segundo identificador unívoco contido na mensagem que define o escravo de destino da mensagem corresponda ao seu próprio identificador unívoco, o escravo estabelece um canal de comunicação na última frequência atualizada que foi definida anteriormente pelo mestre e enviada na última mensagem do mestre, e inicia a comunicação de rádio modo Tx;

h) em seguida, no caso de “g.3”, o escravo criptografa e envia mensagem ao mestre solicitante contendo o identificador unívoco deste escravo (o escravo atual) juntamente com algum dado útil;

i) o processo continua de forma iterativa a partir da etapa “d”.

[22] É possível configurar o escravo para aguardar, quando estiver executando a etapa “e”, um tempo pré-definido no modo Rx antes de voltar para a etapa “d”.

[23] A presente invenção pode ser melhor compreendida através do exemplo abaixo, não limitante.

EXEMPLO 1 – Implementação do processo de comunicação entre transceptores de rádio com redução de vulnerabilidades, mitigação de riscos e de ataques cibernéticos

[24] A tecnologia pode ser concretizada utilizando-se plataformas de prototipação eletrônicas (PPE) baseadas em microcontroladores (PPE-MC), por exemplo Arduino, ESP32 e outros ou computadores de placa única (PPE-CPU) como por exemplo *Raspberry pi*.

[25] As plataformas mencionadas são denominadas de forma genérica como recursos computacionais (1) que na tecnologia ora proposta são conectados a transceptores de rádio (2) controlando-os via comandos. O conjunto de dispositivos (mestres e escravos) comunica entre si formando os nós de uma rede de comunicação (3).

[26] Os transceptores utilizados podem ser módulos baseados nos seguintes *chipsets*: RN2903, eLR100-UL-00, E32915T30D, RFM95W-915S, E220-900T330D. No momento do depósito do pedido de patente estavam homologados no Brasil pela ANATEL (Agência Nacional de Telecomunicações).

[27] No processo de comunicação ora proposto utiliza-se uma configuração do tipo mestre/escravo em conjunto com a técnica de *polling* cíclico com tempos de serviço limitados com intuito de evitar-se colisões de mensagens.

[28] Na tecnologia, o programa é criptografado antes de ser enviado para a memória do PPE para proteger a confidencialidade do identificador unívoco utilizado na autenticação dos membros da rede

entre si, para proteger as chaves criptográficas privadas simétricas usadas para criptografar e/ou descriptografar o conteúdo das mensagens trocadas na rede (criptografia ponto a ponto) e proteger também o próprio conteúdo do programa em que estão expressas as instruções por meio de linguagem de programação. Essa etapa de criptografia do programa é realizada tanto no programa que controla o transceptor mestre como no programa que controla o transceptor escravo, os quais implementam os processos ora pleiteados.

[29] Utiliza-se assinatura digital para verificar a identidade do agente que fornece o programa que será armazenado e executado no recurso computacional (1). O processo de criação de uma assinatura digital consiste em aplicar uma função *hash* sobre a mensagem que se deseja assinar, em seguida criptografa-se o valor *hash* utilizando-se uma chave privada. O resultado será uma mensagem assinada digitalmente. Em seguida, o emissor deve encaminhar a mensagem, junto com a chave pública. O receptor, por sua vez, deverá usar esta chave para descriptografar a assinatura. Se o resultado obtido for igual ao valor *hash* da mensagem recebida, significa que aquela assinatura é válida e que a mensagem não sofreu nenhuma alteração ao longo da transmissão. A assinatura digital visa garantir a autoria do documento, e que a mensagem não tenha sido modificada durante sua transmissão. No caso da tecnologia ora proposta a mensagem é o próprio programa a ser embarcado no recurso computacional (1), o *firmware*. Os principais algoritmos utilizados para implementação da assinatura digital são RSA, ElGamal e algoritmo de Assinatura Digital em Curvas Elípticas ECDSA. (Rivest, R.; A. Shamir; L. Adleman (1978). «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems» (PDF). Communications of the ACM. 21 (2): 120–126. CiteSeerX 10.1.1.607.2677Acessível livremente.), (ElGamal, T. A Public Key

Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: IEEE Transactions on Information Theory, volume IT-31 no. 4, p. 469–472. IEEE, 1985.), (Rivest, R. L.; Hellman, M. E.; Anderson, J. C. ; Lyons, J. W. Responses to NIST’s proposal. In: Communications of the ACM, volume 35, p. 41–54, New York, NY, USA, 1992. ACM.), (Miller, V. S. Use of Elliptic Curves in Cryptography. In: Advances in Cryptology, volume 218, p. 417–426, Berlin, 1985. Springer Verlag).

[30] O protocolo *Transport Layer Security* (TLS) é utilizado na tecnologia proposta na instância do *gateway* na comunicação com redes externas. O TLS é um protocolo de segurança projetado para fornecer segurança nas comunicações sobre uma rede de computadores. O protocolo TLS visa principalmente fornecer privacidade e integridade de dados entre aplicações de computador que se comunicam. A segurança alcançada decorre das seguintes propriedades: 1) a conexão é privada (ou segura) porque a criptografia simétrica é usada para criptografar os dados transmitidos. As chaves para essa criptografia simétrica são geradas exclusivamente para cada conexão e são baseadas em um segredo compartilhado que foi negociado no início da sessão de comunicação, mitigando o “ataque do homem do meio” ou de *replay*. 2) A identidade das partes em comunicação pode ser autenticada usando criptografia de chave pública (ex.: assinatura digital). Essa autenticação pode ser opcional, mas geralmente é necessária para pelo menos uma das partes (geralmente o servidor). 3) A conexão é confiável porque cada mensagem transmitida inclui uma verificação de integridade de mensagens usando um código de autenticação de mensagens para evitar perda não detectada ou alteração dos dados durante a transmissão, a integridade pode ser verificada utilizando-se funções de dispersão criptográfica do tipo *hash* (T. Dierks, E. Rescorla (Agosto de

2008). «The Transport Layer Security (TLS) Protocol Version 1.2». tools.ietf.org (em inglês). Consultado em 6 de novembro de 2020).

[31] Um processo elementar de autenticação entre mestres e escravos da rede é implementado utilizando-se um identificador unívoco de cada dispositivo dos nós da rede (mestres ou escravos). Esse método aplica a autenticação da seguinte forma: cada dispositivo detém uma lista secreta contendo o identificador unívoco dos dispositivos que estão autorizados a enviar mensagens ou solicitar o envio de mensagens por meio de uma mensagem de solicitação.

[32] De forma complementar todo dispositivo ao enviar uma mensagem inclui nela o seu próprio identificador unívoco visando obter a devida autenticação junto ao dispositivo alvo da mensagem. No método proposto, as mensagens só são consideradas se o processo de autenticação for bem sucedido, ou seja, as solicitações de envio de mensagem e recebimento de mensagens só são válidas se o identificador unívoco contido na mensagem corresponder a algum identificador unívoco contido na lista secreta do dispositivo que está recebendo a mensagem; seja uma mensagem normal (mensagem contendo dados e informações específicas da aplicação para qual a rede de comunicação foi criada) ou uma mensagem de solicitação de envio por parte de um dispositivo da rede na função de mestre.

[33] As listas secretas são declaradas como variáveis nos programas. Essa prática de guardar informações do processo no próprio programa é denominada “*hard-coding*” (existe um programa para controlar o mestre e outro programa que controla o escravo). Os programas são criptografados antes de serem armazenados e executados nos recursos computacionais (1). No caso de um dispositivo desempenhando a função de mestre, a sua lista secreta conterá o identificador unívoco de todos os escravos autorizados a enviar mensagens para esse mestre solicitante.

No caso de um dispositivo desempenhando a função de escravo, a sua lista secreta conterá o identificador unívoco de todos os mestres autorizados a solicitar e receber mensagens desse escravo. No processo de comunicação proposto, a mensagem tem uma estrutura mínima de dados apresentada no quadro 1.

Quadro 1 - Estrutura mínima de dados da mensagem na tecnologia proposta.

UID origem	UID destino	Alerta	Solicitação	<i>Payload</i>	Frequência de comunicação
---------------	----------------	--------	-------------	----------------	---------------------------------

[34] Na estrutura assinala-se o UID de quem envia a mensagem (origem) e o UID do destinatário ou destino. O campo de alerta refere-se à situação descrita na etapa “g” do processo de comunicação do escravo que comunica as possibilidades: “Mestre não autorizado e/ou falta de Integridade da mensagem”.

[35] No campo solicitação define-se a situação descrita na etapa “e” do processo de comunicação do mestre quando a mensagem representa uma solicitação de envio de mensagem feita pelo mestre ao escravo.

[36] A carga útil (*payload*) é a parte dos dados transmitidos que é a mensagem real pretendida. Os demais campos podem ser cabeçalhos e/ou metadados que são enviados apenas para permitir a entrega de carga útil. O *payload* poderia ser, por exemplo, uma medida feita por um sensor conectado ao escravo e este envia a medida realizada ao mestre.

[37] O campo de frequência indica a frequência atualizada do canal de comunicação a ser estabelecido na próxima comunicação. Somente o mestre pode alterar esse campo quando receber uma mensagem de alerta de algum escravo ou quando detectar falta de integridade da mensagem recebida. A falta de integridade da mensagem é detectada

indiretamente quando a descriptografia da mensagem recebida resultar em uma mensagem não inteligível, deteriorada ou com estrutura irregular (que pode ser uma adulteração ou uma perda de dados inesperada).

[38] O identificador unívoco é utilizado na tecnologia proposta para autenticação e também verificação indireta de integridade da mensagem. Dessa forma, um mesmo elemento da mensagem possui duas funções, propiciando uma redução no tamanho final da mensagem. Tal redução é muito vantajosa, pois desonera o tamanho total da mensagem para que se possa transmitir mais carga útil (*payload*). Essa economia é muito importante porque o fluxo de transferência de bits em 'bits por segundo' (bps ou b/s) na modulação CSS é da ordem de poucas centenas de Kbps.

[39] As medidas de redução de vulnerabilidade e de impactos utilizadas nos processos ora propostos para comunicação entre transceptores mestre e o transceptores escravo estão presentes no quadro 2.

Quadro 2 - Medidas de redução de vulnerabilidade, de riscos e de impactos.

Medidas	
1	A inicialização do programa, que consiste na etapa de salvar o programa no recurso computacional (1) e executá-lo pela primeira vez, somente ocorrerá após autenticação do agente responsável pelo fornecimento do programa por meio de um processo de assinatura digital com verificação da integridade do programa utilizando <i>hash</i> , essa medida também é conhecida como <i>secure boot</i> (SB);
2	O programa salvo no recurso computacional (1) sempre está criptografado, essa medida também é conhecida como <i>flash encryption</i> (FE), também se desativa a opção de leitura e escrita na memória reservada ao programa;
3	Todas as mensagens trocadas na rede (3) são criptografadas de forma que cada escravo se comunica a um mestre por meio de um par de chaves exclusivo;

-
- 4 As listas secretas contendo os identificadores unívocos dos nós (mestres e escravos da rede de comunicação) autorizados a estabelecer comunicação na rede e as chaves criptográficas necessárias para descriptografar as mensagens são guardadas nos respectivos programas de cada nó (*hard-coded*), sendo que cada programa se encontra criptografado conforme definido no item 2;
-
- 5 As mensagens trocadas na rede (3) só são consideradas válidas se o processo de autenticação for bem-sucedido. O processo de autenticação é concluído com sucesso se o identificador unívoco contido na mensagem corresponder a algum identificador unívoco contido na lista secreta (lista de UIDs autorizados) do dispositivo que está recebendo a mensagem, seja a mensagem normal (mensagem contendo dados e informações específicas da aplicação para qual a rede de comunicação foi criada) ou a mensagem de solicitação de envio por parte de um dispositivo da rede desempenhando a função de mestre;
-
- 6 O código correspondente ao identificador unívoco (UID) que está presente em cada mensagem enviada é usado também para verificação da integridade da mensagem. Pois caso haja alguma alteração da mensagem durante o transporte a verificação no nó de destino irá resultar em uma verificação malsucedida uma vez que a mensagem descriptografada estará deteriorada em consequência da alteração que sofreu durante o transporte e o nó receptor procederá o descarte da mensagem. A verificação mencionada inclui as etapas de descriptografar e de verificar se o código recebido está presente na lista secreta de códigos (UIDs autorizados) conforme descrito no item 5;
-
- 7 Nas mensagens trocadas na rede (3) envia-se também a frequência de comunicação na qual o canal de comunicação mestre/escravo deverá se estabelecer. O mestre poderá alterar essa frequência caso detecte algum nó intruso desautorizado tentando se comunicar na rede (3) com intuito de excluí-lo do canal de comunicação e evitar uma grande quantidade de solicitações desautorizadas que poderia causar uma sobrecarga e indisponibilidade de comunicação da parte do mestre, deflagrando um ataque de DoS (*Denial of Service*);
-
- 8 Nas mensagens trocadas na rede (3) o nó escravo notifica o mestre caso detecte algum nó intruso desautorizado tentando se comunicar na rede (3) para que o nó mestre altere a frequência de comunicação na qual o canal de comunicação mestre/escravo deverá se estabelecer com intuito de excluí-lo (o nó intruso desautorizado) do canal de comunicação e evitar uma grande
-

	quantidade de solicitações desautorizadas que poderia causar uma sobrecarga e indisponibilidade de comunicação da parte do escravo, deflagrando também um ataque de DoS;
9	A comunicação com redes externas que estão fora da rede de comunicação (3) ocorre utilizando-se o protocolo TLS.

[40] Na tabela 1 faz-se uma associação entre as superfícies de ataque com as vulnerabilidades/ameaças e as medidas propostas de redução de vulnerabilidades, de riscos e de impactos. Os impactos são as consequências que decorrem caso um cibercriminoso obtenha êxito ao explorar uma ou mais vulnerabilidades do sistema considerado.

[41] Um exemplo das medidas 1 e 2 (*secure boot* e *flash encryption*) implementadas com plataformas de prototipação eletrônicas baseadas em microcontroladores (PPE-MC), por exemplo o ESP32, é apresentada na página oficial da documentação técnica do ESP32. (ESP32. Secure Boot. ESP-IDF Programming Guides, Security Guides, Espressif Systems (Shanghai) Co., Ltd, 2023. Disponível em: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/security/secure-boot-v1.html>. Acesso em: 14, setembro, 2023.), (ESP32. Secure Boot V2. ESP-IDF Programming Guides, Security Guides, Espressif Systems (Shanghai) Co., Ltd, 2023. Disponível em: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/security/secure-boot-v2.html>. Acesso em: 14, setembro, 2023.), (ESP32. Flash Encryption. ESP-IDF Programming Guides, Security Guides, Espressif Systems (Shanghai) Co., Ltd, 2023. Disponível em: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/security/flash-encryption.html>. Acesso em: 14, setembro, 2023.).

Tabela 1 - Medidas de redução de vulnerabilidade, de riscos e de impactos utilizadas.

Superfícies	Vulnerabilidades	Riscos da exploração	Medidas
-------------	------------------	----------------------	---------

de ataque		da vulnerabilidade	de mitigação
Memória do dispositivo	Informações sensíveis inteligíveis (programa em si, chaves criptográficas, UIDs, conteúdos da mensagem etc.)	Exposição e acesso das informações sigilosas, quebra de confidencialidade uso de credenciais para elevação e escalonamento de privilégios	2, 4
	Conexões de interface serial	Extração de informações sensíveis da memória do dispositivo, elevação e escalonamento de privilégios, controle de dispositivos	2,4
Interfaces do dispositivo	Escalonamento de privilégios (um cibercriminoso consegue de forma ilegítima acesso ao mesmo nível de privilégios de um usuário ou dispositivo autorizados)	Extração de informações sensíveis da memória do dispositivo (Ex.: chaves e credenciais), controle de dispositivos	2, 4
	Credenciais, informações sensíveis (ex.: UID) e chaves criptográficas armazenadas no próprio programa do dispositivo	Extração de informações sensíveis (Ex.: informações hard-coded), elevação e escalonamento de privilégios, controle de dispositivos	2, 4
Firmware do dispositivo	Serviços vulneráveis (Ex.: armazenamento de imagem de firmware sem criptografia)	Descompilação e cópia a partir do firmware	2, 4
	Atualização de firmware sem	Descompilação e cópia a partir do firmware	1, 2, 4
Atualização de firmware			

Serviços de rede dos dispositivos	criptografia.		
	Atualização de firmware sem autenticação.	Firmware de má ou duvidosa procedência	1, 2
	Atualização de firmware sem verificação de integridade.	Firmware adulterado ou modificado	1, 2
	DoS (<i>Denial of service</i>)	Nós intrusos podem enviar um grande número de mensagens causando sobrecarga, indisponibilidade e interrupção da comunicação	3, 4, 5, 7, 8
	Serviços sem criptografia ou Criptografia insuficiente	Extração de informações	3, 4, 5, 6
	Ataques de "Replay" ou MIM (<i>"man in the middle"</i>)	Interceptação de mensagens e extração de informações sensíveis.	3, 4, 5, 6, 7, 8
	Ausência de verificação de integridade de mensagens	Adulteração de mensagens	3, 4, 5, 6
	LAN para Internet	Interceptação de mensagens em texto simples, ataques Replay ou MIM, identidade não conhecida de quem recebe/envia mensagens	3, 4, 5, 6, 7, 8
	Tráfego dentro da LAN	Descobrir a frequência do canal de comunicação para gerar interferências ou interpor nós intrusos para gerar uma sobrecarga enviando um número grande de mensagens e gerar indisponibilidade	3, 4, 5, 6, 7, 8

	(DoS)	
Adulteração de pacotes /mensagens	Interceptação de mensagens e adulteração do conteúdo	3, 4, 5, 6, 7, 8

[42] A medida 2 (quadro 2) dificulta o êxito de um invasor cibercriminoso que busque uma oportunidade para copiar e decompilar o código embarcado no dispositivo.

[43] A medida 1 (quadro 2) é um obstáculo para exploração de vulnerabilidade para o caso em que ocorra um acesso desautorizado ao hardware visando substituir o programa por uma versão produzida por um agente não autorizado e/ou não confiável ou excluir o programa existente.

[44] As medidas 3, 4, 5, 6, 7, 8 visam reduzir as chances de um cibercriminoso obter privilégios e galgar um acesso desautorizado de dispositivos à rede de comunicação pela obtenção de informações como chaves criptográficas e identificadores unívocos de transceptores por meio de interceptação de mensagens da rede contendo tais informações. As medidas 3, 4, 5, 6, 7, 8 também mitigam ataques para interceptação e obtenção das mensagens trocadas na rede em formato inteligível culminando na quebra de confidencialidade das mensagens.

REIVINDICAÇÕES

1. PROCESSO DE COMUNICAÇÃO EM REDE DE TRANSCETORES DE RÁDIO COM REDUÇÃO DE VULNERABILIDADES caracterizado por se aplicar aos nós da rede definidos como mestres e compreender as seguintes etapas:

- a) incluir, no código-fonte do programa, juntamente com as instruções do processo de comunicação ora pleiteado, como variáveis declaradas, os valores de cada identificador unívoco dos transceptores configurados como escravos que estão autorizados a enviar mensagem para o transceptor mestre escravo e também as chaves simétricas privadas exclusivas para criptografar e descriptografar as mensagens recebidas;
- b) utilizar um protocolo de assinatura digital para verificar a autenticidade do agente que está enviando o novo programa a ser armazenado e executado em plataformas de prototipação eletrônicas (PPE) bem como verificar a integridade do arquivo que contém o programa e somente prosseguir se houver autenticação e integridade do programa verificados;
- c) criptografar o programa a ser armazenado e executado no PPE e armazená-lo em uma memória sem possibilidades de leitura ou escrita via meios externos físicos ou via *software* e com criptografia;
- d) atualizar a frequência de comunicação e configurar e iniciar a comunicação de rádio do transceptor no modo de transmissão (Tx);
- e) criptografar e enviar mensagem ao escravo atual contendo a frequência atualizada do canal de comunicação a ser estabelecido na próxima comunicação, o identificador unívoco do mestre juntamente com o segundo identificador unívoco que define e identifica o escravo de destino da mensagem e solicita ao escravo atual que envie a mensagem;

f) após envio, configurar e iniciar a comunicação de rádio modo recepção (Rx) e tentar obter a mensagem enviada pelo escravo atual, e, se a resposta não chegar dentro do tempo estabelecido T_s , retornar à etapa “d” de modo que o próximo escravo seja solicitado;

g) se receber a mensagem, o mestre descriptografa a mensagem com sua chave criptográfica de uso exclusivo com aquele escravo atual;

h) em seguida, o mestre verifica se a mensagem é uma mensagem de alerta ou verifica se o identificador unívoco contido na mensagem corresponde ao de um escravo autorizado:

h.1) caso não haja correspondência, o mestre gera um alerta de segurança “escravo não autorizado tentou estabelecer comunicação” e descarta a mensagem considerada inválida;

h.2) se for uma mensagem de alerta enviada pelo escravo ou uma mensagem inválida, o mestre troca a frequência do canal de comunicação com os escravos e retorna à etapa “d”;

h.3) caso o identificador unívoco contido na mensagem corresponda ao de um escravo autorizado, o mestre encaminha a mensagem para o destino (servidor de dados, de arquivos etc.) com segurança utilizando protocolo *Transport Layer Security* (SSL);

i) em seguida o processo continua de forma iterativa a partir da etapa “d”.

2. PROCESSO DE COMUNICAÇÃO EM REDE DE TRANSCETORES DE RÁDIO COM REDUÇÃO DE VULNERABILIDADES caracterizado por aplicar-se aos nós da rede definidos como escravos e compreender as seguintes etapas:

a) incluir, no código-fonte do programa, juntamente como as instruções do processo de comunicação ora pleiteado, como variáveis

declaradas, os valores de cada identificador unívoco dos transceptores configurados como mestres que estão autorizados a solicitar e a receber mensagens em relação ao transceptor escravo e também as chaves simétricas privadas exclusivas para criptografar e descriptografar as mensagens recebidas dos mestres autorizados ou enviadas aos mestres autorizados;

b) utilizar um protocolo de assinatura digital para verificar a autenticidade do agente que está enviando o novo programa a ser armazenado e executado no PPE bem como verificar a integridade do arquivo que contém o programa e somente prosseguir se houver autenticação e integridade do programa verificados;

c) criptografar o programa a ser armazenado e executado no PPE e armazená-lo em uma memória sem possibilidades de leitura ou escrita via meios externos físicos ou via *software* e com criptografia;

d) configurar e iniciar a comunicação de rádio modo Rx na última frequência atualizada do canal de comunicação que foi definida anteriormente pelo mestre enviada na última mensagem;

e) tentar detectar a mensagem de solicitação de algum mestre;

f) caso a mensagem de solicitação não seja detectada, retornar à etapa “e”;

g) caso a mensagem de solicitação seja detectada, o escravo irá receber a mensagem e descriptografar a mensagem com sua chave criptográfica de uso exclusivo com aquele mestre e em seguida o escravo verifica se o identificador unívoco contido na mensagem corresponde ao de um mestre autorizado a solicitar mensagens e verifica se o segundo identificador unívoco contido na mensagem que define e identifica o escravo de destino da mensagem corresponde ao seu próprio identificador unívoco:

g.1) caso o identificador unívoco contido na mensagem não corresponda ao de um mestre autorizado, o escravo gera um alerta de segurança, descarta a mensagem inválida e envia ao mestre uma mensagem de alerta ao mestre (“Mestre não autorizado e/ou falta de Integridade da mensagem”);

g.2) caso o segundo identificador unívoco contido na mensagem que define o escravo de destino da mensagem não corresponda ao seu próprio identificador unívoco, o escravo retorna à etapa “d”;

g.3) caso o identificador unívoco contido na mensagem corresponda ao de um mestre autorizado e o segundo identificador unívoco contido na mensagem que define o escravo de destino da mensagem corresponda ao seu próprio identificador unívoco, o escravo estabelece um canal de comunicação na última frequência atualizada que foi definida anteriormente pelo mestre e enviada na última mensagem do mestre, e inicia a comunicação de rádio modo Tx;

h) em seguida, no caso de “g.3”, o escravo criptografa e envia mensagem ao mestre solicitante contendo o identificador unívoco deste escravo (o escravo atual) juntamente com algum dado útil;

i) o processo continua de forma iterativa a partir da etapa “d”.

3. PROCESSO DE COMUNICAÇÃO EM REDE DE TRANSCEPTORES DE RÁDIO COM REDUÇÃO DE VULNERABILIDADES, de acordo com a reivindicação 2, caracterizado por configurar o escravo para aguardar, quando estiver executando a etapa “e”, um tempo pré-definido no modo Rx antes de voltar para a etapa “d”.

DESENHOS

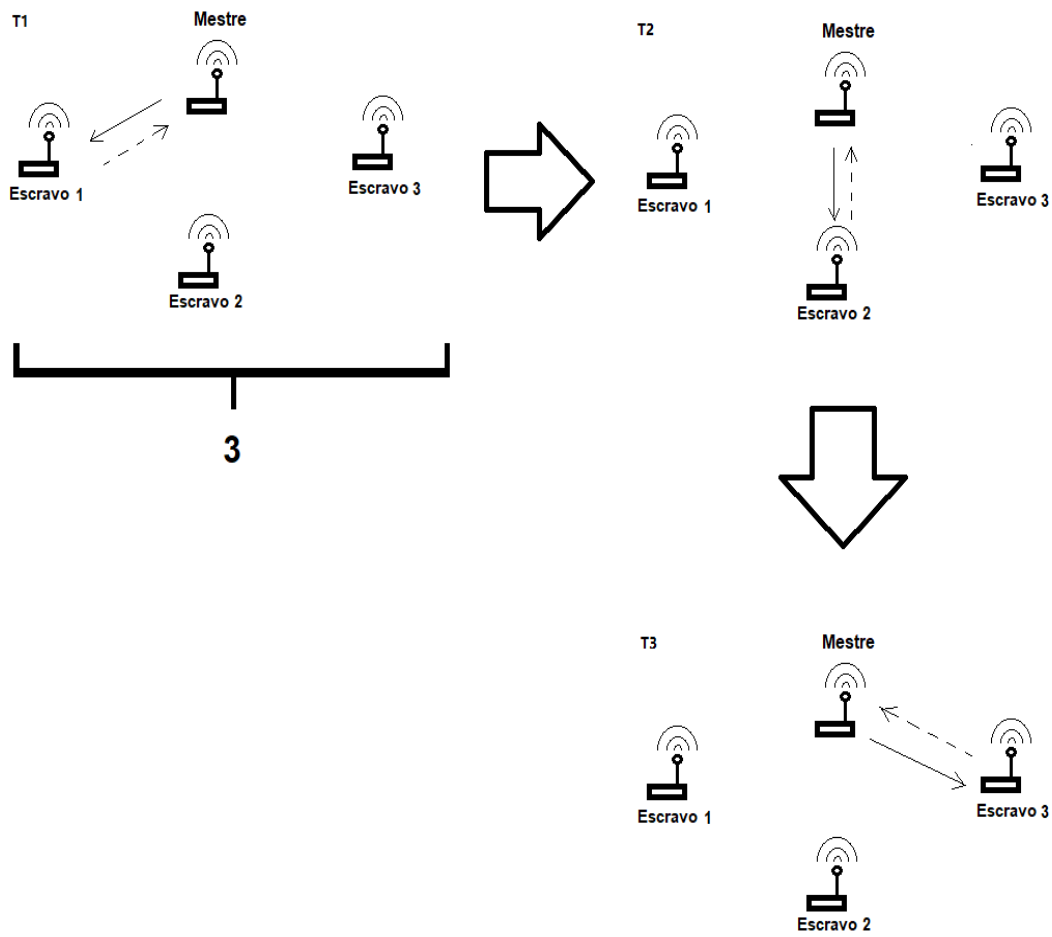


FIGURA 1

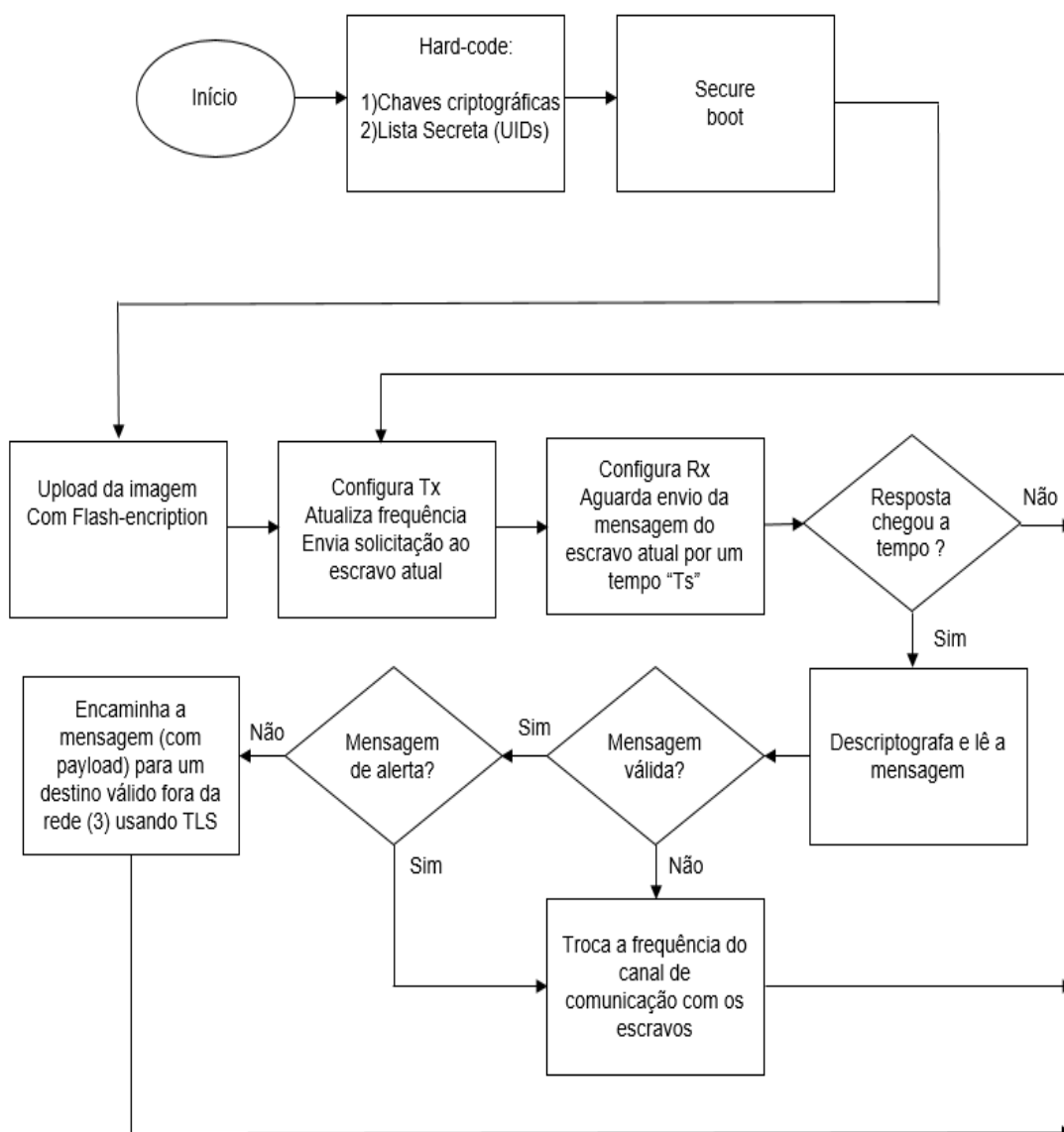


FIGURA 2

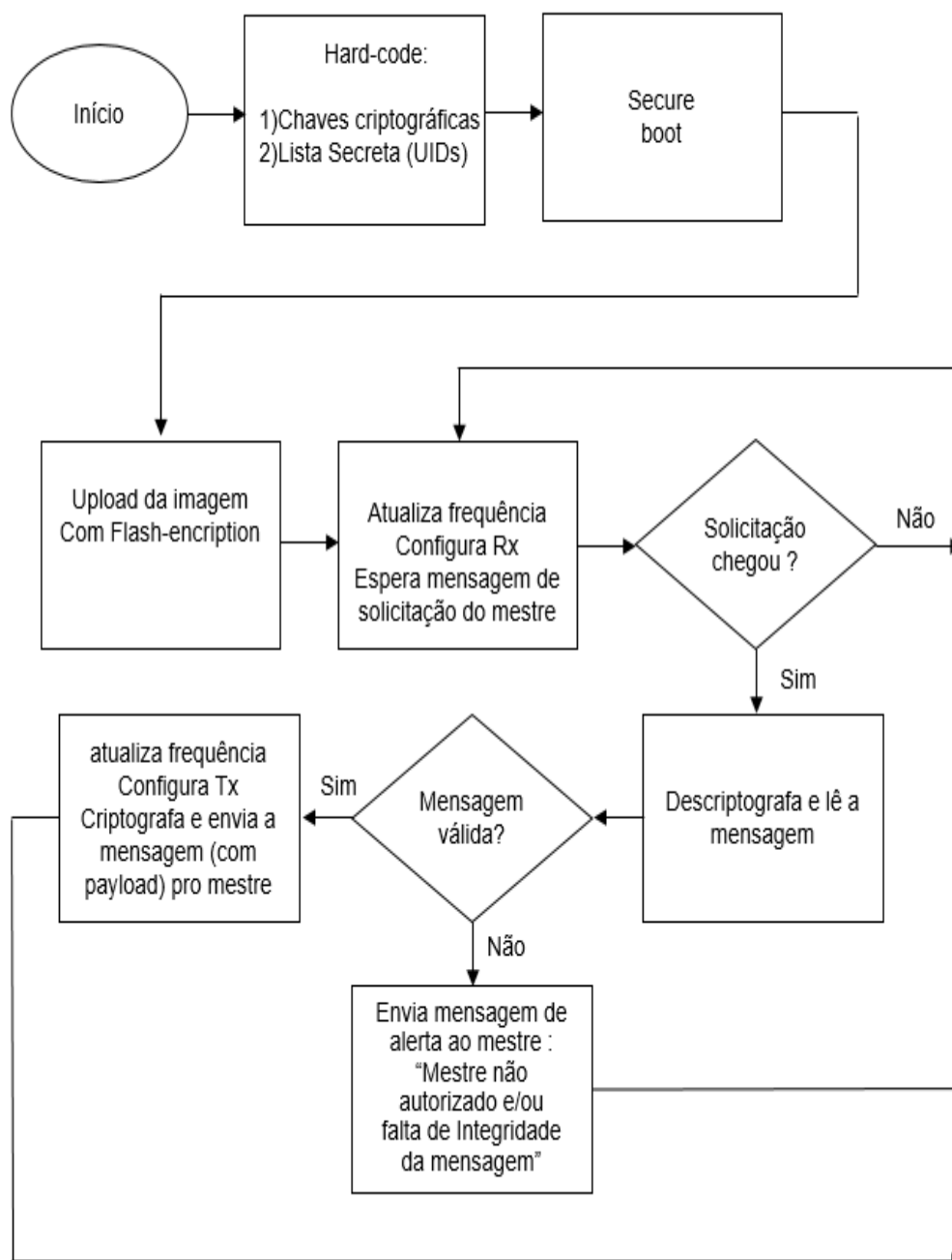


FIGURA 3

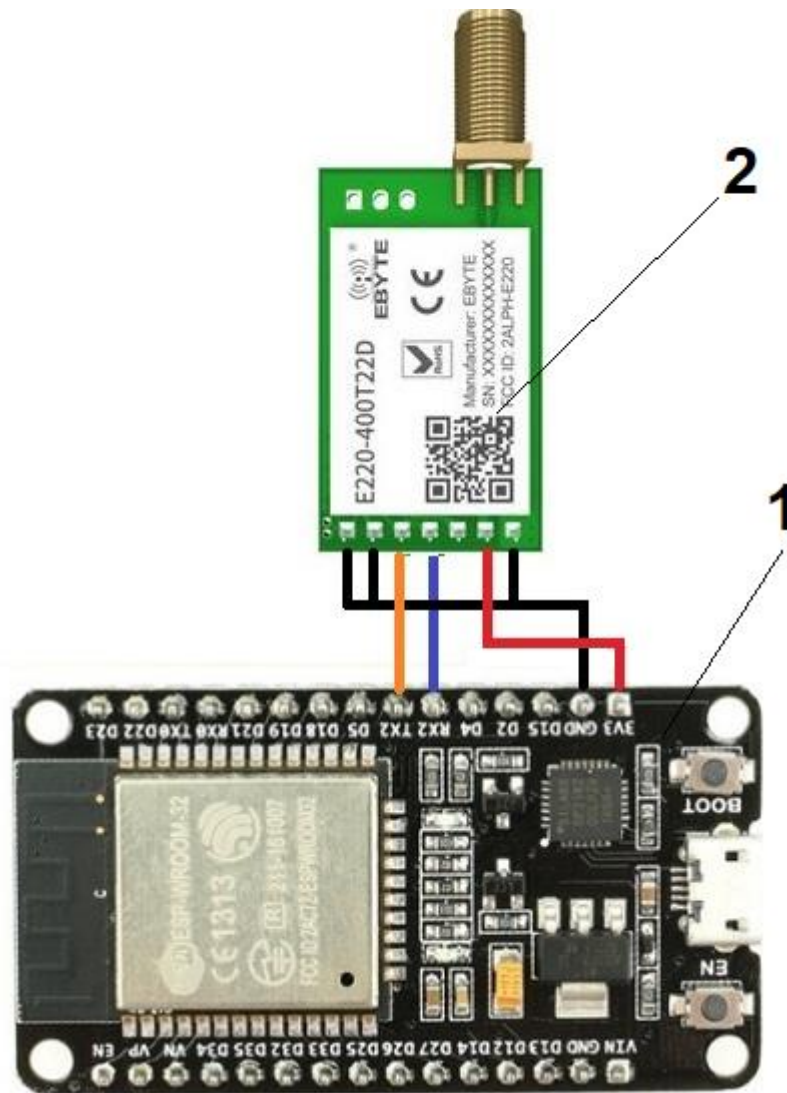


FIGURA 4

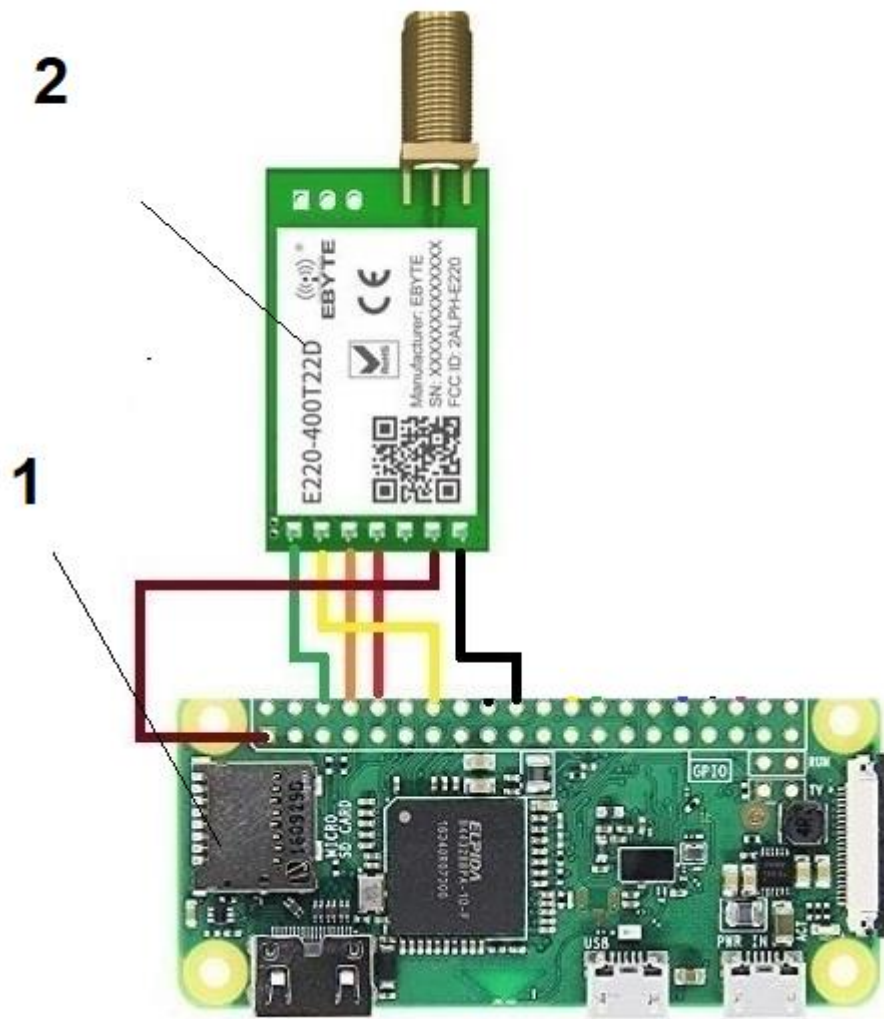


FIGURA 5

RESUMO

“PROCESSOS DE COMUNICAÇÃO EM REDE DE TRANSCÉPTORES DE RÁDIO COM REDUÇÃO DE VULNERABILIDADES”

Propõe-se um processo de comunicação entre transceptores de rádio controlados por plataformas de prototipação eletrônicas (PPE) baseadas em microcontroladores (PPE-MC) ou baseadas em computadores de placa única (PPE-CPU). Os transceptores são preferencialmente de modulação *Chirp spread spectrum* (CSS) (Ex.: *LoRa: Long Range*), operados num modelo de controle de comunicação assimétrico do tipo mestre e escravo com *polling* cíclico e tempo de serviço limitado para evitar colisões de mensagens. O transceptor mestre funciona como um *hub* de comunicação que controla e determina o envio de dados pelos transceptores escravos da rede de comunicação para o mestre (*gateway*). A tecnologia inclui uma camada de segurança para redução de vulnerabilidades e mitigação de riscos que utiliza um identificador unívoco (UID) de cada transceptor no processo de autenticação e verificação de integridade. A tecnologia propicia que a informação transmitida na rede de comunicação seja protegida por criptografia, por exemplo no padrão *advanced encryption standard* (AES). Utilizam-se também funcionalidades de segurança como *software (firmware)* de inicialização seguro ou *secure boot* (SB), criptografia do conteúdo da memória *flash* ou *flash encryption* (FE) e comunicação segura com protocolo *Transport Layer Security* (TLS). A tecnologia proposta se aplica em redes de comunicação, especialmente no contexto de Internet das Coisas (IoT).