Dissertação de Mestrado

Inatel
Instituto Nacional de Telecomunicações

# Extensão da Arquitetura NovaGenesis para Cenários de IoT em Redes LPWAN utilizando LoRa

EPPER BONOMO

JULHO / 2022




# EXTENSÃO DA ARQUITETURA NOVAGENESIS PARA CENÁRIOS DE IOT EM REDES LPWAN UTILIZANDO LORA

EPPER BONOMO

Dissertação apresentada ao Instituto Nacional de Telecomunicações, como parte dos requisitos para obtenção do Título de Mestre em Telecomunicações.

ORIENTADOR: Prof. Dr. Antônio Marcos Alberti.

Santa Rita do Sapucaí
2022

Bonomo, Epper
B719e
Extensão da arquitetura NovaGenesis para cenários de IoT em redes LPWAN utilizando LoRa. / Epper Bonomo – Santa Rita do Sapucaí, 2022.
108 p.

Orientador: Prof. Dr. Antônio Marcos Alberti
Dissertação de Mestrado em Telecomunicações – Instituto Nacional de Telecomunicações – INATEL.
Inclui bibliografia e anexo.

1. NovaGenesis 2. Arquitetura de Internet do Futuro 3. FIA 4. LPWAN 5. LoRa 6. Mestrado em Telecomunicações. I. Alberti, Antônio Marcos. II. Instituto Nacional de Telecomunicações – INATEL. III. Título.

CDU 621.39

Biblioteca "Ministro Oswaldo Bilac Pinto"

Ficha Catalográfica elaborada pelo Bibliotecário da Instituição
CRB6-2718 – Paulo Eduardo de Almeida

**FOLHA DE APROVAÇÃO**

Dissertação defendida e aprovada em _____/_____/_____, pela comissão julgadora:

---

Prof. Dr. Antônio Marcos Alberti
INATEL

---

Prof. Dr. Marcelo Eduardo Pellenz
PUC – PR

---

Prof. Dr. Francisco Martins Portelinha Junior
INATEL

---

**Coordenador do Curso de Mestrado**
Prof. Dr. José Marcos Câmara Brito

*“Se não puder voar, corra. Se não puder correr, ande. Se não puder andar, rasteje, mas continue em frente de qualquer jeito.”*

*Martin Luther King Jr.*

*A Deus,*
*a minha Esposa e filhos,*
*aos meus Pais, irmãos e familiares*
*meus primeiros grandes Professores,*
*meus Amigos de mestrado,*
*meu Orientador.*

# Agradecimentos

Enfim, o grande dia chegou! Aquele para coroar a vitória de uma conquista.
Lembrei-me de quando tudo começou: um colega em longo papo me incentivando a fazer o mestrado, "você vai tirar de letra!". É Jorge, eu não imaginava que precisaria, além do alfabeto, me valer dos conteúdos aprendidos na graduação, desenvolver e aprimorar habilidades desconhecidas, investindo um precioso tempo na aquisição de novos conhecimentos.
Mas, como foi bom! Me senti como se estivesse acabado de passar no vestibular do Inatel em 1991 tendo um mundo novo a conhecer, caminhos desconhecidos a trilhar e muitas montanhas e rios a transpor.
Mas Deus sempre foi muito generoso para comigo, colocando nas minhas mãos ferramentas poderosas que me capacitassem na aquisição de conhecimentos e habilidades desconhecidas, até então, e pessoas certas nas horas mais improváveis.

Amigos, colegas de sala e de laboratório, obrigado pelas mãos estendidas, pelo compartilhamento e a generosidade em socorrer aquele que precisava de ajuda. Difícil listar todos nomes. E, se me esquecer de alguém, me perdoem. Aos amigos **Victor, Élcio, Tibério, Everton, Thiago, Douglas, José Rodrigo, Karina, Fabão, Luís, ... e muitos outros**, meu eterno agradecimento por confiarem em mim e estarem sempre prontos a me apoiar.
Espera aí, está faltando alguém a quem dedico meu agradecimento especial, ao **Rodrigo Hilario** que com toda paciência, respeito e educação soube me apresentar um mundo cheio de códigos, *if*s, *elses*, *trades* e etc, que me ajudaram a estar aqui hoje apresentando este trabalho, com o qual espero contribuir para a comunidade científica. Obrigado **Rodrigo** por seu apoio e persistência, e tenho certeza de que nossa amizade construída durante este tempo em que trabalhamos juntos, será duradoura. Saiba que poderá sempre contar comigo.

Mas nada disso seria possível sem apoio e incentivo familiar, nas horas em que a vontade era de desistir. Valeu os puxões de orelha, abdicação do lazer em família e momentos de descanso para tornar este dia uma realidade. À minha esposa **Karla Cristina**, meus filhos **Pedro Henrique** e **Anna Luíza**, peço perdão pelas faltas na vezes em que precisavam de mim, por privá-los do convívio prazeroso em família, inclusive nos finais de semanas ensolarados e noites enluaradas que não pudemos apreciar junto. Agradeço do fundo do coração pelo suporte recebido durante todo tempo e por nunca terem duvidado da minha capacidade. Vocês são a razão da minha vida, o combustível da minha lamparina, a força que me impulsiona a buscar desafios e vencer todo e qualquer obstáculo que venha aparecer à frente.

À **minha Mãe Penha** agradeço por toda dedicação, incentivo e apoio ao longo de minha vida, que contribuíram para construir o ser humano ético e responsável que sou. A ela peço desculpas pela privação de minha presença e suporte nos momento em que precisou. **Mãe** obrigado pelo poder das palavras sábias **Força, Fé e Foco (3Fs)** que me fortaleceram e direcionaram na reta final.

Aos meu irmãos **Elton e Esley, suas esposas e meus sobrinhos** sou grato por transmitirem sempre boas vibrações e encorajamento que me alentaram nos momentos de fraqueza. Ao meu **Pai - Zedio**, como gostaria que estivesses conosco para compartilhar esta felicidade que transcende qualquer sentimento de conquista. Tenho certeza de que onde estiver, sempre estará nos protegendo, direcionando e dando forças para nos levantarmos quando cairmos; iluminando nossos caminhos e aplaudindo nossas vitórias. Gratidão, certamente é a melhor palavra hoje.

**"Amo vocês hoje e sempre, incondicionalmente"**.

Bom, e o que falar daqueles que me guiaram no caminho do conhecimento. Seria leviano se dissesse que alguém de vocês foi mais importante que o outro, pois assim como qualquer edificação é formada por diferentes componentes, uns rígidos e outros mais flexíveis, mas quando se unem criam uma robustez no nosso conhecimento, contribuindo assim para o no nosso crescimento profissional e humano. Obrigado **Professores**, por serem construtores de mentes! Agradeço especialmente, aos professores **Nazaré, Brito, Guilherme e Joel**. Não posso deixar fora minha faculdade escolhida, **Inatel**, que desde os meus 12 anos de idade, quando morava no interior do Espirito Santo, já fazia parte dos meus sonhos.
Uai! Mas será que não está faltando agradecer a mais alguém? Falta sim, como esquecer alguém imprescindível!? Pois, ele esteve presente no decorrer de toda as etapas desta jornada, desde a primeira entrevista até a avaliação final, tornando nosso convívio muito maior que professor e aluno, construindo um relacionamento de amizade e confiança, dando conselhos que vão além do ambiente acadêmico, sendo válidos para vida toda. A você **Alberti**, minha profunda gratidão pelos ensinamentos e peço desculpas pelas faltas em todo este tempo.

Não posso deixar de citar pessoas que usando de compreensão e flexibilidade, me permitiram realizar esta graduação de mestrado: A vocês **Paulo** e **Rachid**, muito obrigado. Ao **José Luíz Marques** com palavras sábias e muitas vezes simples que me fizeram repensar a forma de como prosseguir, obrigado por se um incentivador. A **meu time de trabalho**, minhas desculpas pelas faltas e o meu agradecimento pelo incentivo constante, especialmente a você **Gustavo**, por me tirar da zona de conforto.

Aos convidados para banca, **Professor Dr. Marcelo Eduardo Pellenz** e **Professor Dr. Francisco Martins Portelinha Júnior**, agradeço pela apreciação do meu trabalho de Pesquisa e Dissertação de Mestrado que humildemente espero que venha a contribuir para a comunidade científica e meus colegas de jornada.

**A Deus** e **à Maria Santíssima** minha ação de graças por me permitir estar aqui hoje usufruindo desta conquista e vencendo mais este desafio da conclusão do meu trabalho de Dissertação de Mestrado. Rogo para que me concedam a alegria de ainda poder vivenciar muitas outras boas experiências nesta minha jornada terrena.

**PS**: Para fechar com chave de ouro, não posso deixar de incluir neste agradecimento, uma pessoa que aos 47 minutos do segundo tempo entrou em campo para me ajudar. À minha **Madrinha Tia Bete**, muitíssimo obrigado pelos ensinamentos e pelas conversas maravilhosas que tivemos durante a correção desse trabalho. Tenho certeza que saio daqui muito mais rico em conhecimento do que quando iniciamos. Obrigado pela paciência e pelo carinho de sempre.

*Epper Bonomo*

# Sumário

**Sumário** xii

**Lista de Figuras** xiv

**Lista de Tabelas** xv

**Lista de Abreviaturas e Siglas** xvii

**Resumo** xxi

**Abstract** xxiii

**1 Introdução - Desafios do cenário de Internet do Futuro para IoT** 1
- 1.1 Contextualização . . . 1
- 1.2 Contribuições . . . 4
- 1.3 Organização do Documento . . . 5

**2 Fundamentação** 7
- 2.1 Arquitetura de Internet do futuro . . . 7
- 2.2 NovaGenesis (NG) . . . 11
  - 2.2.1 Conceitos básicos NovaGenesis . . . 12
  - 2.2.2 Blocos da NovaGenesis . . . 14
  - 2.2.3 Serviços especializados . . . 15
  - 2.2.4 NovaGenesis para embarcados . . . 16
- 2.3 Tecnologias de comunicações LPWAN . . . 24
  - 2.3.1 Wi-Fi HaLow . . . 24
  - 2.3.2 *Narrow Band IoT* (NB-IoT) . . . 26
  - 2.3.3 LTE *Category M* (CAT-M) . . . 27
  - 2.3.4 *Longe Range* (LoRa) . . . 28
  - 2.3.5 Resumo . . . 33

**3 NovaGenesis com LoRa - Do problema a solução** 35
- 3.1 Desafios para uma rede *Internet of Things* (IoT) na Agricultura . . . 35
- 3.2 Metodologia de validação da hipótese . . . 37
  - 3.2.1 Arquitetura de teste para a prova de conceito (PoC) . . . 37
  - 3.2.2 Definição dos recursos para PoC . . . 38
  - 3.2.3 Plano de teste . . . 41

3.2.4 Implementação . . . . . 43
3.2.5 Experimentação - Teste de validação . . . . . 50
3.2.6 Resumo . . . . . 56

**4 Análise dos dados** **57**
4.1 Resultado das coletas de registros/*logs* . . . . . 57
4.2 Metodologia de análise dos dados . . . . . 58
4.3 Apresentação dos resultados . . . . . 59
4.3.1 Medidas de Perda de Mensagens e Fragmentos . . . . . 60
4.3.2 Mensagens NG Fora de Ordem . . . . . 65
4.3.3 Indicadores de performance de serviço . . . . . 66
4.4 Resumo . . . . . 68

**5 Conclusões e Propostas Para Novas Pesquisas** **69**
5.1 Considerações finais . . . . . 69
5.1.1 Revisão dos objetivos . . . . . 69
5.1.2 Conclusões obtidas . . . . . 70
5.1.3 Sugestões para futuros trabalhos . . . . . 71
5.1.4 Repensando as conclusões do trabalho de pesquisa . . . . . 72
5.2 Reflexão . . . . . 73

**6 Contribuições para a Comunidade Científica** **75**
6.1 Publicações e Premiações . . . . . 75

**Referências Bibliográficas** **77**

# Lista de Figuras


2.1 Serviços e Blocos NovaGenesis. . . . . 12
2.2 Serviços e Blocos EPGS. . . . . 17
2.3 Estrutura de Tarefas NovaGenesis e geração de SVNes. . . . . 18
2.4 Formato da linha de comando NG. . . . . 18
2.5 Formação de mensagens e comandos NG executados pelo EPGS. . . . 20
2.6 Exemplo de linhas de comando NG da mensagem "*Hello*". . . . . 20
2.7 Ciclo de Vida do serviço EPGS. . . . . 20
2.8 Ciclo de Vida do serviço EPGS - Inicialização. . . . . 21
2.9 Ciclo de Vida do serviço EPGS - Exposição. . . . . 21
2.10 Ciclo de Vida do serviço EPGS - Oferta de Serviço. . . . . 22
2.11 Ciclo de Vida do serviço EPGS - Aceitação do Serviço. . . . . 23
2.12 Ciclo de Vida do serviço EPGS - Publicação de Dados. . . . . 23
2.13 Wi-Fi 802.11ah, longo Alcance para IoT. . . . . 25
2.14 Classes de rede para dispositivos LoRa. . . . . 30
2.15 Janelas de transmissão do LoRa. . . . . 30
2.16 Tabela de taxa de dados para LoRa em frequência de 915 MHz. . . . . 31
2.17 Topologia Geral de uma arquitetura LoRa. . . . . 32
2.18 Dimensões das redes LPWAN. . . . . 33

3.1 Plano de trabalho. . . . . 37
3.2 Cenário da NG com LoRa incluindo *Gateway*. A figura mostra outros serviços NG do core, como o PGCS e o NRNCS, ambos parte do núcleo da NG. . . . . 38
3.3 Impactos do LoRa no processo de inicialização da NovaGenesis. . . . 44
3.4 Inclusão da opção de LoRa no EPGS_Controller. . . . . 45
3.5 Inclusão da opção de LoRa no EPGS_Defines. . . . . 45
3.6 Parâmetros de inicialização do PGCS. . . . . 46
3.7 Script de inicialização para NG. . . . . 46
3.8 Macro Fluxo Mensagens NG implementados no Gateway. . . . . 47
3.9 Macro Fluxo Mensagens NG implementados no Gateway (NG => EPGS). . . . . 48
3.10 Macro Fluxo Mensagens NG implementados no Gateway (NG => EPGS). . . . . 48
3.11 Macro Fluxo Mensagens NG implementados no Gateway (EPGS => NG). . . . . 49
3.12 Ambiente de teste em laboratório. . . . . 50

3.13 Recorte do arquivo data.txt na aplicação IoTTestApp da NovaGenesis. 52
3.14 Fluxo de mensagens NG para cálculo do RTT . . . . . 53
3.15 Recorte do arquivo data.txt na aplicação IoTTestApp da NovaGenesis. 54
3.16 Recorte do arquivo data.txt na aplicação IoTTestApp da NovaGenesis. 54
3.17 Recorte do arquivo pós processado do Wireshark™. . . . . 55
3.18 Recorte do arquivo gerado pelo Teraterm com os *logs* de impressão na porta serial do EPGS. . . . . 56
3.19 Recorte do arquivo gerado pelo Teraterm com os *logs* de impressão na porta serial do GW. . . . . 56

4.1 Metodologia de análise dos dados/*logs* coletados. . . . . 58
4.2 Resultado consolidado das análises dos testes válidos realizados. . . . 59
4.3 Perda de mensagens NG, fragmentos e mensagens fora de ordem. . . 60
4.4 Ofensores de Perda de mensagens NG em uma Arquitetura NG sobre uma rede LoRa . . . . . 61
4.5 Cenário de investigação de RF e resultados obtidos. . . . . 62
4.6 Nível de interferência RF no local de teste. . . . . 63
4.7 Detalhamento dos Fragmentos perdidos. . . . . 64
4.8 Perda de mensagens NG, fragmentos e mensagens fora de ordem. . . 65
4.9 *Round Trip Time* (RTT) medido na Aplicação IoTTestApp da NG. . . 67
4.10 Resumo dos resultados de análise de experimento. . . . . 68

5.1 Proposta para projetos futuros de NG utilizando LoRa. . . . . 72

6.1 Certificado de melhor artigo do XIII Workshop de Pesquisa Experimental sobre Internet do Futuro (WPEIF 2022). . . . . 76

# Lista de Tabelas

2.1 Serviços NG . . . . . 15

3.1 Componentes do Cenário de teste. . . . . 38
3.2 Características técnicas ESP-32 e SX1272. . . . . 39
3.3 Recursos de *Software* e *Hardware* para realização de testes da prova de conceito. . . . . 40
3.4 Número de fragmentos de tarefas transmitidos em enlace LoRa. . . . 41

# Lista de Abreviaturas e Siglas

| | |
|---|---|
| **3GPP** | 3rd Generation Partnership Project |
| **ADR** | Adaptive Data Rate |
| **APP** | Application Service |
| **AS** | Autonomo System |
| **BLE** | Bluetooth Low Energy |
| **BPSK** | Binary Phase Shift Key |
| **CAT-M** | LTE Category M |
| **CDN** | Content Delivery Network |
| **CESI** | China Electronics Standarization Institute |
| **CID** | Content Identification |
| **CSS** | Chirp Spread Spectrum |
| **DDOS** | Distributed Denial-of-Service |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DHT** | Distributed Hash Table |
| **DNS** | Domain Name System |
| **DSSS** | Direct Sequence Spread Spectrun |
| **EPGS** | Embedded Proxy Gateway Service |
| **ETArch** | Entity Title Architecture |
| **ETSI** | European Telecommunication Standards Institute |
| **E-UTRA** | Evolved Universal Terrestrial Radio Access |
| **FAO** | Food and Agriculture Organization |
| **FDMA** | Frequency Division Multiplex Access |
| **FI** | Future Internet |
| **FIA** | Future Internet Architecture |
| **FIOT** | Future Internet of Things |
| **FSK** | Frequency Shift Keying |
| **GIRS** | Generic Indirection Resolution Service |
| **GSM** | Global System for Mobile |
| **GW** | Gateway |

| | |
|---|---|
| **HID** | Host Identification |
| **HT** | Hash Table |
| **HTS** | Hash Table Services |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IoT** | Internet of Things |
| **IR** | Indirection Resolution |
| **ISM** | Industrial Scientific and Medical |
| **ISO** | International Organization for Standardization |
| **ITU** | Internatinal Telecomunication Union |
| **LAN** | Local Area Network |
| **LoRa** | Longe Range |
| **LoRaWAN** | Longe Range WAN |
| **LPWAN** | Low Power Wide Area Network |
| **LTE** | Long-Term Evolution |
| **M2M** | Machine to Machine |
| **MAC** | Media Access Control |
| **mMTC** | massive Machine Type Communications |
| **MIMO** | Multiple – ImputsMultiple – Outputs |
| **MTC** | Machine-Type Communication |
| **NAC** | Network Access Control |
| **NAT** | Network Access Translation |
| **NB** | Name Binding |
| **NB-CIoT** | Narrow Band Celular IoT |
| **NB-IoT** | Narrow Band IoT |
| **NID** | Network Identification |
| **NLN** | Natural Language Name |
| **NRNCS** | Name Resolution and Networking Cache System |
| **OFDM** | Orthogonal Frequency Division Multiplex |
| **OFDMA** | Orthogonal Frequency Division Multiplex / Multiple Access |
| **OS** | Operational System |
| **PDU** | Protocol Data Unit |
| **PG** | Proxy Gateway |
| **PGCS** | Proxy-Gateway-Controller Service |
| **PS** | Publish/Subscriber |
| **PSM** | Power Saving Mode |
| **PSS** | Publish/Subscriber Services |

| | |
|---|---|
| **QAM** | Quadrature Amplitude Modulation |
| **RF** | Radio Frequency |
| **RFID** | Radio Frequency Identification |
| **RTOS** | Real Time Operating System |
| **RTT** | Round Trip Time |
| **SDN** | Software Defined Networking |
| **SF** | Spread Factor |
| **SNR** | Signal to Noise Ratio |
| **SHM** | Shared Memory |
| **Shmid** | Shared Memore ID |
| **SID** | Service Identification |
| **SNMP** | Simple Network Management Protocol |
| **SSID** | Service Set Identifier |
| **SVN** | Self-Verifying Name |
| **SVNes** | Self-Verifying Names |
| **TCP** | Transmission Control Protocol |
| **TIC** | Tecnologia da Informação e Comunicação |
| **UMTS** | Universal Mobile Telecommunications System |
| **UN** | United Nations |
| **VM** | Virtual Machine |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |
| **WSN** | Wireless Sensors Networks |
| **XDRX** | Extended Discontinuous Reception |
| **XIA** | eXperssive Internet Architecture |

# Resumo

Bonomo, E. Extensão da NovaGenesis aplicada para cenários de IoT em redes LPWAN (Longa Distância) utilizando Enlace LoRa [dissertação de mestrado]. Santa Rita do Sapucaí: Instituto Nacional de Telecomunicações; 2022.

Esta Dissertação expande trabalhos anteriores visando melhorar a *Future Internet Architecture* (FIA) chamada NovaGenesis (NG) em cenários de *Internet of Things* (IoT), especialmente para aplicações *Low Power Wide Area Network* (LPWAN). A princípio, serão discutidos brevemente os conceitos básicos necessários para o entendimento da NovaGenesis, bem como as características fundamentais da tecnologia de comunicação *Longe Range* (LoRa). Esta Dissertação de Mestrado estende a NovaGenesis para integração com LoRa, atualizando sua versão embarcada, desenvolvendo e configurando os recursos necessários do *Operational System* (OS) e do dispositivo. Em seguida, é proposto um cenário de avaliação experimental definindo uma metodologia a ser aplicada para comprovar os benefícios da NovaGenesis com LoRa para IoT. As evidências coletadas nos testes em laboratório subsidiam e comprovam a viabilidade da implementação de um FIA em uma LPWAN, com baixa capacidade de *throughput* e com possíveis perda de pacotes. Foi avaliado a performance da arquitetura proposta para esta prova de conceito (PoC) e seus ofensores foram identificados, foram validados todas as etapas do Ciclo de Vida do *NÓ* NovaGenesis chamado *Embedded Proxy Gateway Service* (EPGS) garantindo a continuidade do serviço, assim como o nível do serviço entregue pela NovaGenesis à uma aplicação consumidora de dados. Os resultados obtidos dos testes demonstraram a viabilidade de integração de uma FIA NG em uma rede LoRa, onde os elementos da NG se demonstraram flexíveis e transparentes para a arquitetura proposta para comprovar esta hipótese. Até onde sabemos, esta é a primeira vez que o LoRa é integrado a uma FIA, avaliando seu desempenho. Por fim, delimita-se os pontos ainda em abertos para futuros trabalhos e a conclusão deste artigo.

***Palavras-Chave*:** NovaGenesis, Arquitetura de Internet do Futuro, FIA, LPWAN, LoRa, LoRaWAN, IoT, CAT-M, NB-IoT, CCN, MDM, ETArch e XIA

# Abstract

Bonomo, E. Extensão da NovaGenesis aplicada para cenários de IoT em redes LPWAN (Longa Distância) utilizando Enlace LoRa [dissertação de mestrado]. Santa Rita do Sapucaí: Instituto Nacional de Telecomunicações; 2014.

This Master Thesis expands previous works to improve the *Future Internet Architecture* (FIA) called NovaGenesis regarding *Internet of Things* (IoT) scenarios, specially for *Low Power Wide Area Network* (LPWAN) applications. First, the basic concepts necessary to understand NovaGenesis, as well as the fundamental characteristics of the *Longe Range* (LoRa) communication technology will be briefly discussed. This Thesis extends NovaGenesis for LoRa integration, updating its embedded version, developing, and configuring the required Operational System and device resources. Afterwards, an experimental evaluation scenario is proposed in order to prove the benefits of NovaGenesis with LoRa for IoT. The evidence collected from the laboratory tests subsidize and prove the feasibility of implementing a FIA on a LPWAN with low throughput capacity and packet loss. The performance of the architecture proposed for this proof of concept (PoC) was evaluated and its offenders were identified, all stages of the NovaGenesis lifecycle for the IoT node called *Embedded Proxy Gateway Service* (EPGS) were validated, ensuring the continuity of the service, as well as the service level delivered by NovaGenesis to a data application. The results obtained from the tests demonstrated the feasibility of integrating an FIA NG into a LoRa network, where the elements of the NG proved to be flexible and transparent for the proposed architecture to prove this hypothesis. To the best of our knowledge, this is the first time LoRa is integrated with a FIA, evaluating its performance. Finally, the points still open for future work and the conclusion of this article are delimited.

***Keyords*:** NovaGenesis, Future Architecture Internet, FIA, LPWAN, LoRA, LoRaWAN, IoT, CAT-M, NB-IoT, CCN, MDM, ETArch e XIA

# Capítulo 1

# Introdução - Desafios do cenário de Internet do Futuro para IoT

## 1.1 Contextualização

AO longo dos últimos anos, vem-se observando um crescimento exponencial do número de dispositivos capazes de se conectar a Internet, como por exemplo: geladeiras, televisores, lâmpadas, carros, tratores, entre outros. Estudos recentes indicam que mais de 70 bilhões de dispositivos estarão conectados a Internet até 2025 [1, 2]. A *Internatinal Telecomunication Union* (ITU) explorou como o *Internet of Things* (IoT) pode ajudar o mundo a atingir as metas de desenvolvimento sustentável alinhadas aos desafios do *Sustainable Development Goals* (SDG) da *United Nations* (UN) e estimula o desenvolvimento e implementação padronizada dessa tecnologia visando a interoperabilidade entre as diferentes arquiteturas de IoT [3]. Governos e organizações em todo o mundo começaram a sentir a grande importância de construir, controlar e monitorar a infraestrutura de IoT. Entidades como *International Organization for Standardization* (ISO), *Institute of Electrical and Electronics Engineers* (IEEE), *European Telecommunication Standards Institute* (ETSI), *China Electronics Standarization Institute* (CESI) tem se concentrado em alguns aspectos da IoT, como definir políticas, arquiteturas, segurança, privacidade, desenvolvimento de dispositivos e uma camada de comunicação física [4].

A linha de separação entre homem e máquina, que já foi óbvia, está começando a desaparecer pelo enorme papel que as máquinas vem executando em nossas aplicações do dia a dia [5]. Consequentemente, a definição clássica de Internet que foi usada por muitos anos como a rede pública mundial de computadores, não é mais uma descrição clara do que temos presenciado. Computadores não são mais os principais e únicos componentes desta rede — variantes de *hardware* autônomos ou embarcados estão se tornando os componentes dominantes no que é conhecido como coisas (*Things*).

A ITU define de forma clara e abrangente que as coisas não são apenas os dispositivos físicos, mas também os objetos de informação (virtuais) que podem ser identificados e integrados em redes. Na recomendação ITU-T Y.2060 "*Overview of Internet of Things*" [3], aprovada em 2012, define: (a) "*Things*" como um objeto do mundo físico (coisa física) ou a informação (coisa virtual), que é capaz de ser identificado e

integrado na redes de comunicações; (b) IoT foi definida como uma infraestrutura global para a sociedade da informação, permitindo serviços avançados interconectando coisas (físicas e virtuais) com base em tecnologias de informação e comunicação interoperáveis existentes e em evolução; (c) da mesma forma, o dispositivo possui recursos obrigatórios de comunicação e opcionais de detecção, atuação, captura de dados, armazenamento e processamento.

As coisas físicas podem ser detectadas, acionadas e conectadas, enquanto as coisas virtuais (por exemplo, objeto de dados, conteúdo multimídia, software aplicativo) podem ser armazenadas, processadas e transmitidas por meio de redes. As coisas físicas também podem se associar ou serem representadas, por coisas virtuais no mundo da informação, por meio de mapeamento em alguma linguagem, contudo algumas coisas virtuais também podem existir independentemente. IoT não é apenas uma infraestrutura local para interconectar coisas dentro de uma localidade (por exemplo, um prédio, uma empresa ou uma cidade), mas uma infraestrutura global para conectar coisas por meio de redes de comunicação subjacentes interoperáveis. Neste sentido, duas vertentes surgiram com objetivo de ampliar a capacidade da Internet para suportar esta crescente demanda de novos serviços, impulsionados pela IoT.
A ***primeira*** é baseada na evolução da Internet atual, que utiliza estrutura dupla de protocolos com o IPv6. Esse caso, cobre cenários IoT onde energia e capacidade dos dispositivos são abundantes.
Para atender aos requisitos de eficiência energética, recursos computacionais limitados e a escalabilidade em cenários IoT, uma versão otimizada denominada *IPv6 over Low-Power Wireless Personal Area Networks* (6LoWPAN) [6] foi implementada.
Esse caminho da pilha dupla carrega em sua essência, limitações que dificultam a evolução da Internet, tais como: (a) **nomeação e resolução de nomes limitada**; (b) **falta de auto-organização**; (c) **desacoplamento de identificadores e localizadores** autoverificáveis; dentre muitas outras [7].

Sempre paira a questão de até onde esta arquitetura suportará ou será flexível o suficiente para receber novos serviços e garantir a segurança dos dados, informações e usuários.
Por estes e outros motivos, um ***segundo*** caminho de pesquisa foca em desenvolver novas arquiteturas do zero, por meio de um conceito chamado "*Clean Slate*". Estas novas arquiteturas levam em consideração os aprendizados anteriores, os serviços conhecidos e a preparação para outros serviços ainda não populares ou a serem inventados.

Ambos os caminhos são denominados de ***Future Internet*** **(FI)**.

Existem importantes projetos de propostas para novas arquiteturas que buscam atender a este repensar da Internet, denominados de *Future Internet Architecture* (FIA). Dentre elas podemos destacar:

*a*) a ***Named Data Networking*** **(NDN)** [8] uma evolução da *Content Centric Network* (CCN) [9] que trabalha com armazenamento de conteúdo e mapeamento do caminho para devolver os dados desejados pelo solicitante, do ponto mais próximo e pelo seus nomes;

*b*) a ***Entity Title Architecture*** **(ETArch)** [10] é um projeto Brasileiro que propõe uma arquitetura baseada em roteamento por títulos, separando os planos de controle e dados, criando ambientes seguros de comunicação entre entidades (deno-

minado *workspace*), que controla todo o ciclo de vida;

*c*) a ***eXpressive Internet Architecture*** **(XIA)** [11, 12] é uma arquitetura iniciada pela Universidade de "Carnegie Mellon" com uma proposta para melhorar radicalmente a capacidade de evolução e a confiabilidade da Internet. Para atingir esse objetivo, a XIA define uma única rede que oferece suporte inerente para comunicação entre vários *principals*, incluindo *hosts*, conteúdo e serviços, podendo acomodar entidades futuras desconhecidas. O design da XIA é baseado em uma cintura estreita como a Internet de hoje, mas com capacidade de evoluir para: ***acomodar*** novos modelos de uso de aplicativos e *incorporar* tecnologias aprimoradas de ***link***, armazenamento e computação à medida que surgem. A XIA também foi projetada em torno do princípio central da segurança intrínseca, no qual a integridade e a autenticidade da comunicação são garantidas; e

*d*) a ***NovaGenesis (NG)*** [7, 13] é uma arquitetura desenhada e proposta em 2008 por Antônio Marcos Alberti, et al., pesquisador do Inatel - Instituto Nacional de Telecomunicações. É uma arquitetura projetada do "Zero", que integra redes e nuvem com o objetivo de criar um ambiente essencial para troca, processamento e armazenamento de informações. A NG é composta de um sistema distribuído e orientado a serviços que utilizam: nomeação, ligações de nomes, resolução de nomes, contratos, *cache* de rede e controle de ciclo de vida, que satisfazem as necessidades e requisitos de serviços emergentes, incluindo implementação em *software* de protocolos que garantem uma maior escalabilidade e segurança.

Em uma diversidade de cenários para IoT, onde centenas de dispositivos são distribuídos em qualquer lugar e a diferentes distâncias. Não é possível pensar em uma arquitetura sem usar comunicações sem fio e dispositivos equipados com: (a) Sensores; (b) Componentes de *Radio Frequency* (RF); (c) Atuadores; (d) Com circuitos construídos em blocos ou isolados; (e) Tendo características específicas ou genéricas, dependendo da aplicação; e (f) Componentes de micro-controlador. Estes dispositivos constituem um nó em uma rede de sensores sem fio, também conhecida como *Wireless Sensors Networks* (WSN) [14].

Diversas tecnologias de comunicações sem fio habilitam as redes IoT para diferentes cenários. Pode-se classificar estas redes de acordo com o seu alcance (curta ou Média/longa distância) e sua regulamentação de frequência, sendo elas **licenciadas** que obrigatoriamente precisam ser liberadas pelo órgão regulador, por exemplo Agência Nacional de Telecomunicações (Anatel) ou **não licenciada** onde o espectro é definido, contudo seu uso não exige liberação pelo órgão regulador. Também podem ser encontradas em algumas literaturas tecnologias celulares e não celulares.

Em curtas distâncias, visando atender aplicações como varejo, saúde, rastreamento *indoor*, casas inteligentes, são identificados sensores conectados por redes Wi-Fi (802.11a/b/g/n) [15], *Bluetooth Low Energy* (BLE) [16] e Zigbee (802.15.4) [17]. Um dos fatores e requisitos para a escolha da tecnologia a ser utilizada está associada a disponibilidade de recursos energéticos dos dispositivos finais sendo que, em grande parte dos sensores utilizando Wi-Fi necessitará de fonte de energia externa, enquanto para o BLE e Zigbee utilizam preferencialmente baterias. As tecnologias de curto alcance são regulamentadas por órgãos competentes, contudo não exigem licenciamento para sua utilização e são consideradas como não celulares.

Quando se pensa em cenários de longos alcances para IoT, dois grandes grupos se destacam: ***um*** ao qual não se requer licenciamento do uso de frequência, como exemplo, LoRa [18], SigFox [19] e Wi-Fi Halow (802.11/ah) [20], também consideradas como não celulares; e um ***segundo*** que dependem de licenciamento de órgãos competentes para sua utilização, onde se destacam o *Narrow Band IoT* (NB-IoT) [21] e LTE *Category M* (CAT-M) [22]. As tecnologias celulares NB-IoT e o CAT-M, disponibilizadas pelo *3rd Generation Partnership Project* (3GPP), utilizam infraestrutura da rede móvel LTE existente, que possuem protocolos mais simples melhorando a eficiência energética dos dispositivos finais, aumentando a vida útil das baterias e garantindo um melhor controle do uso de espectro, uma vez que utilizam frequências licenciadas. Estas redes também são conhecidas como rede de longo alcance com baixo consumo de energia ou simplesmente *Low Power Wide Area Network* (LPWAN).

As FIA usufruem destes meios de comunicações atualmente disponíveis, sejam eles em sua forma primitiva ou com adequações baseadas em redes sem fio.

## 1.2 Contribuições

Até onde vai nosso conhecimento, embora existam muitas pesquisas e desenvolvimentos relativos a IoT, a falta infraestrutura aberta e acessível para uma adoção mais ampla da IoT em diferentes cenários de abordagem utilizando FIA. Com o intuito de expandir a abrangência da FIA em cenários de IoT que demandam extensas coberturas, como por exemplo o agronegócio, redes de monitoração inteligentes, cidades inteligentes, etc., essa Dissertação de Mestrado propõe a implementação integral da FIA NovaGenesis utilizando uma comunicação por uma rede *Longe Range* (LoRa), conectando os dispositivos IoT ao núcleo da rede NG. Trabalhos anteriores provaram em laboratório a viabilidade de implementar uma versão reduzida da NG para dispositivos embarcados [7], voltados a aplicações de IoT, em ambiente com disponibilidade de banda, baixa latência e comunicação em via dupla utilizando Ethernet e Wi-Fi. Nesta Dissertação de Mestrado, expandimos este conceito para um ambiente onde o tempo em que os dados permanecerão no ar (*Time on Air*), pode influenciar na comunicação em longas distâncias e com perda de pacotes, podendo atender aos desafios da agricultura para melhorar a eficiência da produção visando alimentar a população mundial, como será abordado a frente. Nos próximos capítulos serão abordadas as principais características da arquitetura NG, assim como do LoRa, e os desafios de uma implementação conjunta, bem como os resultados obtidos em laboratório que comprovaram sua viabilidade inicial e suas oportunidades de ampliar ainda mais as funcionalidades suportadas pela NG.

As principais contribuições desse trabalho são:

*a*) Desenvolvimento da arquitetura NG com LoRa para conectividade de IoT;

*b*) Aprimoramento do serviço embarcado NG chamado *Embedded Proxy Gateway Service* (EPGS) para executar em dispositivos ESP-32 LoRa;

*c*) Preparação do sistema operacional RTOS para execução do EPGS;

*d*) Aprimoramento da aplicação IoT NG (IoTTestApp) para funcionamento em conjunto com o EPGS LoRa;

*e*) Desenvolvimento de um *Gateway* LoRa para Wi-Fi e vice-versa, visando comunicação com os serviços do núcleo NG e IoTTestApp.

## 1.3 Organização do Documento

O restante desta Dissertação de Mestrado é organizada como segue: No **Capítulo 2** são apresentados as arquiteturas objeto desta hipótese que serão integradas, no **Capítulo 3** são abordados os principais desafios de se integrar a NG em uma rede LoRa utilizando plataformas abertas pra desenvolvimento e as grandezas desejadas a serem medidas em laboratório. Uma metodologia de teste foi definida para guiar os passos a serem seguidos, com objetivo de obter o maior número de amostras que pudesse subsidiar a hipótese deste trabalho. Nesta prova de conceito foi utilizada o ESP-32 LoRa da *Heltec Automation*. Os resultados obtidos baseados em registros/*logs* e trocas de mensagens na rede Ethernet coletados por ferramentas de monitoração são apresentados no **Capítulo 4** e mostraram um excelente desempenho da NG em uma rede LoRa com perda total próxima de 4% para um volume expressivo de publicações de medições de temperatura em uma arquitetura bastante complexa. Foram identificados os principais ofensores de perda neste cenário, sendo que a NG e o EPGS demonstraram excelentes resultados. O **Capítulo 5** encerra essa Dissertação de Mestrado, delimitando os pontos em aberto para futuros trabalhos e apresentando as conclusões e contribuições para o Estado da Arte, expandido a abrangência da arquitetura FIA NovaGenesis em cenários IoT de longa distância utilizando redes LoRa. O **Capítulo 6** adiciona informações sobre artigos relacionados a esta Dissertação de Mestrado.

# Capítulo 2

# Fundamentação

ESTE capítulo divide-se em três partes: a primeira, faz uma introdução à FIA e seus principais desafios; a segunda parte, apresenta em detalhes a NovaGenesis, uma FIA que será objeto desta Dissertação de Mestrado. A terceira parte detalha as principais rede LPWAN apresentando suas características destacando a LoRa que suportará a FIA NG.

Os desafios para esta integração são apresentados no próximo capítulo.

## 2.1 Arquitetura de Internet do futuro

A arquitetura atual da Internet está baseada em uma pilha de protocolos que possui o IP como ponto de estreitamento, desenhada há 40 anos para atender a uma demanda de comunicações pontuais entre computadores e servidores.

Nos dias atuais, a Internet tem um papel importante na sociedade, onde podemos notar seu uso em meios operacionais, financeiros, de pesquisas entre outros. Porém, para atender a crescente demanda baseada em serviços, a arquitetura atual IP apresenta desafios relacionados à: endereçamento, mobilidade, segurança, confiabilidade da rede e disponibilidade dos serviços, diagnóstico de problemas e gerenciamento de rede, qualidade de serviço, escalabilidade, modelo econômico e liberdade de inovação [23].

O endereçamento IP é apontado como um dos principais desafios de uma Internet do futuro, dado que possuem princípios em desacordo com os requisitos atuais, como por exemplo a escassez de endereços e a semântica, acumulando funções de identificação e localização. O problema de escassez até foi tratado por mais uma adaptação na estrutura atual, com o aumento do número de bits que compõe o endereçamento, de 32 para 128, surgindo assim o IPv6 [24]. Com o aumento significativo da quantidade de IPs, se resolve esta questão de limite de entidades a serem identificadas, mas continua a apresentar em sua estrutura a semântica dupla. Contudo, a não interoperabilidade entre o endereçamento atual IPv4 e IPv6 dificultam a adoção do mesmo nas redes atuais, por exigir um elevado investimento, fazendo com que sua adoção seja de forma muito lenta. Além desta técnica, a implementação de funções como *Dynamic Host Configuration Protocol* (DHCP) e *Network Access Translation* (NAT) também ajudaram a sobrevida da Internet atual com o IPv4 uma vez que trazem mecanismos de otimização

dos endereços disponíveis. Porém, quando se analisa a função do NAT, ele fere um dos princípios definidos da Internet para comunicação fim a fim [25, 26].
A forma de endereçamento e nomeação adotada na Internet, abre oportunidade para que uma estação possa se passar por outra simplesmente com a clonagem do endereço IP, criando brechas de segurança. É necessário que as novas redes tenham condições de preservar a privacidade do usuário e implementar métodos de autenticação seguros para os dispositivos.

Espera-se que, nos próximos anos, haja um crescimento no número de dispositivos conectados, também impulsionados com a integração dos celulares à Internet. Segundo a previsão do ITU-R estima-se cerca de 17 bilhões de assinaturas de serviço móveis em 2030, sendo 70% impulsionado por *smartphones* e os demais por *tablet* ou *smart devices* [27]. Outro ofensor também são os dispositivos *Machine to Machine* (M2M) que tendem alcançar um total de 97 bilhões de assinaturas até 2030.

Este crescimento de dispositivos móveis, impulsionado pela necessidade de mobilidade dos usuários, fere [23] a forma definida no projeto original da Internet baseada no princípio de comunicação *host* a *host*. A conexão imediata passa a ser comprometida, dado que estes dispositivos não terão mais localização fixa, pois mudam de identificação a cada mudança de rede, domínio ou pontos de acesso. Isso acontece, pois a cada mudança um novo endereçamento é atribuído levando a perda da conexão. A perda de conexão também pode ocasionar outro problema que é a dificuldade do *Trasnmission Control Protocol* (TCP) identificar com precisão o real motivo de uma perda de pacote, por exemplo, por falha na transmissão, colisão na tratativa de acesso ao meio e quebra da conectividade devido a mobilidade, tendo que alterar a janela de congestionamento sempre que uma perda é detectada [28].

A preocupação com os aspectos de segurança tem sido cada vez mais demonstrada pelos usuários, provedores de serviços, indústrias e desenvolvedores de aplicações. Segundo relatório da Cisco [29] globalmente o número de ataques cresceu 776% entre 100 Gbps e 400 Gbps comparando 2018 e 2019, e é esperado um número de *Distributed Denial-of-Service* (DDOS) de 15.4 milhões em 2023. Uma das principais causas da ausência de segurança na arquitetura atual é que, a mesmas foram criadas inicialmente para atender a demandas de usuários confiáveis em uma rede restrita, onde não se requeria mecanismos para proteger a infraestrutura. Com a comercialização da Internet e a participação de milhares de usuários, esta ameaça ficou mais latente seja por usuários maliciosos ou aqueles que não possuem conhecimento técnico adequado para manter suas máquinas atualizadas, podendo estas serem elementos alvos para iniciar um ataque a rede ou até mesmo ser um disseminador de vírus em uma rede [30].

Os problemas de segurança não se restringem apenas aos usuários. Elementos de rede também são susceptíveis a ataques, pois os protocolos de roteamento não possuem premissas de segurança forte. Assim como mecanismos de autenticação e monitoração permitem que ataques passem a ser mais frequentes também em redes de operadoras, tal como noticiado em [31, 32]. Isso demonstra que a segurança deve permear todas as camadas da arquitetura da rede. Um modelo de reputação pode ser uma ferramenta fundamental para punir ou premiar uma entidade de acordo com suas atitudes, segundo [33] este mecanismos é denominado como “Responsabilização”. A utilização de *Firewall* ajuda na prevenção da chegada de tráfego indesejado a clientes, mas não

consegue proteger a rede.

De acordo com o relatório anual publicado pela Nestscout em 2021 [34], no primeiro semestre de 2021 houve aproximadamente 5,4 milhões de ataques do tipo DDOS, cerca de 11% a mais em relação ao mesmo período do ano de 2020 com um tempo médio de 50 minutos de duração. Os principais alvos destes ataques nas redes estão relacionados aos vetores, *Domain Name System* (DNS), sincronismo de TCP e conexões de *Virtual Private Network* (VPN) . Estes ataques só não tiveram consequências maiores, porque empresas especializadas em planos de defesa buscam criar soluções de mitigação para reduzir ou até mesmo eliminar os impactos. O sucesso de um ataque na rede pode representar a indisponibilidade do serviço para algumas centenas de milhares de usuários.

Alguns dos métodos utilizados para impactar os serviços estão relacionados ao sequestro de dados por meio de encriptação de dados (*Data Encryption*), onde os atacantes exigem pagamento para fornecer a chave de descriptografia, outro método coloca a vítima em dupla extorsão, pois além de roubar os dados da vítima, também bloqueiam o serviço até que pague, podendo até ter seus dados expostos ou vendidos (*Data Theft*). Para dificultar ainda mais a restauração do serviço, adicionam aos anteriores um ataque de DDOS.

Existe um consenso de que a segurança deve permear todas as camadas da arquitetura da Internet para que se obtenha um ambiente mais seguro. Neste contexto, de acordo com [23], os requisitos de tratamento dos ataques de negação de serviço, autenticação dos usuários e dispositivos de forma eficiente, indicam que a criação de um sistema de confiança e um sistema de responsabilização são pontos chaves a serem considerados em uma nova arquitetura de Internet. A autenticação de usuários, assim como o acesso aos dispositivos são grandes brechas para invasão, dado que muitos dos dispositivos permanecem com seus usuários e senhas de rede padrão ou em formato de fácil descoberta, passando a ser alvo que favoreça o início de um ataque. Câmeras, dispositivos IoT, roteadores, ou qualquer elemento conectado a Internet são dispositivos elegíveis por atacantes mal intencionados [34].

Outro ponto importante na arquitetura da rede atual é a entrega dos serviços que demanda um elevado grau de confiabilidade e disponibilidade. Por exemplo, a rede telefônica disponibiliza nível de serviço acima de 99,9%. Apesar de a Internet ter sido desenhada com mecanismos de roteamento que tratassem falhas de enlace aumentando assim sua disponibilidade, segundo estudos realizados por [35] e relatórios do Gartner e Cisco, estima-se que a indisponibilidade de serviço na rede chegue a 40% [29]. Uma arquitetura que entregue níveis de serviço adequados às demandas das aplicações existentes e as novas que venham a surgir passam a ser um desafio na implantação de uma nova Internet.

A manutenção e o gerenciamento da Internet atual é algo complexo e trabalhoso por não possuir ferramentas adequadas que proporcionem visibilidade dos problemas de rede para uma rápida atuação. O protocolo de gerenciamento *Simple Network Management Protocol* (SNMP), criado na década de 80 é o mais conhecido. Contudo, sua utilização fica mais restrita a monitoração de dispositivos de rede, deixando aberto problemas de gerenciamento de aplicações. Dado que os usuários de rede não possuem conhecimentos técnicos suficientes para identificar problemas, a ausência de mecanis-

mos de diagnósticos e correção de erros levam a um elevado número de reclamações. A existência de mecanismos que possibilitem a autoconfiguração da rede por meio de políticas e restrições administrativas pré-definidas, assim como a autonomia devem ser conceitos importantes para uma Internet do Futuro. Para tal, a separação dos planos de controle e dados [23] são defendidos por pesquisadores. Ter mecanismos que possibilitem a garantia da qualidade do serviço prestado *Quality of Service* (QoS) em uma dimensão global é um ponto chave para o sucesso de uma nova arquitetura, dado que a Internet atual está baseada no princípio do "*best effort*" e que qualquer implementação para garantia da qualidade do serviço fim a fim, requer acordos entre os diferentes *Autonomo System* (AS).

O crescimento exponencial do número de estações e dispositivos conectados a Internet, assim como o aumento pela demanda de aplicações como: vídeo, streaming e outros, vêm exigindo cada vez mais a abertura das tabelas de roteamento para levar ao usuário uma melhor experiência, assim como a utilização de soluções de distribuição de conteúdo por meio de *Content Distribution Network* (CDN). Contudo, o aumento de entradas na tabela de roteamento para atingir um elemento da rede torna-se ineficiente tanto no roteamento quanto no mecanismos de mobilidade. Pensar em uma nova arquitetura de Internet que não seja mais centrada no *host* e sim na informação (conteúdo, dado ou serviço), faz com que a mesma se abstraia da rede e se preocupe em alcançar a informação desejada, independente de sua localização, podendo até estar armazenada em um ou mais pontos da rede, levando a uma melhor experiência e qualidade de serviço e garantindo a credibilidade da informação.

Segundo o autor de [23], outro fator que também deve ser considerado em uma FIA é um modelo econômico flexível e que proporcione uma liberdade de evolução. Isso porque, a Internet atual não permite a um provedor de serviço ter a visão e gestão fim a fim de seu cliente, a não ser que o mesmo esteja dentro do seu domínio. Isso dificulta a implementação de serviços diferenciados, alinhando as expectativas de serviço dos clientes e à remuneração adequada dos provedores, dado que hoje se restringem a simplesmente encaminhar pacotes de serviços básicos e prover banda. Implementações de serviços como *caching*, segurança, qualidade de serviço, entre outros são oferecidos pelos provedores de serviço, contudo ferem o principio e conexão fim a fim além da premissa da inteligência nas extremidades.

Mecanismos que proporcionem a capacidade de mudar e evoluir a tecnologia de rede [26] com as características desejadas passam a ser elementos fundamentais em uma FIA, dando liberdade e autonomia aos provedores de serviços, reguladores e aos clientes em trocar e comercializar os dados, criando assim um modelo econômico impulsionado pela IoT. Na Internet atual podemos identificar alguns atores, importantes geradores de conflito: o cliente que quer trocar dados; o provedor de serviço que deseja ter lucros sobre sua infraestrutura; o governo que precisa aplicar leis que protejam e regulamente o comércio; empresas de direitos autorais que desejam proteger seu conteúdo; provedores de conteúdo que buscam lucro; entre outros. Para atender a estes requisitos econômicos e flexibilidade de inovação, adoção de técnicas de virtualização passa a ser elemento fundamental nesta nova arquitetura [36].

As melhorias necessárias a serem implementadas na arquitetura de Internet não estão concentradas em um único tópico ou ponto específico. Analisando de forma

isolada, pode-se seguir por implementações pontuais para resolver tópicos, por meio de adaptações da arquitetura atual. Contudo, não se tem algo limpo e escalável, não blindado para o futuro devido a uma visão míope das futuras demandas. O redesenho da arquitetura atual torna-se imprescindível para que se tenha mecanismos e meios de atender novas demandas de forma fácil e sem impacto, sendo esta flexível para receber novos serviços ainda não conhecidos. Por meio das lições aprendidas na arquitetura atual foi possível identificar os pontos que precisam ser cobertos em uma FIA, como abordado nos parágrafos anteriores.

Outro ponto importante a ser ressaltado, é a necessidade de experimentação em larga escala destas FIA, validando assim em ambiente controlado, sua viabilidade e capacidade de suportar novos serviços. Um ambiente de teste (*testbed*) que possa suportar estas arquiteturas torna-se imprescindível para que pesquisadores de todo mundo implementem e validem estas proposições.

Os esforços empreendidos pelos pesquisadores em desenvolver FIA podem ser classificadas em diferentes aspectos, sejam por sua abordagem técnicas ou diversidade. Algumas delas focam em buscar soluções pontuais para problemas conhecidos, porém por outro lado existem arquiteturas que buscam implementar em uma forma mais ampla, conceitos abrangendo todos os tópicos que uma nova arquitetura necessite, como já citado acima.

Dentro desta análise, podemos identificar significativos projetos ao redor do mundo, principalmente nos EUA, Europa, Ásia e Brasil, que trazem em seu desenho soluções inovadoras, quebrando paradigmas com implementações diferentes do que hoje existe em uma cintura estreita da Internet atual. Ou seja, arquiteturas desenvolvidas do zero, como se a Internet nunca existisse, também conhecidas como "*Clean Slate*", contudo, levando como base as necessidades já identificadas pelo mercado atual e prevendo em seu núcleo características flexíveis para suportar e resolver novos serviços ainda não conhecidos.

## 2.2 NovaGenesis (NG)

A NovaGenesis traz em sua essência o repensar da Internet levando em consideração as lições aprendidas desde a implementação da Internet atual na década de 70, onde a rede desenvolvida pela ARPANET tinha como objetivo a comunicação entre *hosts* para fins militares [37]. Com sua abertura para as entidades acadêmicas na década de 90 e em seguida para o mercado, sua estrutura inicial foi sendo adequada aos novos serviços emergentes, em especial impulsionados pela Web, comunicação social e *streaming*. Estas adequações, dificultam a evolução da Internet atual, pois carregam problemas estruturais desde a sua concepção e implementações originais.

O repensar da Internet pela ótica da NovaGenesis leva em consideração os aprendizados da Internet atual. Esta arquitetura é o resultado de uma extensa pesquisa realizada nos requisitos de iniciativas de FI, tecnologias e mudanças com uma expressiva relevância no cotidiano da sociedade atual, incluindo em sua estrutura a capacidade de ser flexível o suficiente para suportar novos serviços emergentes. A NG é formada por um conjunto de sistemas distribuídos onde qualquer tratamento ou troca de informação

é considerada como um serviço, sendo portanto uma arquitetura centrada em serviços.

A NovaGenesis reúne em uma única arquitetura características [38, 39] que possibilitam sua convivência com as redes legadas, assim como outras arquiteturas que venham a surgir. É estruturada em três camadas com funções bem definidas [7,40,41]: a camada *Convergence Layer*, é responsável pela comunicação entre serviços internos da própria NG, ou quando fora, adaptar as mensagens a serem enviadas para a camada de enlace; na camada *NovaGenesis Layer* estão os serviços especializados; e na camada *Application Layer* as aplicação são implementadas. A Figura 2.1 ilustra as camadas definidas acima.

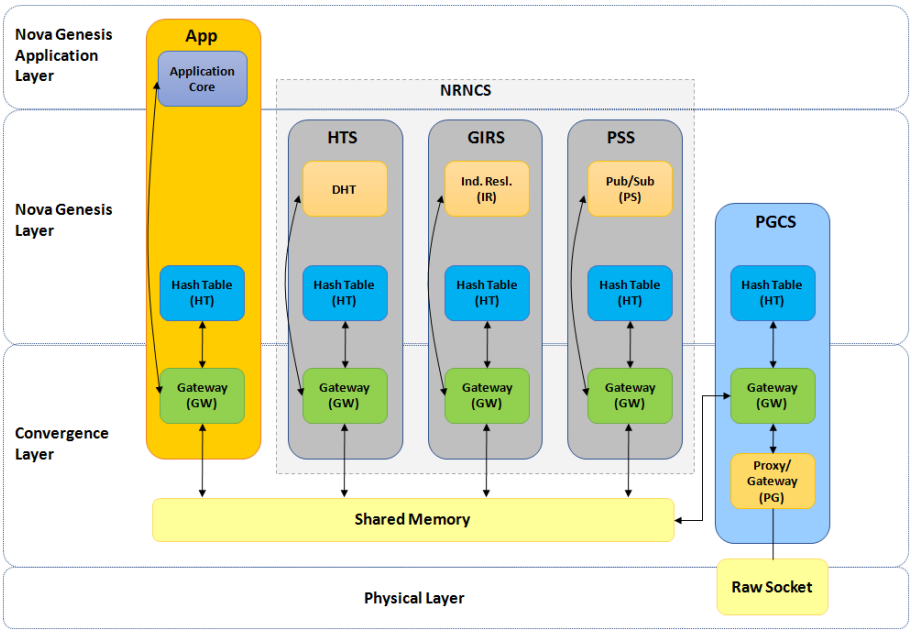



Figura 2.1: *Serviços e Blocos NovaGenesis.*
Fonte: Baseada na Dissertação de Mestrado de Thiago Bueno da Silva, Figura 2.9, NovaGenesis Control Agent for Future Internet eXchange Point.

## 2.2.1 Conceitos básicos NovaGenesis

Antes de evoluir na estrutura da arquitetura NG, faz-se necessário definir os conceitos básicos e princípios [38] em que a NG se baseia. Dentre eles destacam-se, como a NG trata a identificação e localização, nomeação e ligações de nomes, mobilidade, auto-organização, segurança, rastreabilidade, entre outros. Nesta subseção, serão explorados alguns conceitos básicos que apoiarão o decorrer desta dissertação.

### 2.2.1.1 Nomeação

O nome é uma forma de denotar uma existência [7] e pode carregar ou não um significado. A NG suporta tanto nomes em seu formato natural, *Natural Language Name* (NLN), ex.: carro, casa, etc, como também nomes sem significados para humanos, denominados de "Nomes Planos", ex.: um número hexa decimal.

Os nomes planos são originados a partir de um NLN utilizando uma função *hash*. Estes nomes gerados a partir de um NLN são denominados *Self-Verifying Name* (SVN). Um nome pode ser denominado como SVN pois uma vez passado pela função *hash*, é possível retornar a sua informação original. A NG utiliza o algorítimo "MurMurHash3" para geração dos *Self-Verifying Names* (SVNes) [7].

#### 2.2.1.2 Ligação de nomes e Resolução de Nomes

Uma Ligação de Nomes, *Name Binding* (NB), é um mapeamento entre dois ou mais nomes na forma [7, 38]: $<$ chave; valor(es) $>$. Nesta forma de denotação é possível indicar que uma entidade "chave" contém o(s) "valor(es)" ou os "valor(es)" estão contidos na "chave", contribuindo assim para a localização da entidade.

Na NG uma "**Entidade**" designa a existência física e virtual que tem função de lidar com informações ou dados. A resolução de nomes está associado em encontrar os nomes associados a uma chave.

#### 2.2.1.3 Identificação e Localização

Um dos grandes problemas da arquitetura atual é que o IP carrega em um único identificador a informação de identificação do dispositivo e sua localização para um mesmo segmento de rede. A NovaGenesis propõe em sua arquitetura a separação de ID/Loc [7, 42], sendo um "Nome" para representação da identificação da entidade e outro para sua localização. Esta separação possibilita que um dispositivo mude de localização sem perder sua identidade. Desta forma, abrangendo qualquer entidade, seja ela um *hardware*, um sistema operacional, um processo, conteúdos e até *hosts*.

Na NG, uma Ligação de Nomes NB [7, 42] é feita entre o identificador e o localizador a fim de conectar a identificação e a localização de uma entidade. Por exemplo, um dispositivo IoT pode usar o seu próprio nome (número de série, código de barras, etc) como identificador (Id), e uma posição de coordenada geográfica como localizador (Loc), ou seja $<$"Cord. Geográfica"; "Número de Série"$>$.

#### 2.2.1.4 Mobilidade

A NovaGenesis suporta mobilidade pela verificação de nomes. Em toda mudança de localização os serviços são notificados de alterações de NB e suas ligações de nomes são atualizadas, assim proporcionando que serviços encaminhem ou roteiem mensagens para destinos consistentes sem a perda da conexão, dado que a identificação do dispositivo é mantida [7, 42]. A independência de Identificador e Localizador permite que uma entidade possa ser encontrada mesmo em cenários com mobilidade dos dispositivos.

#### 2.2.1.5 Encaminhamento e Roteamento

O roteamento e encaminhamento na NG são baseado em nomes, *Name Based Routing* (NBR) [7,42]. Utilizam os SVNes expostos para obter informações de identificação e localização de existências, roteamento, topologia de rede, estado de enlace, congestionamento e demais necessidades. Toda entidade é identificada por resultado de função

*hash* autoverificável. A tupla formada pelos SVNes dos identificadores do hardware, sistema operacional, processo e bloco é utilizada para identificar unicamente o destinatário. Quando um *NÓ* é introduzido na rede NG, ele obrigatoriamente deve enviar uma mensagem de *Hello*.

### 2.2.2 Blocos da NovaGenesis

A estrutura da NG é formada por blocos com funções bem definidas utilizadas na comunicação entre entidades. Para um melhor entendimento da NG serão definidos nas próximas subseções os elementos básicos que compõem as funções da NG.

#### 2.2.2.1 *Shared Memory* (SHM)

Funciona como um barramento de comunicação, sendo utilizado pelos serviços internos em um mesmo *Operational System* (OS) para trocar mensagens [7].

#### 2.2.2.2 *Gateway* (GW)

É um componente interno dos serviços da NG que interage diretamente com a memória compartilhada, SHM, do OS. Todas as mensagens trocadas internamente pelos serviços num mesmo OS, *Virtual Machine* (VM) ou *container* são realizadas na SHM [7].

#### 2.2.2.3 *Hash Table* (HT)

É um componente interno que armazena qualquer tipo de ligações entre nomes, i.e. NB [7]. Ela fornece um repositório para armazenamento interno de ligações locais para os processos realizarem suas ações. Exemplo, registrar os SVNes do *peer* de cada bloco individual.

#### 2.2.2.4 *Distributed Hash Table* (DHT)

Armazena as ligações entre nomes, em linguagem natural e auto-verificável, pertencentes as entidades da rede representadas por serviços publicados e assinados, em um domínio. As ligações são distribuídas de acordo com uma chave binária [7]. Durante a publicação de uma ligação de nomes são definidos quais outros serviços estão autorizados a serem assinado.

#### 2.2.2.5 *Indirection Resolution* (IR)

É um bloco pertencente ao serviço *Generic Indirection Resolution Service* (GIRS) que realiza ações específicas. É responsável por decidir qual a HT mais apropriada para armazenar as ligações entre nomes [7].

#### 2.2.2.6 *Publish/Subscriber* (PS)

É um bloco que propicia o encontro, *rendezvous*, entre os (*Publishers*) e os (*Subscribers*) habilitando-os a realização de contratos entre as partes de forma segura [7].

#### 2.2.2.7 *Application Core - App*

É o bloco onde é propriamente implementada a aplicação *core* da NovaGenesis [7].

### 2.2.3 Serviços especializados

Os serviços especializados da NG seguem uma estrutura padrão com a combinação de alguns dos blocos definidos anteriormente e formam o núcleo da NovaGenesis.
A Tabela 2.1 a seguir, reúne os blocos de função para cada serviço especializado da arquitetura NG que serão explorados nesta subseção.

| Função | App | HTS | GIRS | PSS | PGCS |
|---|---|---|---|---|---|
| App | X | | | | |
| DHT | | X | | | |
| IR | | | X | | |
| PS | | | | X | |
| PG | | | | | X |
| HT | X | X | X | X | X |
| GW | X | X | X | X | X |

Tabela 2.1: *Serviços NG*

#### 2.2.3.1 *Hash Table Services* (HTS)

O HTS é responsável por armazenar os NB e seus conteúdos associados, caso existam. Em um caso hipotético, onde um sensor esteja publicando medições de temperatura, este conteúdo é armazenado em um arquivo na pasta do componente HTS no Linux. Este arquivo quando submetido a uma função *hash* pode gerar SVN, onde a combinação deste identificador com o nome do arquivo gera o NB [7, 38, 42]. Os NBs gerados são organizados por categorias na estrutura do HTS visando permitir maior escalabilidade. Estes NBs estão separados em dois grupos: **um** que reage a estímulos de entrada, intermediário ou de saída, denominado de *Passive Digital Inhabitant* (PDI) e **outro**, que está associado a estímulos ou comandos vindos de processos ou aplicativos que são denominados de *Active Digital Inhabitant* (ADI) [38].

#### 2.2.3.2 *Publish/Subscriber Services* (PSS)

O PSS é um serviço da NG que cria um ambiente de encontro, "*rendezvous*", de publicadores e interessados em assinar os conteúdos. Permite a publicação e assinatura de conteúdo por meio de ligação entre nomes [7, 38, 42]. O PSS armazena quais serviços estão pré-autorizados a acessar os NB possuindo seis primitivas: (a) publicar um NB/dados; (b) publicar NB/dados e notificar outros serviços; (c) assinar um NB/dados; (d) assinar um NB/dados e notificar os outros serviços; (e) entregar uma assinatura de NB/dados; e (f) revogar um NB/dados publicado.

#### 2.2.3.3 *Generic Indirection Resolution Service* (GIRS)

O GIRS é um serviço intermediário entre o HTS e o PSS. O GIRS é responsável por selecionar e encaminhar os NBs/dados publicados pelo PSS ao HTS correto, onde serão armazenados em uma estrutura de tabela *hash*. A escolha da tabela *hash* pelo GIRS é feita por meio de um cálculo que leva em consideração o resto da divisão da chave do NB pelo número de instâncias de HTS disponíveis [7, 38, 39, 42].

#### 2.2.3.4 *Name Resolution and Networking Cache System* (NRNCS)

A união dos serviços HTS, GIRS e PSS forma um novo serviço denominado de NRNCS [7], que foi implementado em 2021. O papel do NRNCS é armazenar SVNes, fornecer *cache* de conteúdo de rede e melhorar a troca de dados, promovendo a descentralização do acesso aos conteúdos.

#### 2.2.3.5 *Proxy-Gateway-Controller Service* (PGCS)

O PGCS acumula a função de três serviços fundamentais para a NovaGenesis [7, 39, 42]: (a) ser um ***Gateway*** para encapsular e extrair mensagens NG sobre uma tecnologia de rede, como por exemplo Ethernet, Wi-Fi ou LoRa; (b) ser um ***proxy*** para representar os outros serviços NG dentro de um OS; e (c) funcionar como **controlador** iniciando o domínio e configurando dispositivos físicos quando necessário, similares a um controlador de *Software Defined Networking* (SDN).
O PGCS também tem uma tabela *hash* interna que armazena as ligações entre nomes descobertos.

#### 2.2.3.6 *Application Service* (APP)

As APP desenvolvidas no conceito da NG, podem ser consumidoras ou publicadoras de dados, conteúdos, métricas, comandos de ações, entre outras.
Segue a estrutura de código fractal da NG utilizando os blocos HT e GW para se comunicar com os demais serviços da NG. Um exemplo de aplicação NG é a “IoTTestApp”, que foi desenvolvida com objetivo de consumir os dados publicados pelo EPGS. Ela assina um contrato com o PGCS e com o EPGS, criando um ambiente seguro de troca de dados entre as entidades envolvidas.

### 2.2.4 NovaGenesis para embarcados

A NG foi desenvolvida em linguagem de programação C++ para ser implementada em dispositivos sem limitações de recursos computacionais, operando sobre o sistema operacional Linux. Contudo, a versão inicial limita sua implementação em cenários de IoT quando instalados em dispositivos com restrições de capacidade de processamento e memória. Objetivando estender a abrangência da NG até o *End Point*, uma versão reduzida da NG foi desenvolvida pelo pesquisador Vaner José Magalhães e Gabriel Dias Scarpioni [7] com orientação do Prof. Dr. Antônio Marcos Alberti, sem perder as suas características, funções e princípios básicos definidos na arquitetura principal.

O **EPGS** [7], reúne em uma versão compacta todas os características da NG com capacidade para ser instalado em dispositivos que utilizam sistemas operacionais leves (FreeRTOS, *Real Time Operating System* (RTOS), etc), que podem ser embarcados em *hardwares* como Arduino, ESP-32, NXP, entre outras plataformas abertas de mercado. O EPGS foi desenvolvido como uma versão reduzida do PGCS da NG, mantendo todas as características de segurança e confiabilidade, baseadas em contratos assinados entre as entidades publicadoras e assinantes por meio do PSS em uma arquitetura controlada por *software*. O EPGS segue o mesmo princípio da NG de utilizar nomes autoverificáveis gerados a partir do *hardware* dos *NÓS*, e é capaz de gerar, enviar, receber e interpretar comandos NG dentro de tarefas pré definidas para seu ciclo de vida.

O EPGS tem a capacidade de adaptar as mensagens para serem enviadas em qualquer camada de enlace, fragmentando e remontando os pacotes.
Em adicional, o EPGS tem métodos para receber informações sobre o dispositivo, características do sensores e dados coletados. Ele otimiza os algorítimos para o uso mínimo de memória ROM e processamento, visando economia de energia e o uso da memória RAM utiliza métodos de alocação dinâmica. A figura 2.2 ilustra os blocos que compõem o EPGS e sua comunicação com o núcleo da NovaGenesis.

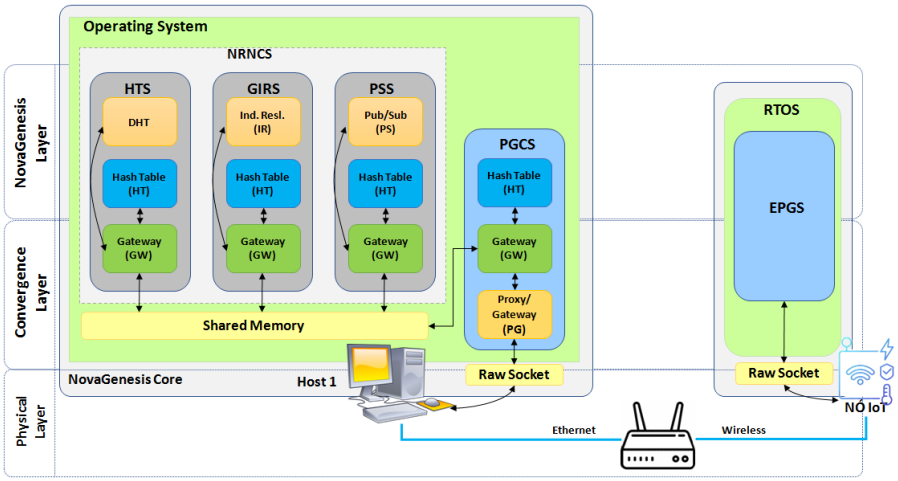



Figura 2.2: *Serviços e Blocos EPGS.*

Os nomes autoverificáveis gerados pelo EPGS contém características de *Hardware* (*Hardware ID* - HID), *Software* (*Operational System ID* - OSID), processos (*Process ID* - PID) ou funcionalidades, utilizando o algorítimo **MurMurHash3**. Para uma entrada de tamanho variado, um nome autoverificável de 4 *Bytes* é gerado. De forma a evitar possíveis conflitos de *hash*, para entradas de pequeno tamanho, o EPGS [7] implementa um vetor multiplicador utilizando os 16 primeiros números primos (do 2 ao 53), aumentando assim em 16 vezes o tamanho, reduzindo a probabilidade de conflito de *hash*. A ligação entre nomes autoverificáveis pode indicar um destino ou origem de um dado onde está contido, ou quem contém o dado desejado. Os comandos NovaGenesis utilizam os SVNes para identificar e rotear as mensagens NG. O protocolo de comunicação entre o EPGS e o núcleo da NG é baseado em tarefas que indicam as ações a serem executadas dentro do ciclo de vida do serviço.

A Figura 2.3 ilustra todas as etapas do processo, desde a geração dos SVNes pelo EPGS, até a composição das tarefas NG.

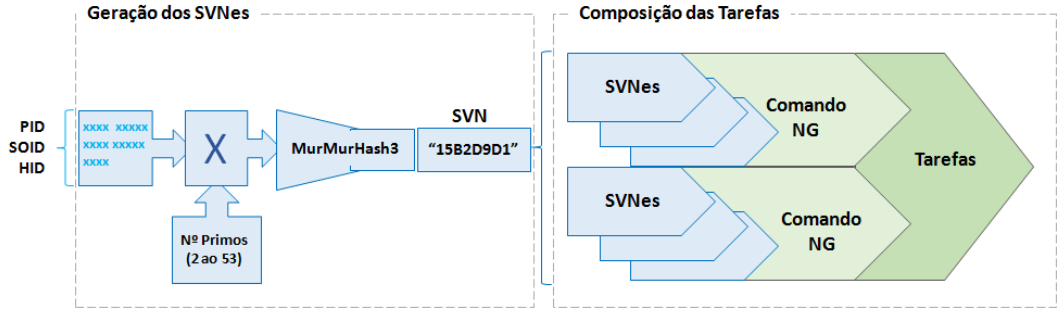



Figura 2.3: *Estrutura de Tarefas NovaGenesis e geração de SVNes.*

#### 2.2.4.1 Tarefas

Uma tarefa é uma ação a ser executada, composta por um conjunto de linhas de comando NovaGenesis. As mensagens NG possuem todos os comandos e dados necessários para a comunicação e processamento entre as entidades envolvidas. Cada comando ocupa uma linha e é composto por duas partes [7, 38, 40]:
O ***Header***, contém o nome, a alternativa e a versão do comando. Todo comando NG é iniciado pelos caracteres "ng" precedido por um sinal de menos "-" e o nome do comando (m, hello, p, info,...). Em seguida dois sinais de menos "- -" indicam o início da alternativa (cl, ihc, notify, payload,...), e por fim, tem-se a versão do comando.
A segunda parte do comando é composta pelos ***Arguments***, os quais são agrupados por colchetes "[...]" podendo cada comando ter mais de um argumento, sendo cada argumento separado pelos sinais de menor e maior "< ... >".
A Figura 2.4 [38, 40] ilustra uma linha de comando com seu *Header* e os *Arguments*. Essa linguagem *script* é única e exclusiva da NovaGenesis, introduzindo controle de versão nos pacotes e seus comandos.

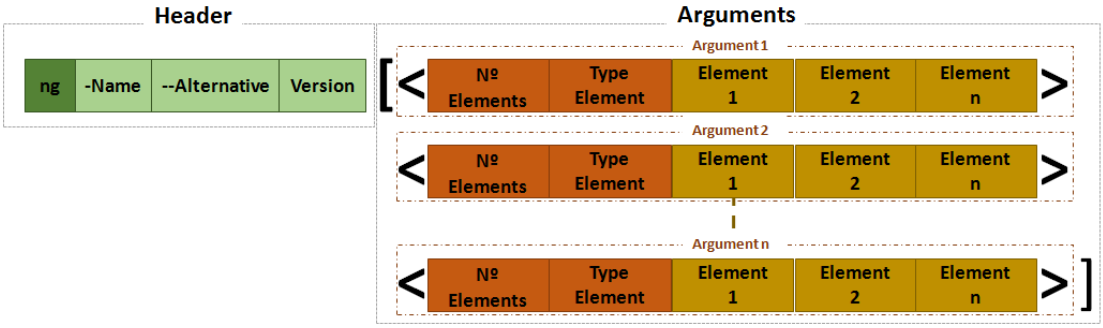



Figura 2.4: *Formato da linha de comando NG.*

Na versão embarcada da NovaGenesis, apenas as seguintes tarefas são implementadas pelo EPGS e fazem parte do ciclo de vida dos serviços NovaGenesis.

- ***Hello***

  É Responsável por apresentar o *NÓ* aos outros pares da rede. O *Hello* é enviado em *Broadcast* pelos PGCSes. Eles informam quais são os componentes, interfaces e identificadores de um serviço NovaGenesis. Os identificadores SVNes utilizados no atual roteamento são únicos: *Hardware Identification* (HID), *Process Identification* (PID), *Operation System Identification* (OSID). Outros tipos de roteamento da NovaGenesis aguardam implementação.

- ***Exposition***

  É responsável por enviar ao PSS as características que descrevem onde e como o EPGS está instalado. Facilita quando um cliente for procurar por um serviço embarcado no PSS.

- ***Service Offering***

  Nesta etapa são apresentadas as características dos serviços prestados pelo EPGS e seu *Service Level Agreement* (SLA). Por exemplo qual sua precisão, qual sua função, variação, faixa de atuação, etc. De certa forma, pode-se dizer que é o primeiro passo para o estabelecimento de um contrato.

- ***Service Acceptance***

  Caso algum cliente tenha interesse pelo serviço ofertado, o EPGS é notificado e recebe uma chave de contrato. E para confirmar, responde com a aceitação do serviço.

- ***Data Publishing***

  Após a realização da negociação do contrato, o EPGS está pronto para disponibilizar para seus clientes os dados requisitados, ou seja publicar propriamente os dados de medição de acordo com os contratos assinados via PSS. Os dados publicados em um arquivo "*.JSON"são enviados no *payload* de uma mensagem. O formato JSON facilita a leitura/escrita por humanos e a interpretação/geração pelas máquinas, requerendo uma quantidade menor de memória para armazenar a informação útil. O padrão JSON só foi usado devido a compatibilidade com outras aplicações NovaGenesis.

A Figura 2.5 ilustra os comandos e seus atributos necessários para a composição das tarefas NG enviadas pelo EPGS, tal qual utilizadas em todo seu ciclo de vida englobando: Anúncio (*Hello*), Exposição de Palavras Chaves (*Exposition*), Publicação de Oferta de Serviço (*Service Offering*), Negociação de Contrato (*Service Acceptance*) e Publicação de Dados (*Data Publishing*).

| Tasks / Command Line | Hello | Exposition | Service Offering | Service Acceptance | Data Publishing | Header: ng command | Header: Name | Header: Alternative | Header: Version | Arguments |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | ng | - name | --Altern. | Ver. | [<Arg1> <Arg2> <Arg3>.... <Arg"n">] |
| Routing | 1 | 1 | 1 | 1 | 1 | ng | -m | --cl | 0.1 | [< 1 s 15B239D1> < 4 s "HID" "SOID" "PID" NULL> < 4 s "Dest_HID" "Dest_SOID" "Dest_PID" |
| Hello | 2 | | | | | ng | -hello | --ihc | 0.2 | [< 9 s "HID" "SOID" "PID" NULL NULL NULL "Architecture" "Interface" "Identification">] |
| Publish Name (Bind) | | 2* | | | | ng | -p | --b | 0.1 | [< 1 s "Category"> < 1 s "Name 1"> < 1 s "Name 2">] |
| Publish Data | | | 2 | | 2 | ng | -p | --notify | 0.1 | [< 1 s "Category"> < 1 s "Content SCN"> < 1 s "File Name"> < 5 s pub "PSS_HID" "PSS_SOID" "PSS_PID" |
| Payload Information | | | 3 | | 3 | ng | -info | --payload | 0.1 | [< 1 s "File Name">] |
| Key Signature | | | | 2* | | ng | -s | --b | 0.1 | [< 1 s "Category">< 1 s "Key">] |
| Message Type | | 3 | 4 | 3 | 4 | ng | -message | -- type | 0.1 | [<1 s "Message Type">] |
| Message Sequence | | 4 | 5 | 4 | 5 | ng | -message | --seq | 0.1 | [< 1 s "Sequential Number">] |
| Verification | 3 | 5 | 6 | 5 | 6 | ng | -scn | --seq | 0.1 | [< 1 s "Message Hash">] |
| Non NG Characteristics | | | 7* | | | ng | -sr | --b | 0.1 | [< 1 s "Category"> < 1 or 5 s "Characteristc"> < 1 s "Value">] |
| Payload | | | 8 | | 7 | | | | | { Payload } |

Legenda: * Numero de comandos é variável

Figura 2.5: *Formação de mensagens e comandos NG executados pelo EPGS.*

A Figura 2.6 ilustra um exemplo das três linhas de comando que formam uma mensagem de "*Hello*".

```
ng -m --cl 0.1 [ < 1 s 15B239D1 > < 4 s 0DA5BBDF A9F22CA3 078D9474 528F2553 > < 4 s FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF > ]
ng -hello --ihc 0.1 [ < 9 s 0DA5BBDF A9F22CA3 078D9474 528F2553 EB99994C E5587B5D Wi-Fi wlp18s0 1c:65:9d:e6:65:71 > ]
ng -scn --seq 0.1 [ < 1 s D65E3D4F > ]
```

Figura 2.6: *Exemplo de linhas de comando NG da mensagem "Hello".*

#### 2.2.4.2 Ciclo de vida NovaGenesis

A sequência de tarefas trocadas entre o EPGS e a NG determinam o ciclo de vida da entidade seguem a sequência ilustrada na Figura 2.7 e serão detalhadas no decorrer desta subseção.

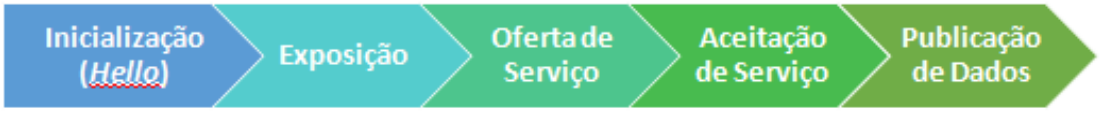



Figura 2.7: *Ciclo de Vida do serviço EPGS.*

- ***Hello***

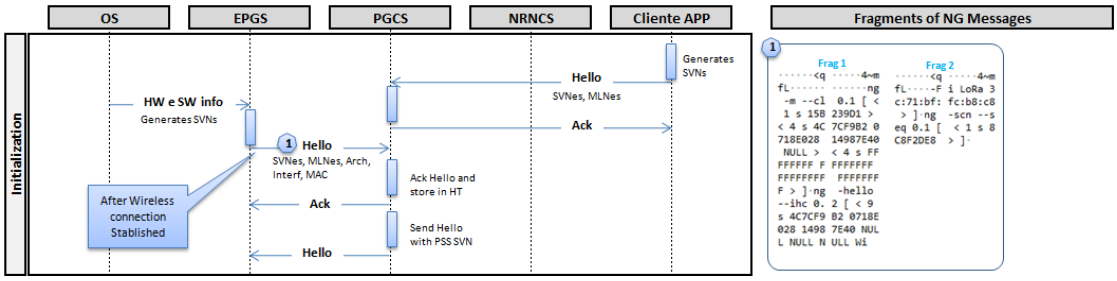



Figura 2.8: *Ciclo de Vida do serviço EPGS - Inicialização.*

Considerando que o núcleo da NG, composto pelo PGCS e NRNCS, já esteja ativo, ao se iniciar uma aplicação ou um *NÓ* EPGS, o processo de inicialização é disparado com objetivo de apresentar/expor sua existência aos demais pares da rede [7]. A mensagem de *Hello* é enviada em *broadcast* contendo: os SVNes, identificadores únicos (processo, *hardware*, *software* e sistema operacional), informações de sua arquitetura de rede (*Stack* - Wi-Fi, Ethernet, LoRa,..), interface e seu identificador de rede - *Media Access Control* (MAC).
A inicialização do EPGS somente pode ser disparada após o dispositivo ter a garantia da conectividade estabelecida, fazendo-se necessário que o *NÓ* esteja conectado à um *Service Set Identifier* (SSID) da rede Wi-Fi, ou quando utilizando LoRa ter passado por todo processo de inicialização, seleção de canal e descoberta do *Gateway*, conforme ilustrado na Figura 2.8.

Em um primeiro momento, o endereço do PSS não é conhecido pelo EPGS, após a confirmação do recebimento do *Hello* pelo PGCS, o endereço auto-verificável do PSS é enviado ao EPGS que os armazenas em uma tabela *hash* interna.

- ***Exposition***

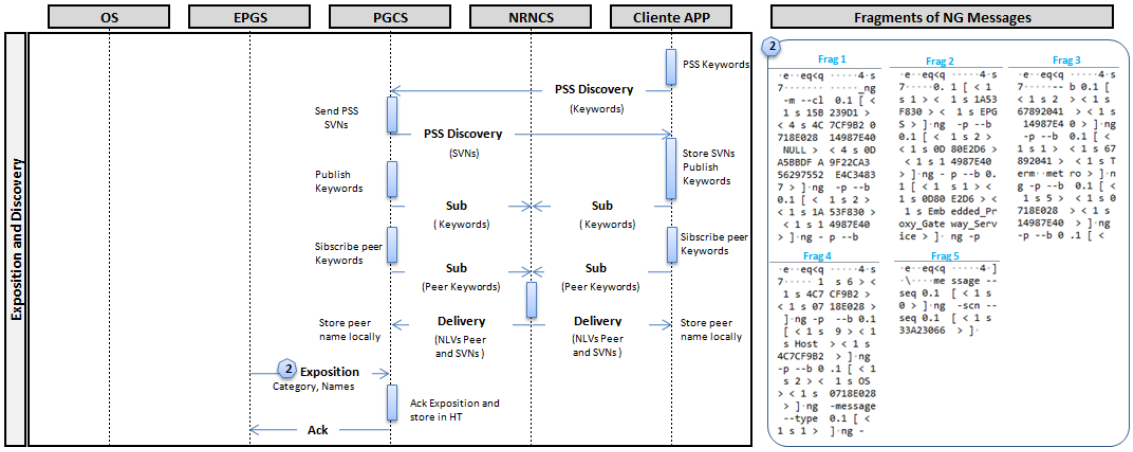



Figura 2.9: *Ciclo de Vida do serviço EPGS - Exposição.*

Após o EPGS receber os nomes autoverificáveis de identificação do PGCS, inicia-se a etapa de descoberta e exposição dos demais serviços da NG conforme ilustrado na Figura 2.9.

O EPGS expõe suas características do *hardware* onde está instalado para o PSS. A exposição do EPGS é feita por meio de ligações entre palavras chaves de nomes em linguagem natural e suas representações em forma de nomes autoverificáveis. O PSS será responsável por criar o ambiente de troca de dados entre as entidades publicadoras e assinantes interessados nestes dados, possibilitando que uma aplicação interessada em medida de temperatura possa assinar um contrato para receber essa informação desejada. Para tal, a aplicação compartilha suas palavras chaves e solicita o dados do PSS onde poderá assinar o serviço que tenha interesse. A aplicação pode ser notificada sempre que uma nova publicação de temperatura venha ocorrer.

- ***Service Offering***

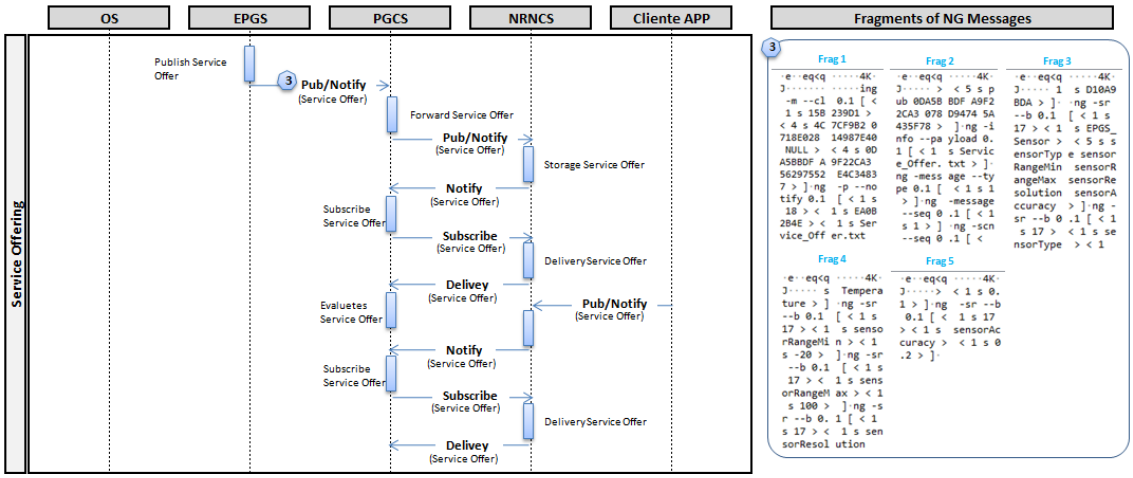



Figura 2.10: *Ciclo de Vida do serviço EPGS - Oferta de Serviço.*

A próxima etapa é a oferta do serviço, onde o EPGS envia para o PSS através do PGCS informações sobre as características do sensor contendo sua precisão, variação máxima e mínima, unidade de medida (Graus Célsius), entre outras informações que sejam necessárias para este exemplo, onde o *NÓ* EPGS é um sensor de temperatura. A Figura 2.10 ilustra os fragmentos de mensagens que compõem a etapa de oferta de serviço.
Este é o primeiro passo no estabelecimento de um contrato de serviço entre um publicador e um assinante de dados.

- ***Service Acceptance***

Caso algum cliente tenha interesse pela oferta de serviço publicado, a negociação do contrato é iniciada. Após ser notificado pelo PSS do interesse pelo serviço, o EPGS envia a mensagem de aceitação do serviço assinando a chave de contrato recebida. A Figura 2.11 ilustra o processo de aceitação do serviço.
Esta etapa finaliza o estabelecimento do contrato acordado entre o EPGS e a aplicação "IoTTestApp", que será consumidora de dados de medições de temperatura. A versão atual da aplicação recebe os dados publicados pelo EPGS, via PSS, e armazena em um arquivo com extensão ".txt".

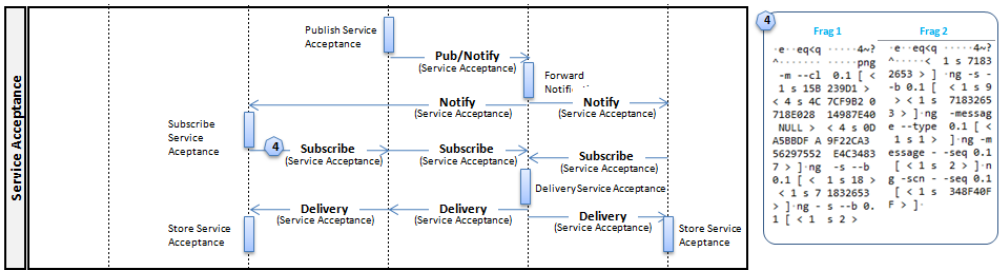



Figura 2.11: *Ciclo de Vida do serviço EPGS - Aceitação do Serviço.*

Concluídas as etapas acima, esta é a última para que os dados sejam compartilhados entre o publicador e o assinante. O EPGS será responsável por publicar os dados de temperatura e a aplicação "IoTTestApp" em consumir estes dados conforme ilustrado na Figura 2.12. Quando uma publicação de dados for enviada pelo EPGS contendo medida de temperatura, por exemplo em um arquivo "*.JSON", o PGCS ao receber esta publicação encaminha para o PSS, que será responsável em notificar aos interessados que uma nova medição de temperatura está disponível. A aplicação, "IoTTestApp", assina o novo dado e o PSS entrega esta informação.

- ***Data Publishing***

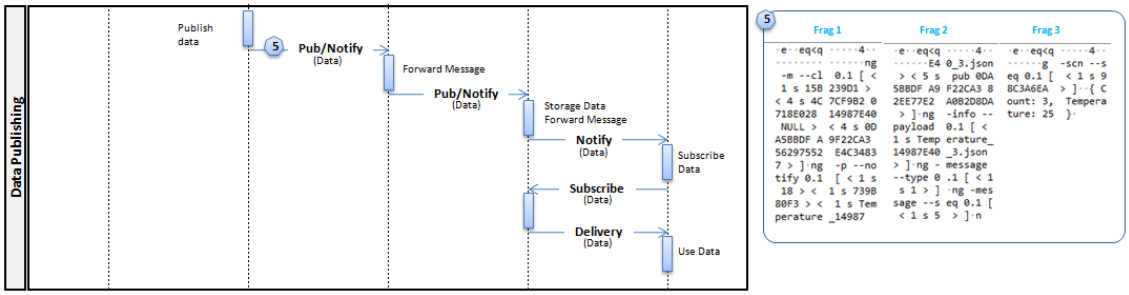



Figura 2.12: *Ciclo de Vida do serviço EPGS - Publicação de Dados.*

O processo de envio de publicação de dados é repetido em intervalos de tempos pré definidos. A aplicação "IoTTestApp" armazena estas medidas recebidas no arquivo "data.txt". Como a NG utiliza mecanismos de publicação e assinatura do serviço, e dentre seus princípios tem a notificação dos interessados, sempre que um novo dado está disponível, é possível medir a performance do serviço entregue pela NG. Neste caso a aplicação "IoTTestApp", gera um segundo arquivo chamado "IoTTestApp_Core_SubRTT" [40]. Este arquivo entrega informações ricas dos tempos entre o momento que recebe uma notificação do PSS, até o momento que o dado é recebido e armazenado.

## 2.3 Tecnologias de comunicações LPWAN

Em ambientes de IoT diferentes cenários podem ser identificados, desde uma geladeira, uma lâmpada em uma praça pública ou um sensor em uma lavoura de soja com quilômetros de extensão, todos conectados a Internet. Cada cenário pode exigir uma arquitetura ou tecnologia de comunicações distinta para atender aos requisitos da IoT em relação ao seu consumo energético, distância de alcance em uma rede sem fio, gestão e escalabilidade. Estas técnicas de conexão sem fio para atender a cenários IoT podem ser separadas em dois grandes grupos como definidos em [43]:

- O **primeiro** considera cenário de **curto alcance**, onde podemos destacar tecnologias como: *Radio Frequency Identification* (RFID), Zigbee, Wi-Fi e BLE, que têm como principal objetivo atender a cenários de IoT em curtas distâncias (alguns metros) contudo, não serão objetos dessa Dissertação de Mestrado.
- um **segundo** grupo contempla as tecnologias que possibilitam dispositivos se conectarem em **alguns quilômetros**, onde se destacam: LoRa, Wi-Fi HaLow, NB-IoT e CAT-M. As técnicas de longo alcance podem ser divididas em frequências licenciadas e não licenciadas ou citados em algumas literaturas como celulares e não celulares. As frequências licenciadas possuem maior controle dos órgãos reguladores, garantindo um menor nível de interferência e uma melhor qualidade de serviço.

Nos cenários de IoT, principalmente em casos de grandes áreas de cobertura e conectividade de longas distâncias, algumas características são importantes e precisam ser avaliadas, como por exemplo, o **tempo de vida das baterias** em casos de dispositivos autônomos, sua capacidade de **escalar** considerando uma quantidade extremamente elevada de dispositivos, **ser robusto** para interferências devido percorrer grandes distâncias, suportar **mobilidade**, ser **flexível** para trabalhar com diferentes taxas de dados, ter capacidade de garantir um **nível de segurança dos dados** transmitidos além da **qualidade de serviço**. Neste sentido surgem tecnologias que almejam atender a estes requisitos para cenários de IoT denominada de LPWAN [44].

Nas próximas subseções serão abordadas as principais tecnologias de LPWAN com um maior detalhamento para o LoRa.

### 2.3.1 Wi-Fi HaLow

Os diferentes padrões do Wi-Fi além de serem grandes impulsionadores de tráfego de acesso à Internet para suportar aplicações de *streaming*, redes sociais, transferência de dados, vídeo, entre outros, possibilitaram que uma enorme quantidade de elétrico domésticos se conectassem à Internet.
Vencer barreiras, paredes e longas distâncias sempre foi o grande desafio para a tecnologias Wi-Fi por trabalharem em frequências elevadas, 2,4 e 5 GHz, demandando a construção de arquiteturas mais complexas envolvendo repetidores em topologia *mesh* para aumentar sua cobertura.
Com o objetivo de alcançar distâncias maiores sem carregar o fardo destes dispositivos agregados e proporcionando conectividade como banda apropriada aos dispositivos IoT, a ***Wi-Fi Alliance*** **(R)** introduziu um novo padrão denominado IEEE

802.11ah [20] operando em frequência conhecida como Sub 1 GHz (S1G), mesma utilizada por outras tecnologias LPWAN como o *Longe Range WAN* (LoRaWAN ®). O padrão 802.11ah suporta IP nativamente, diferente das demais tecnologias LPWAN em frequências não licenciadas, que requerem um GW para se conectarem com as aplicações em nuvem.

De acordo com ***Wi-Fi Alliance*** (R) [20] o 802.11ah especifica 5 larguras de canais, 1, 2, 4, 8 e 16 MHz, sendo que os dois menores visam alcançar longas distâncias com taxa de dados pequenos, atendendo a sensores por exemplo, e as outras três para aplicações que demandam uma maior capacidade de dados, contudo com distâncias reduzidas, como por exemplo sistemas de vídeo monitoramento.
A Figura 2.13 ilustra de forma gráfica a relação entre canais, distância e taxa de dados. Com uma largura de canal de 1 MHz é possível alcançar até 1 Km com uma taxa de dados de 150 Kbps, uma taxa de transmissão de dados de 86,7 Mbps quando utilizado canais com largura de 16 MHz.
Segundo [20] o Wi-Fi HaLow (Long Range, Low Power Wi-Fi for IoT) vem como um forte concorrente das tecnologias LPWAN, quando considerado para cenários de médio alcance, pois traz em sua estrutura características de uma tecnologia mundialmente adotada em diversos seguimento, além de poder usufruir de ferramentas de gestão e controles já disponíveis para versões anteriores. Aplicações de cidades inteligentes, agricultura, condomínios residenciais entre outros podem vir a se beneficiar desta tecnologia onde, além de possibilitar a expansão da IoT, também prover Internet para áreas carentes de recursos de conectividade.

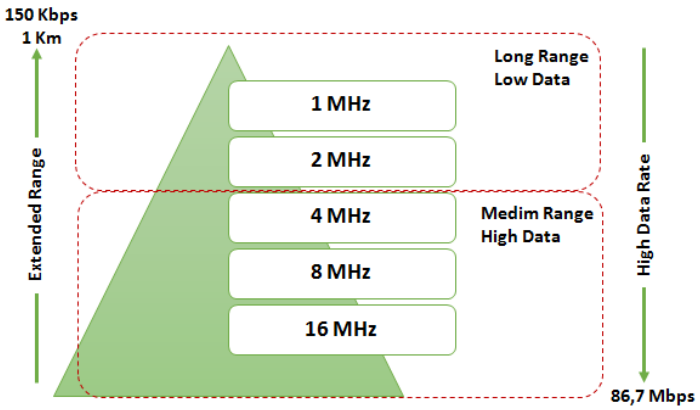



Figura 2.13: *Wi-Fi 802.11ah, longo Alcance para IoT.*
Fonte: Baseado em Wi-Fi HaLow ™ Technology Overview, Figure 1, Wi Fi HaLow operates in sub 1 GHz in channels ranging from 1 to 16 MHz.

Um dos pontos chaves do Wi-Fi HaLow é o baixo consumo de energia, habilitando dispositivos providos de bateria a funcionar por anos. Ajustes de algumas funcionalidades na camada MAC, listados em [20], possibilitaram uma significativa economia de energia pelo *end point*. Comparado com outras tecnologias LPWAN, Wi-Fi HaLow se apresenta como uma tecnologia promissora para atender aplicações de médio alcance devido a sua baixa complexidade e poder usufruir de infraestruturas e modelos operacionais já conhecidos.

### 2.3.2 NB-IoT

O NB-IoT foi uma rápida resposta do 3GPP à crescente demanda de conectividade dos dispositivos IoT e pressionado pela disputa com outras tecnologias, conforme abordado em [43]. Foi especificado e definido no *Release* 13 de junho de 2016 do 3GPP utilizando bandas das redes *Long-Term Evolution* (LTE) ou *Global System for Mobile* (GSM) tendo como 5 principais objetivos para *Machine-Type Communication* (MTC) [21]: (a) **melhoria da cobertura** *indoor*; (b) suportar **conexões massivas** de terminais com pequenos pacotes de dados; (c) **reduzir a complexidade** e custo dos terminais; (d) aumentar a eficiência energética; e (e) suportar **diferentes latências**.
Esta tecnologia chama mais a atenção da indústria, visto que é possível sua implementação com apenas upgrade de software na rede, preservando assim o investimento. Sua implementação pode ser feita em três cenários, utilizando uma frequência independente "*Stand Alone Mode*", na banda de guarda "*Guard Band*" que utiliza as frequências de borda do LTE e dentro da frequência LTE denominado "*In Band*".

O NB-IoT especifica um novo rádio para terminais IoT, que aumenta a cobertura *indoor*, suporta o número massivo de conexão de baixa taxa de transferência, possui baixa sensibilidade a atrasos utilizando dispositivos de baixo custo e menor consumo de energia. O NB-IoT é uma nova tecnologia de rádio que coexiste com os sistemas GSM, *Universal Mobile Telecommunications System* (UMTS) e LTE já existentes.

Para suportar conexões massiva com transferências de pequenos pacotes de dados a uma baixa frequência em um mesmo canal 180 KHz, foram definidos dois possíveis cenários [21, 43], um com 12 sub portadoras de 15 KHz e outro de 48 sub portadoras de 3,75 KHz. Isso possibilita uma taxa de dados por sub portadora de até 200 Kbps, 5 vezes menor que a outra variação do *Release* 13 do 3GPP para conexão CAT-M1. Podendo alcançar distâncias entre 10 à 15Km.

Com objetivo de prolongar a vida útil da bateria, foi implementado funcionalidades como *Extended Discontinuous Reception* (eDRX) e *Power Saving Mode* (PSM) [21], onde o dispositivo permanece em modo *standby* por longo tempo. O conceito destas técnicas é de monitorar o *downlink* durante um curto período e permanece dormindo o tempo restante. Enquanto em conexões eDRX pode ser configurado um intervalo de até 10,24 segundos [45], para NB-IoT este tempo pode ser estendido até 10485,76 segundos (2,91 horas), o que permite uma alta economia de energia para os caso onde a latência não é impacto. Com objetivo de aumentar a área de cobertura os blocos de transporte podem ser transmitidos várias vezes, por exemplo 128 vezes no *uplink* e 2048 no *downlink*, melhorando a relação sinal ruido e permitindo a decodificação do sinal.

Mesmo não sendo abordado neste documento (em detalhes) as implementações evolutivas do 3GPP desde a *Release* 8 até o 14 são apresentadas em [43].

### 2.3.3 CAT-M

O LTE-M também conhecido como CAT-M1 é uma simplificação do termo LTE-MTC para *Low Power Wide Area* (LPWA), publicado pelo 3GPP em 2016 no release 13, para atender a demanda de IoT, fazendo frente as iniciativas de tecnologias não padronizadas pelo 3GPP. LTE-M é uma tecnologia de longa cobertura com baixo consumo, suportado por dispositivos de baixa complexidade, provendo cobertura extensa, permitindo o reuso da rede LTE. O CAT-M1 assim como o NB-IoT estão em linha das recomendações mínimas do IMT-2020 do ITU [46] para cenários de acessos massivos *massive Machine Type Communications* (mMTC), preparando para o próximo salto em direção próxima geração, 5G.

Assim como o NB-IoT, o CAT-M1 também utiliza técnicas de PSM e eDRX, com objetivo de reduzir o consumo, aumentando assim a vida útil da bateria. Segundo [22] é possível implementar a combinação das duas técnicas, contudo um ponto de atenção é com relação as definições dos intervalos de espera, para garantir o sucesso do envio dos *pages* na rede.

A extensão de cobertura também é aplicada com objetivo de maiores alcances. Dois modos são definidos: **Modo A** com até 32 vezes de repetição e o **Modo B** com até 2048 vezes de repetição. De acordo com [22], normalmente adota-se o modo A na maioria das aplicações e o modo B para casos onde precisam de uma maior penetração do sinal, por exemplo áreas subterrâneas de um prédio, porém nestes cenários é importante que o dispositivo permaneça estacionário e com poucas transmissões diárias.

O CAT-M1 definido no *Release* 13 opera com largura de banda de 1.4 MHz o que possibilita uma taxa de transmissão de dados de até 1 Mbps com um alcance máximo de 11K,. No *Release* 14 novas larguras de bandas foram definidas possibilitando taxas de dados de até 4 Mbps no CAT-M2, que utiliza largura de banda de 5 MHz. Outras melhorias como, *Multicast Downlink Transmission*, *Location Services using Enhanced*, *Increased Voice over* LTE (VoLTE) e *Coverage for Halfduplex*, podem ser vistas em maiores detalhes em [22, 47]. Em comparação com NB-IoT pode-se dizer que é uma solução de ponta, mas com uma complexidade maior.

### 2.3.4 LoRa

A LoRa foi desenvolvida pela Semtech com objetivo de permitir comunicações de longo alcance, com baixo consumo de energia e uma taxa de dados suficiente para atender cenários de IoT. Opera na faixa de frequência não licenciada conhecida como Sub 1 GHz (S1G), podendo alcançar distâncias de até 15Km [44]. LoRaWAN $^{R}$ fornece um mecanismo de controle de acesso ao meio, permitindo que muitos dispositivos finais se comuniquem com um *Gateway* usando a modulação LoRa. Enquanto a modulação LoRa é proprietária, o LoRaWAN $^{R}$ é um padrão aberto desenvolvido pela **LoRa *Alliance***.

#### 2.3.4.1 Arquitetura de Rede

A LoRa se desponta com uma tecnologia para atender aos principais requisitos de IoT sendo estruturado em duas camadas [18, 48]: Uma **primeira** associada a **camada física**, também conhecida como **LoRa MAC**, que define a modulação e cria os enlaces para comunicações de longo alcance, utilizando o *Chirp Spread Spectrum* (CSS), técnica muito utilizada em comunicações militares e espaciais por atingir grandes distâncias devido sua robustez à interferências alcançando distâncias de até 5Km em ambiente urbano e podendo chegar a 15Km em áreas rurais. Uma característica fundamental das soluções baseadas em LoRa são os requisitos de energia ultrabaixa, o que permite a criação de dispositivos operados por bateria que podem durar até 10 anos.
Uma técnica proprietária de modulação de espectro de propagação derivada da tecnologia CSS existente, a LoRa oferece uma compensação entre sensibilidade e taxa de dados, enquanto opera em um canal de largura de banda fixa de 125 KHz ou 500 KHz (para canais de *uplink*) e 500 KHz (para canais de *downlink*). Além disso, LoRa usa fatores de espalhamento ortogonais. Isso permite que a rede preserve a vida útil da bateria dos *NÓS* finais conectados, fazendo otimizações adaptativas dos níveis de energia e taxas de dados de um *NÓ* final individual. Por exemplo, um "*End Point*" localizado próximo a um GW deve transmitir dados com um fator de espalhamento baixo, pois é necessário muito pouco "*link budget*". No entanto, um "*End Point*" localizado a vários quilômetros de um GW precisará transmitir com um fator de espalhamento muito maior. Esse fator de espalhamento mais alto fornece ganho de sensibilidade de recepção, embora a taxa de dados seja, necessariamente menor.

O ganho de sensibilidade no LoRa é introduzido no canal de RF multiplicando o sinal de dados com um código de espalhamento ou sequência de "*Chip*". Ao aumentar a taxa de "*Chip*", aumentamos os componentes de frequência do espectro total do sinal. Em outras palavras, a energia do sinal total agora está espalhada por uma faixa mais ampla de frequências, permitindo que o receptor diferencie um sinal com uma relação *Signal to Noise Ratio* (SNR) mais baixa (ou seja, pior).
No LoRa, a quantidade de código de espalhamento aplicada ao sinal de dados original é chamada de *Spread Factor* (SF). A modulação LoRa tem um total de seis fatores de espalhamento (SF7 a SF12). Quanto maior o fator de espalhamento utilizado, mais longe o sinal poderá viajar e ainda ser recebido sem erros pelo receptor de RF.

**Outra** camada é a **LoRaWAN ®**, onde se define os protocolos de comunicação e as adequações aos tipos de classes de rede.
A LoRaWAN ® possui três tipos de classes de rede [18] que definem a forma como será a comunicação entre o *NÓ* e o *Gateway*, que estão diretamente relacionadas à eficiência energética do dispositivos remotos descritos abaixo:

- Na **Classe A** a comunicação bidirecional é habilitada sempre que for transmitido algo pelo *NÓ* LoRa. A transmissão do *NÓ* LoRa no *uplink* sempre será precedido por duas janelas curtas de transmissão enviadas pelo GW. Pode ser considerada a mais básica e com a melhor eficiência de consumo energético. Os intervalos entre as transmissões do *NÓ* LoRa são definidos de acordo com cada aplicação. A transmissão no *downlink* sempre terá que aguardar a janela até o próximo agendamento do *uplink* conforme ilustrado na Figura 2.15 (a). Em termos de dispositivos podemos destacar sensores equipados com bateria, onde requer uma melhor eficiência energética.
- Os *NÓS* LoRa na **Classes B**, habilitam *slots* extras de recepção. Em adição a janelas randômicas na Classe A, o *NÓ* LoRa na Classe B abre novas janelas de transmissão em tempos pré definidos para transmissão no *downlink*. Para que isso ocorra, é necessário que, tanto o *NÓ* LoRa como o GW estejam sincronizados, desta forma, uma mensagem de ***Beacon*** sincronizada no tempo é enviada pelo GW. Isso permite que o servidor saiba quando tem uma janela disponível para transmitir conforme ilustrado na Figura 2.15 (b). Devido a necessidade do *NÓ* LoRa precisar estar atento para receber mensagens de sincronismo e possuir janelas extras, sua eficiência energética é menor que a da Classe A. Na Classe B, dispositivos com funções de atuadores equipados com bateria passam a ter uma maior aderência, uma vez que possui uma boa eficiência energética com controle de latência no *downlink*, pois o *NÓ* LoRa e o GW utilizam *slots* de transmissão no *downlink* sincronizados por *beacon*.
- A **Classe C** possui uma janela de comunicação praticamente contínua, apenas sendo interrompida quando o *NÓ* LoRa for transmitir algo no *uplink*. A Classe C possui uma menor eficiência energética em relação as Classes A e B, contudo, oferece uma menor latência conforme ilustrado na Figura 2.15 (c). Devido os dispositivos ouvirem continuamente, possui uma baixa latência o que possibilita um acesso imediato para comunicação de *downlink*, por isso é mais utilizado em atuadores alimentados por energia.

A Figura 2.14 ilustra de forma resumida as principais características das classes de rede adotadas pela LoRaWAN ®.

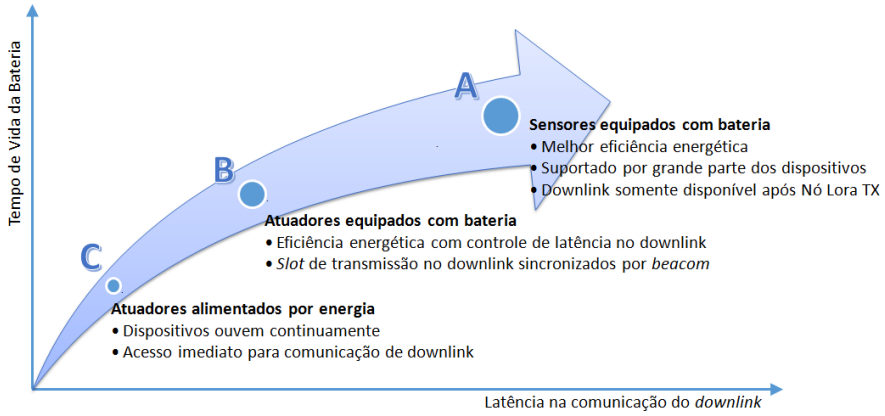



Figura 2.14: *Classes de rede para dispositivos LoRa.*
Fonte: baseado em LoRaWAN - A technical overview of LoRa® and LoRaWAN.

O funcionamento das janelas de transmissões do LoRaWAN ® torna-se necessário, pois podem gerar limitações para a implementação de uma FIA sobre sua estrutura de transmissão LoRa. A Figura 2.15 ilustra a forma de operação das janelas de transmissão e recepção em LoRa, indicando qual a relação entre eficiência energética e latência, mostrando que as duas são inversamente proporcionais.

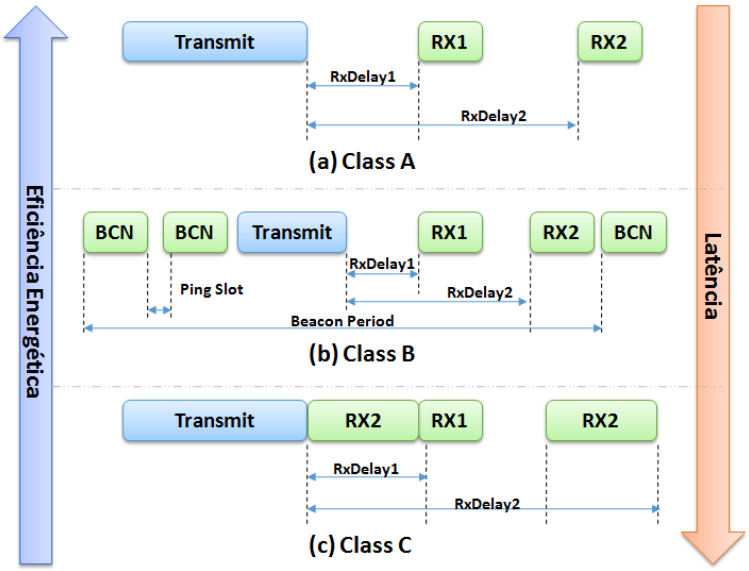



Figura 2.15: *Janelas de transmissão do LoRa.*
Fonte: baseado em LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities, Figura 2.4, LoRaWAN communication classes.

### 2.3.4.2 Características de transmissão LoRa

A comunicação entre *NÓS* e GW é distribuída em diferentes canais de frequência e taxas de dados. A seleção da taxa de dados é uma adequação entre alcance de comunicação e duração da mensagem, sendo que comunicações com taxas de dados diferentes não interferem umas nas outras.

As taxas de dados na LoRa variam de 0,3 kbps a 50 kbps [49]. Para maximizar a vida útil da bateria dos *NÓ* e a capacidade geral da rede, a infraestrutura de rede LoRa pode gerenciar a taxa de dados e a saída de RF para cada dispositivo final, individualmente por meio de um esquema *Adaptive Data Rate* (ADR).

A LoRa prevê o suporte à diversas faixas de frequência da *Industrial, Scientific and Medical* (ISM), se adequando as diferentes regulamentações existentes distribuídas como segue [49]: (a) para a região da Europa a **faixa de 863-867 MHz**, comumente referenciada como 868 MHz, pode chegar a uma taxa de dados de 50 Kbps quando operando em modulação *Frequency Shift Keying* (FSK) com um *payload* máximo de 222 Bytes; (b) a **faixa de frequência de 902-928 MHz**, utilizada como *default* em 915 MHz, é regulada para operar em toda América e continente Ártico, podendo operar em largura de banda de 125 KHz ou 500 KHz com 64 ou 8 canais respectivamente. A taxa máxima de transmissão suportada nesta faixa de 915 MHz é de 21,9 Kbps com um *payload* útil máximo de 222 Bytes, utilizando um SF igual a 7 em uma banda de 500 KHz; (C) a **faixa de 779-787 MHz** definida para ser utilizada na China também pode chegar a uma taxa de dados de 50 Kbps quando operando em FSK; e (d) definido para utilização na Europa a **frequência de 433 MHz**, também alcançando uma taxa de dados de 50 Kbps em modulação FSK.
Para efeito de visualização a Figura 2.16 ilustra em forma de tabela as taxas máximas de dados e seu payload em cada SF em um cenário utilizado para a região da América na frequência de 915 MHz.

| Configuração | | US902-928 | | | | | |
|---|---|---|---|---|---|---|---|
| | | Banda [KHz] | Taxa [bps] | Payload [Bytes] | Banda [KHz] | Taxa [bps] | Payload [Bytes] |
| SF | 12 | 125 | - | | 500 | 980 | 33 |
| | 11 | 125 | - | | 500 | 1760 | 109 |
| | 10 | 125 | 980 | 53 | 500 | 3900 | 222 |
| | 9 | 125 | 1760 | 129 | 500 | 7000 | 222 |
| | 8 | 125 | 5470 | 242 | 500 | 12500 | 222 |
| | 7 | 125 | 12500 | 242 | 500 | 21900 | 222 |

Figura 2.16: *Tabela de taxa de dados para LoRa em frequência de 915 MHz.*

#### 2.3.4.3 Arquitetura de Rede LoRaWAN ®

Muitas redes existentes utilizam uma arquitetura de rede *mesh*, onde os dispositivos finais *NÓS* encaminham as informações de outros *NÓS*, para aumentar o alcance da comunicação e/ou a área de cobertura. Contudo, esta técnica adiciona complexidade, reduz a capacidade da rede e reduzir a vida útil da bateria, pois os *NÓS* recebem e encaminham informações de outros *NÓS*, que provavelmente são irrelevantes para eles. A arquitetura em estrela de longo alcance, utilizada pela LoRa, passa a ser mais relevante pensando em preservar a vida útil da bateria e de reduzir a complexidade operacional.

Os principais elementos que compõem a arquitetura LoRaWAN ® são: o Dispositivos Finais ou simplesmente ***NÓ***, o ***Gateway*** **(GW)** e o ***Network Server*** **LoRa (NSL)** [50].

Os *NÓS* são equipados com sensores ou atuadores e podem estar conectados a um ou mais GW LoRa. Já os GW tem função de agrupar os *NÓS* e entregar os dados transmitidos para um NSL. O NSL tem um papel importante para controlar todos os elementos da rede, definindo o uso de frequência, controle de admissão, segurança, etc.

Em uma rede LoRaWAN ®, os *NÓS* não estão associados a um GW específico, os dados transmitidos por um *NÓ* geralmente são recebidos por vários GW. Cada GW encaminhará o pacote recebido do *NÓ* para o servidor de rede NSL em nuvem por meio de algum *backhaul* (celular, Ethernet, satélite ou Wi-Fi). A inteligência e a complexidade são deixadas para o servidor da rede que gerencia e filtra pacotes redundantes recebidos, realiza verificações de segurança e define o melhor GW para se comunicar. Se um *NÓ* estiver em movimento não há necessidade de transferência entre GW, este é um recurso crítico para habilitar rastreamento de ativos, que é atendido pela LoRa, nativamente e gerenciado pelo LoRaWAN ®.

A Figura 2.17 ilustra de forma geral os elementos componentes da arquitetura LoRa / LoRaWAN ®.

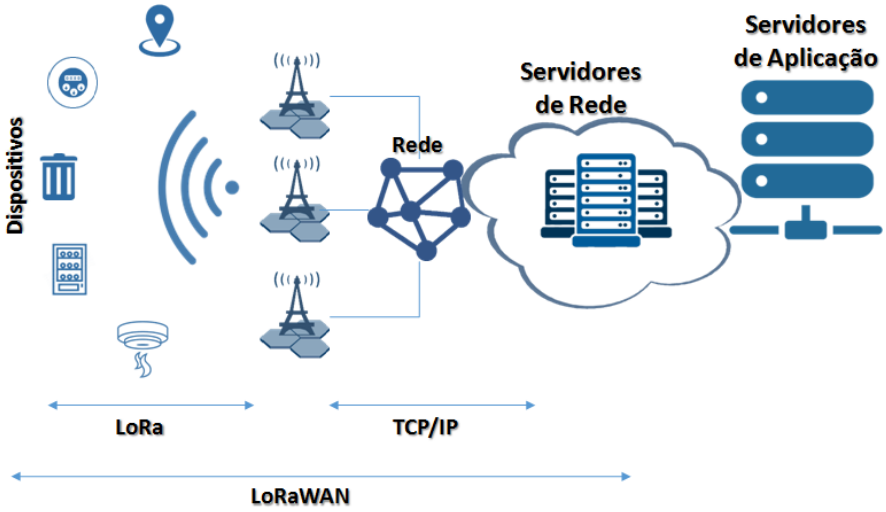



Figura 2.17: *Topologia Geral de uma arquitetura LoRa.*

#### 2.3.4.4 Comparativo das LPWANs

As subseções anteriores abordaram as tecnologias LPWAN e suas características para os cenários de IoT. Uma vez que, o objetivo desta Dissertação de Mestrado é estender a FIA NG em uma rede LPWAN, faz-se necessário definir qual destas tecnologias possibilita a realização de uma prova de conceito por meio da integração destas duas arquiteturas, ou seja, FIA sobre uma rede LPWAN.
A Tabela 2.18 ilustra de forma resumida as principais características das tecnologias apresentadas. Dentre as tecnologias LPWAN a LoRa foi a escolhida para implementação do protótipo que subsidiará a esta Dissertação de Mestrado devido: (a) possuir diversas plataformas abertas de mercado com baixo custo; (b) ter a capacidade de implementar redes de comunicação para IoT de forma rápida sem a necessidade de aprovação de órgãos reguladores; (c) proporcionar cenários de testes para curto, médio e longo alcance baseado na escolha do SF; (d) possuir uma taxa de dados e um tamanho de

*payload* capaz de suportar as mensagens NG completas ou fragmentadas. Assim contribuindo para o desenvolvimento e a integração das duas arquiteturas objeto desta prova de conceito.

| Tecnologia / Dimensões | Tecnologias de Médio e Longo Alcance | | | |
|---|---|---|---|---|
| | Não Licenciada | | Licenciada | |
| | LoRa | Wi-Fi HaLow 802.11 ah | CAT-M | NB-IoT |
| **Organização Padronizadora** | Lora Alliance | IEEE | 3GPP | 3GPP |
| **Maximo alcance** | 2 - 5 Km (Urbano), 15 Km (Não urbano) | Até 1Km em 802.11 ah | ~11 Km | 10 - 15 Km |
| **Alcance** | Longo | Médio | Longo | Longo |
| **Taxa de TX** | ~50 Kbps | 150 Kbps | < 1 Mbps | ~150 Kbps |
| **Vida da Bateria** | > 10 anos | > 10 anos | > 10 anos | > 10 anos |
| **Mobilidade** | Sim | Sim | Sim | Sim |
| **Integração com IP** | Requer Gateway | Nativo | Sim | Sim |
| **Open Hardware** | Sim | Não | Não | Não |

Figura 2.18: *Dimensões das redes LPWAN.*

### 2.3.5 Resumo

Neste capítulo, abordamos os principais desafios de uma FIA para suportar os serviços existentes, garantindo sua interoperabilidade com o legado, estando preparada para novos serviços que venham a surgir. Em específico a arquitetura NovaGenesis foi apresentada com maiores detalhes demonstrando estrutura, camadas, comandos, blocos, serviços especializados, ciclo de vida e os princípios básicos.
A NG é uma arquitetura orientada a serviço que utiliza nomeação e ligação entre nomes desacoplando o identificador e localizador, e implementa em sua estrutura *cache* de rede que possibilita a entrega do conteúdo do ponto mais próximo do assinante. Possui uma versão reduzida para ser embarcada em dispositivos com baixa capacidade computacional, implementando uma arquitetura completa.

Paralelo as pesquisas de novas arquiteturas, as tecnologias de conectividade vem evoluindo ao longos dos anos para atender cenários de IoT, os quais empregam requisitos de baixo consumo, longos alcances, baixa complexidade, entre outros temas discutidos neste capítulo. As tecnologias de LPWAN vem se destacando por novos desenvolvimentos ou adequações em estruturas existentes. Também foi definido dentre as diferentes LPWANs qual delas possibilita a realização de uma prova de conceito, onde a LoRa foi a escolhida.

# Capítulo 3

# NovaGenesis com LoRa - Do problema a solução

O Trabalho anterior [7] provou a viabilidade de se implementar uma arquitetura FIA NovaGenesis em dispositivos embarcados utilizando redes Wi-Fi, garantindo todo o ciclo de vida do serviço, incluindo a publicação de dados de medição de temperatura. Contudo, sua implementação e gerenciamento para cobrir grandes áreas ou atingir longos alcances, torna a arquitetura complexa e inviável, uma vez que há necessidade de se inserir muitos pontos de repetição para alcançar a área desejada.

Desta forma, abre-se uma oportunidade de se expandir a NovaGenesis em cenários IoT para longo alcance, utilizando tecnologia de comunicação LPWAN para atender projetos de cidades inteligentes, agricultura, redes de monitoração inteligentes, indústrias com aplicações não criticas, etc. Desta foram, demonstrando sua aplicabilidade em cenários que exigem grandes coberturas e com comunicação segura entre as entidades.
O trabalho proposto por essa Dissertação de Mestrado visa comprovar a hipótese de estender o componente da arquitetura NovaGenesis, chamado EPGS, utilizando a LoRa como camada de enlace.
Nesse capítulo serão abordados os esforços empreendidos, desafios e ajustes necessários na NG e no EPGS, para garantir a convivência das duas arquiteturas em um cenário de IoT. Esta integração assegura que todas as etapas do ciclo de vida da NG sejam suportados, atendendo cenários IoT que demandam cobertura de extensas. Estes cenários poderão ser atendidos de forma integral, por uma FIA cobrindo toda sua extensão, desde o *NÓ* até o núcleo da rede.
Também será apresentado a metodologia aplicada para planejar, implementar e medir/coletar dados, que subsidiem a avaliação da performance FIA NG utilizando uma rede LoRa.

## 3.1 Desafios para uma rede IoT na Agricultura

É sabido que existem grandes desafios a serem enfrentados nas próximas décadas para alimentar toda população mundial [51–54], que está crescendo muito rápido e com expectativa de chegar a mais de 9,7 bilhões, até 2050, segundo relatório da UN [55].

Sabe-se que os métodos atuais de cultivo e mecanismos de produção, não serão capazes de atender a demanda mundial para alimentar toda a população. Apesar do desenvolvimento ocorrido nas últimas décadas, nas áreas de agronomia e pecuária como, por exemplo, melhoramentos genéticos, intensificação da produção, e etc, no entanto, a preocupação com o crescimento sustentável tornou-se objeto de discussões e abordagens de entidades como a *Food and Agriculture Organization* (FAO), que levou reguladores como a ITU a definir e sugerir agentes responsáveis para uma Agricultura de serviços inteligentes [56].
Ao introduzir este problema no acompanhamento das Tecnologia da Informação e Comunicação (TIC), as aplicações IoT poderão implementar e auxiliar na gestão de ponta a ponta da cadeia produtiva. Para isso, dispositivos presentes nas diversas áreas da atividade humana e aplicações disponíveis em nuvem, passam a ter grande relevância. Para que isso ocorra, a existência de uma infraestrutura de rede e uma arquitetura desenhada que acomode todos os elementos conectados torna-se necessária, dando suporte a esta explosão de dispositivos. Uma rede de comunicação eficiente e adequada é indispensável para alimentar as aplicações hospedadas em um ponto central (Data Center ou Nuvem), com objetivo de gerar informações contextualizadas para tomada de decisão.

Conforme condições anteriores apresentadas, a proposta desta Dissertação de Mestrado é implementar a FIA NG permeando pelos elementos que compõe a rede LoRa, expandindo sua utilização em IoT para comunicação de longo alcance contribuindo assim, para atender desafios propostos pelos ITU e UN, por exemplo em cenários da agricultura.

Dentre os principais desafios para esta prova de conceito, pode-se destacar:

(a) A definição de um *hardware* que possa suportar o LoRa para comunicações de longa distâncias em conjunto com o EPGS embarcado e convivendo harmonicamente;

(b) Adequar os códigos anteriores desenvolvido considerando Wi-Fi para este novo cenário;

(c) Avaliar e ajustar parâmetros da NovaGenesis considerando as características da LoRa, que podem vir a restringir ou impedir esta implementação;

(d) Avaliar *Gateway* existentes, ou desenvolver um, que possibilite a interligação entre a rede LoRae a rede local, onde está o núcleo da NovaGenesis; e

(e) Validar que todo o ciclo de vida do serviço gerenciado pela NG seja suportado neste ambiente de teste.

Desta forma, é possível validar uma aplicação de uma FIA em uma rede LPWAN em um cenário para atender medições de temperatura para a Agricultura.

## 3.2 Metodologia de validação da hipótese

De forma a garantir que todos os pontos fossem abordados para validação da hipótese desta pesquisa, a seguinte metodologia foi aplicada para realização do teste.
A Figura 3.1 ilustra de forma geral as principais etapas da metodologia seguida de forma a alcançar o objetivo desta prova de conceito. As ações e resultados de cada etapa serão melhores detalhadas nesta seção. As etapas de "Coleta e análise de dados" e "Apresentação dos Resultados" serão abordados, a seguir, no capítulo 4

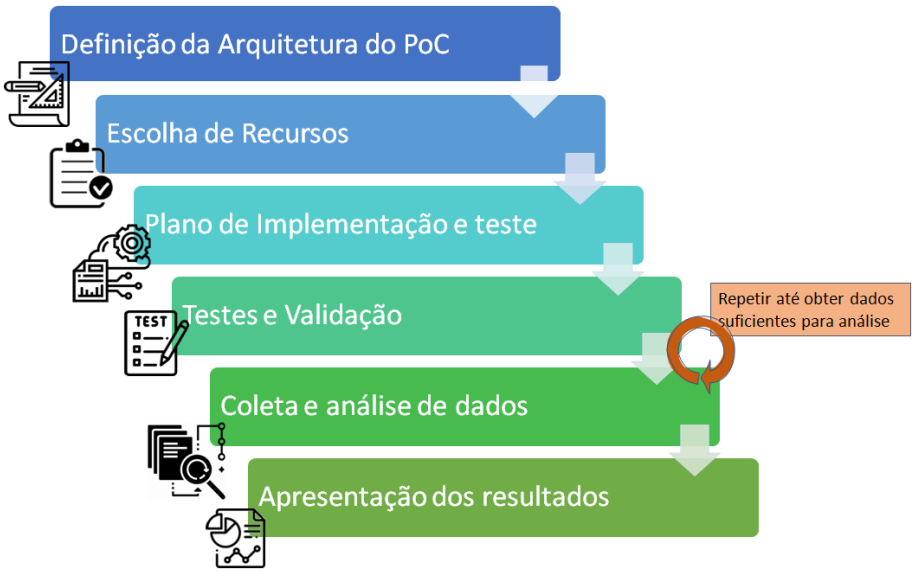



Figura 3.1: *Plano de trabalho.*

### 3.2.1 Arquitetura de teste para a prova de conceito (PoC)

Para avaliar a NovaGenesis com LoRa foi definido um cenário de teste e implementado um protótipo contendo um *NÓ* remoto provido de sensor de temperatura, no qual embarca o EPGS sendo capaz de transmitir essas medidas para o núcleo da NovaGenesis, utilizando como meio a comunicação LoRa.
O núcleo da NG é instalado em um servidor central, conectado a uma rede Ethernet. Para interligar estas duas redes, atendendo ao cenário proposto, um GW de protocolo traduz pacotes NG encapsulados em LoRa para Wi-Fi e vice-versa. Um roteador Wi-Fi é utilizado para viabilizar esta comunicação de ponta a ponta, entre a rede local Ethernet e o GW LoRa.
A Figura 3.2 ilustra o cenário de laboratório e a Tabela 3.1 define as funções de cada elemento envolvido.

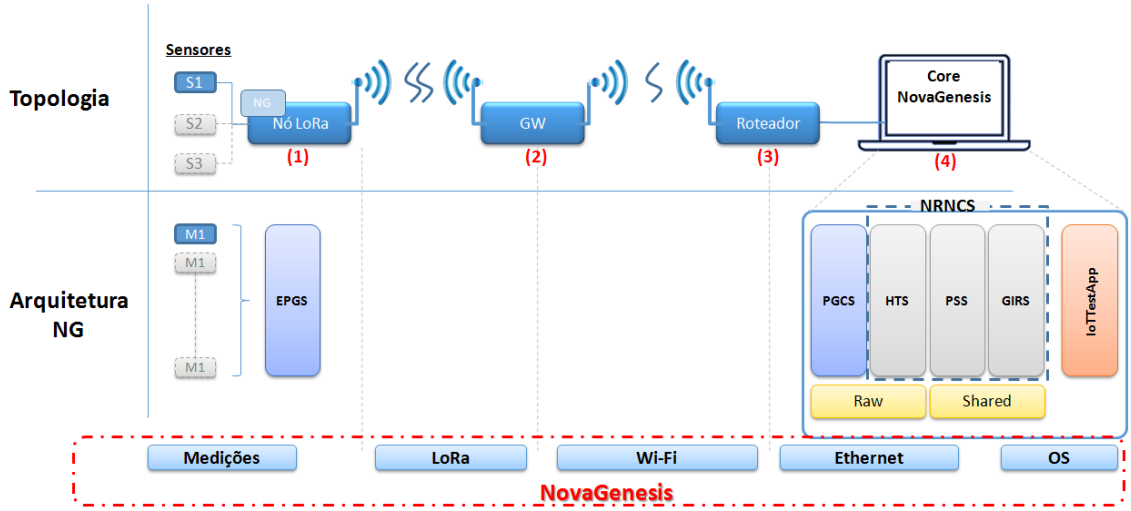



Figura 3.2: *Cenário da NG com LoRa incluindo Gateway.*
*A figura mostra outros serviços NG do core, como o PGCS e o NRNCS, ambos parte do núcleo da NG.*

Tabela 3.1: *Componentes do Cenário de teste.*

| **Componente** | **Descrição** | **Função** |
|---|---|---|
| EPGS | Embedded Proxy Gateway Service | Uma versão reduzida da NG para dispositivos embarcados. Responsável pela inicialização, exposição e publicação de dados coletados nas interfaces de entrada e saída onde estão conectados os sensores. |
| GW | Gateway LoRa Wi-Fi | Faz a adequação/tradução de mensagens LoRa e Wi-Fi, implementa controle de fluxo por meio de semáforos e controle de filas. |
| Roteador | Roteador Wi-Fi | Conecta o Gateway LoRa a rede local. |
| NG Core | Núcleo NovaGenesis | Núcleo da solução NG. Os módulos PGCS e NRNCS (HTS, PSS e GIRS) são responsáveis pelo controle, descoberta, exposição e gestão do ciclo de vida dos serviços. |
| IoTTestApp | Aplicação | Aplicação consumidora de dados de temperatura. Assina contrato com o PSS e com o EPGS. |

### 3.2.2 Definição dos recursos para PoC

Com o objetivo de encontrar no mercado os componentes de *hardware* e *software* mais adequados, que pudessem auxiliar na comprovação da hipótese desta Dissertação de Mestrado, alguns requisitos foram considerados: (a) utilizar plataforma aberta (*open-source*); (b) possuir recursos para um rápido desenvolvimento e implementação; (c) ser neutra do ponto de vista de monitoração, ou seja, não interferir ou manipular dados gerados durante os testes; e, (d) ser flexível para ajustes necessários caso identificados durante os testes.

#### 3.2.2.1 Do *hardware* para suportar o EPGS

Dentre as plataformas *open-source* pesquisadas no mercado as seguintes foram avaliadas: O "NUCLEO-L073RZ + P-NUCLEO-LRWAN1 – SX1272" da *Multitech* e o "ESP-32 LORA 915/868 Mhz + WIFI" da *Heltec Automation*.

Ensaios preliminares de validação das plataformas realizados em laboratório, demonstraram:

- O *hardware* da *Multitech* suportou embarcar o EPGS e os outros *software* necessários para este experimento. Contudo, requer um *Gateway*, "MTCDT-H5-210A" com interfaces LoRa e Ethernet, para interligar as redes LoRa e Ethernet. Foi identificado que ele não possui código aberto, estando limitado apenas aos parâmetros de configuração disponíveis em uma interface gráfica, o que restringe o desenvolvimento para o cenário proposto, além de não possibilitar monitoramento e identificação de problemas.
- Já o *hardware* da *Heltec* apresentou capacidade de memória e processamento suficiente para embarcar todos os *software* (EPGS, RTOS e os protocolos de comunicação LoRa) e possibilitou em adicional o desenvolvimento de um *Gateway* para ligar com a rede Ethernet, uma vez que o ESP-32 LoRa entrega uma plataforma aberta suportando desenvolvimento customizados. Também permite habilitar monitoração em tempo real, dando uma maior visibilidade na análise da integração das duas arquiteturas.

A Tabela abaixo ilustra de forma resumida, as principais características técnicas comparativas das duas plataformas analisadas, que contribuem com a escolha do *hardware* do ESP-32 LoRa.

Tabela 3.2: *Características técnicas ESP-32 e SX1272.*

| **Característica** | **SX1272** | **ESP-32 LoRa** |
|---|---|---|
| Modelo | STM32L073RZT6 in LQFP64 packege + SX1272 | ESP-32 com Wi-Fi e LoRa SX1276 868/915MHZ com Display Oled |
| Processador | ARM$^c$32-bit Cortex$^c$-M0 + MPU | Xtensa 32-Bit LX6 Dual Core |
| CPU *Clock* | De 32 KHz até 32 MHz max CPU | 80 à 240 MHz (Ajustável) |
| Memória | ROM: 6K, RAM: 20Kb e Flash Externa: 4Mb / 32-Bit | ROM: 448K, SRAM: 520Kb e Flash Externa: 4Mb / 32-Bit |
| Temperatura | -40 até 125 $^o$C | -40 até +85 $^o$C |
| Compatibilidade IDE | IDE Arduino | IDE Arduino / Espressif |
| Interfaces comunicação | Rede LoRa com o SX1232 | Bluetooth 4.2 / Wi-Fi 802.11 / Rede LoRa de até 3,6km |

Além do exposto acima, outros elementos da característica do ESP-32 LoRa também reforçaram a escolha do dispositivo como plataforma de desenvolvimento. Ele reúne em um único *hardware*, características que viabilizam a prova de conceito, tais como: (a) ser uma plataforma aberta para desenvolvimento; (b) possibilitar a distribuição de aplicações nos 2 núcleos de processamento; (c) possuir capacidade de memória suficiente para suportar os códigos do EPGS, do sistema operacional RTOS e do protocolos de comunicação; (d) ter suporte para vários protocolos utilizados em IoT; (e) ter capacidade de replicar os testes com ajustes das frequências para diferentes regiões do planeta; (f) ter um baixo consumo de energia, quando operando em modo *deep sleep*; (g) possibilitar a habilitação de monitoração dos processos para posterior análise; e (h) ser de baixo custo.
Demais características técnicas podem ser visualizadas no *datasheet* em [57].

#### 3.2.2.2 Dos demais elementos necessários para a PoC

Como apresentado na Figura Figura 3.2, além dos dispositivos para suportar o EPGS, outros elementos de *hardware* e *software* são necessários para esta implementação, monitoração durante todo o período de teste e tratativa dos dados que comprovarão esta hipótese.
Dentre os *software* necessários, destacam-se ferramentas que possibilitam: a captura de registros/*logs* exportados em diversos pontos da topologia; a seleção, a organização e a contextualização de dados aplicáveis na comprovação do experimento; e a compilação dos códigos dos programas a serem instalados nos diversos dispositivos.

A tabela 3.3, lista todos os recursos requeridos e utilizados na prova de conceito, apresentando de forma resumida suas principais funções.

Tabela 3.3: *Recursos de Software e Hardware para realização de testes da prova de conceito.*

| Recurso | Tipo | Qtde | Descrição |
|---|---|---|---|
| **ESP-32 LoRa** | HW/ FW | 2 | Um com função de ***NÓ* LoRa** com o *firmware* do EPGS e outro com a função de ***Gateway***. Ambos instalados em sistema operacional (SO) RTOS. |
| **Computador*** | HW/ SO | 1 | Computador com SO Linux Ubuntu versão 22.04, capacidade mínima de 6GB de memoria RAM e espaço livre em disco suficiente para instalação dos *software* aqui listados. |
| ***NovaGenesis*** | SW | 1 | O **Software da NovaGenesis** na versão disponível no github.. A versão considera ajustes necessários para utilização em LoRa. |
| ***Roteador*** | HW | 1 | Roteador Wi-Fi com suporte a 802.11n. |
| ***Eclipse*** | SW | 1 | O **Eclipse** foi a ferramenta base para o desenvolvimento dos códigos para o ESP-32 (EPGS e *Gateway*). Utilizou o SDK da Espressif com versão de IDE 2021-09. |
| ***CLion*** | SW | 1 | O **CLion** foi utilizado como compilador para NG minimizando possíveis variações com projetos anteriores. |
| ***Wireshark™*** | SW | 1 | Instalado no mesmo computador do *Core* da NG para monitorar as trocas de pacotes na rede local LAN. Facilitará em análise posteriores. |
| ***Teraterm*** | SW | 1 | Emulador de terminal implementado por software. Utilizado para coleta de registros/*logs* em porta serial-USB dos ESP-32 LoRa. Instalado no mesmo computador do *Core* NG. Facilitará em análise posteriores. |
| ***MS-Excel*** | SW | 1 | Ferramenta de edição de planilhas utilizada para organizar os registros/*logs* coletados para subsidiar análises comprovatória desta prova de conceito. |

**NOTA**:
* Para este experimento os *software* da NovaGenesis, Eclipse, CLion, Wireshark™, Teraterm e MS-Excel foram instalados em um mesmo notebook com a seguintes características: Processador Intel Core i5, com 2.67GHz—2.66GHz e memória RAM de 6GB.

#### 3.2.2.3 Parâmetros de configuração *Wireless*

De forma a garantir um replicabilidade dos testes realizados, foram definidos os seguintes parâmetros de configurações nos enlaces sem fio LoRa e Wi-Fi.

No trecho Wi-Fi, que interliga o ESP-32 com função de GW e o roteador, foi utilizado o padrão 802.11n em frequência 2.4GHz e adotado o canal 11.

Já no trecho LoRa foi adotado o SF 7 (SF7) com uma largura de banda de 500 KHz, que possibilita uma maior taxa de transmissão de dados (21.9 Kbps) com um *payload* de 222 Bytes. Nos testes foi utilizado o canal de comunicação LoRa como camada física, não sendo implementado nenhuma forma de controle de acesso e aplicação disponível no LPWAN.

Vale reforçar que esta característica do LoRa relativo ao tamanho do *payload* obriga a fragmentação e remontagem das mensagens pelo EPGS e NG. A tabela 3.4 ilustra a quantidade de fragmentos necessários a serem transmitido no canal LoRa.

| **Tarefa** | **Tamanho (Bytes)** | ***Nº de Frag. em LoRa*** |
|---|---|---|
| ***Hello*** | 341 | 2 |
| ***Exposition*** | 981 | 5 |
| ***Service Offering*** | 991 | 5 |
| ***Service Acceptance*** | 535 | 3 |
| ***Data Publishing*** | 991 | 5 |

Tabela 3.4: *Número de fragmentos de tarefas transmitidos em enlace LoRa.*

### 3.2.3 Plano de teste

Definidos os recursos a serem utilizados para implementar a arquitetura proposta para esta prova de conceito, um plano de teste foi elaborado objetivando a validação de elementos fundamentais para a arquitetura NovaGenesis e seu comportamento, quando utilizando uma rede de comunicação LoRa.
O plano leva em consideração a análise das etapas do ciclo de vida da NG, desde sua inicialização até a publicação de dados, avaliando a performance da arquitetura proposta.
Passos para desenvolvimento do plano:

1. **Inicialização do EPGS**
   - *a*) **Objetivo** (Para que fazer):
     Validar todas as etapas de inicialização do EPGS até a publicação dos dados, assegurando que o ele será iniciado somente após o estabelecimento do enlace LoRa.
   - *b*) **Execução** (Como fazer):
     Verificar nos *logs* do Wireshark™ se os pacotes/mensagens NG, trocados nas etapas do ciclo de vida do EPGS, seguem conforme apresentados na Figura 2.4, certificando se as características da LoRa impedem a evolução deste processo.
   - *c*) **Resultado Esperado** (O que esperar):
     O EPGS deverá respeitar o tempo para que o *NÓ* LoRa estabeleça o enlace e que todas as etapas do ciclo de vida da NG sejam concluídos com sucesso. Um arquivo contendo as publicações de medição de temperatura, “data.txt”, dever ser criado em um diretório do computador pela aplicação “IoTTestApp”.

2. **Continuidade do Serviço**
   *a*) **Objetivo** (Para que fazer):
   Garantir que o experimento consiga gerar números suficientes de amostras de publicações de dados, que subsidiarão a defesa desta hipótese.
   *b*) **Execução** (Como fazer):
   Verificar se após a conclusão das etapas de inicialização do EPGS, o arquivo "data.txt" continua sendo atualizado com novas linhas de medições de temperatura,verificando e um editor de texto ou **Browser** a inserção de novas linhas no arquivo.
   Acompanhar em tempo real por meio do Wireshark™ as mensagens de publicação de dados envidas pelo EPGS.
   *c*) **Resultado Esperado** (O que esperar):
   O número de sequência da amostra no arquivo "data.txt" seja incrementado, demonstrando que houve uma nova publicação de temperatura. Este número deverá ser equivalente ao identificado na mensagem do Wireshark™.
3. **Performance**
   *a*) **Objetivo** (Para que fazer):
   Avaliar a performance da arquitetura proposta garantindo a comprovação da hipótese de uma continuidade de serviço NG sem perdas significativas.
   *b*) **Execução** (Como fazer):
   Avaliar se houve descontinuidade ou inversão de sequência das amostras salvas no arquivo "data.txt", identificando os motivos destes desvios e pontuando seus ofensores.
   *c*) **Resultado Esperado** (O que esperar):
   Indicadores de desempenho da arquitetura: (i) pacotes/mensagens perdidas; (ii) fragmentos de pacotes/mensagens perdidas; (iii) desordenação de pacotes.
4. **Nível de Serviços**
   *a*) **Objetivo** (Para que fazer):
   Avaliar quais os níveis de serviço entregues pela NG para aplicações consumidoras. Os dados publicados nesta prova de conceito pelo EPGS, restringe-se a medições de temperatura.
   *b*) **Execução** (Como fazer):
   Identificar no arquivo "IoTTestApp_Core_SubRTT.dat" as informações/campos que demonstrem os níveis de serviço entregues pela NG à aplicação "IoTTestApp", avaliando os intervalo entre publicações, desvio médios e tendências.
   *c*) **Resultado Esperado** (O que esperar):
   Uma planilha formatada com os dados oriundos do arquivo "IoTTestApp _Core_SubRTT.dat", que possa suportar a geração de gráficos e/ou relatórios, relativos a este índice.

Para alcançar dados suficientes que possam comprovar a hipótese desta Dissertação de Mestrado, os registros/*logs* dos testes realizados devem conter número suficiente de amostra em um período ininterrupto. Desta forma, foi definido para estes testes, inter-

valos de 2 segundos entre publicações, o que significa, em 1 horas estará disponível cerca de 1800 registros de publicações de dados para análise. Testes preliminares de validação em outras periodicidades foram realizadas, por exemplo 5, 10, 30 segundos, contudo optou-se por esta periodicidade para conseguir o maior número de amostra num menor espaço de tempo, ou seja 2 segundos entre publicações. Para efeito de padronização e seleção dos testes a serem avaliados será adotado que, um teste válido terá uma quantidade mínima de 1800 amostras.

### 3.2.4 Implementação

Para identificar os pontos de ajustes em códigos ou parâmetros garantindo a integração entre estas duas arquiteturas, testes preliminares foram realizados, sem validade comprovatória, para assegurar que todas as etapas do ciclo de vida da NG estejam em condições de serem avaliadas.

Como premissa, preservou-se intacta toda a estrutura de código da LoRa, para assegurar que qualquer implementação ou ajustes sejam executados na arquitetura NG, comprovando a sua flexibilidade em se adequar a outras camadas de enlace, além das já citadas anteriormente.

As alterações de código ou parâmetros identificados nos testes preliminares serão apresentadas no decorrer da explanação.

#### 3.2.4.1 Esforço para integrar a NG em uma rede LoRa

Conforme abordado no Capítulo 2, a NovaGenesis foi construída com objetivo de ser flexível suficiente para suportar tecnologias emergentes, ou até mesmo interoperar com redes legadas. Neste sentido, o EPGS herdou também esta característica, porém em uma versão reduzida.
O protótipo atual do EPGS implementado opera sobre um enlace Wi-Fi, levando em consideração parâmetros necessários para seu correto funcionamento. A portabilidade deste código para operar em um enlace LoRa requer ajustes, devido suas características descritas no Capítulo 2.
Outro ponto a ser observado é a versão atual do EPGS, desenvolvida para o *hardware* do “NXPLPC1769”, o que exige uma validação e ajuste do código para ser embarcado no “ESP-32 LoRa”.

O protótipo atualizado do EPGS, para comprovação desta hipótese, inclui em seu código, modificações no processo de inicialização garantindo assim que o enlace LoRa já esteja ativo, uma vez que possui características próprias, tais como: janelas de transmissão e recepção limitadas, tamanho máximo de pacote (222 Bytes) e processo de auto descoberta para encontrar o *Gateway* que irá se conectar antes de iniciar qualquer transmissão ou recepção. A garantia de possuir um enlace LoRa estabelecido e operacional, é imprescindível, antes de disparar o processo de inicialização da NG. Desta forma, o EPGS expande a capacidade da FIA NG em trabalhar numa rede LoRa.
Testes preliminares também identificaram a necessidade de ajuste dos temporizadores da NovaGenesis, que definem o intervalo entre mensagens enviadas, assegurando que estes respeitem as janelas de transmissão no sentido do *downlink*, conforme abordado no Capítulo 2. Foi utilizada uma aplicação já desenvolvida para cenários IoT, ajus-

tando os tempo de intervalo entre mensagens para garantir e respeitar as janelas de transmissão. Isso demonstra a capacidade de adaptação da FIA NG a novos meios de comunicação, como por exemplo BLE, Zigbee, 5G, entre outros, que podem ser objetos de futuros estudos.

A Figura 3.3 ilustra os principais pontos de impactos no processo de inicialização da NG, quando utilizando LoRa, que serão discutidos nas próximas subseções. Nas demais etapas, exposição, oferta de serviço e publicação de dados não foram necessários ajustes do lado da NG. Nos testes preliminares foi verificado que a NG tratou de forma transparente a fragmentação e remontagem de mensagens NG, o que não exigiu nenhuma adaptação por parte da NG neste requisito.

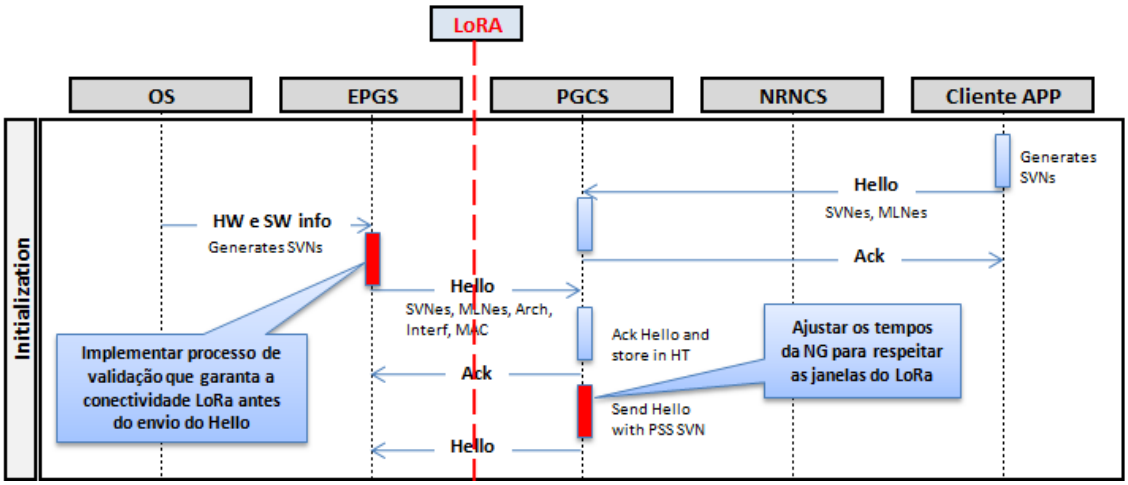



Figura 3.3: *Impactos do LoRa no processo de inicialização da NovaGenesis.*

### 3.2.4.2 Adequações EPGS e NG

Para atender aos pré requisitos exigidos pela LoRa, respeitando seu processo de inicialização e as janelas definidas para transmissões e recepção, foram necessários adequações dos códigos de *software* do EPGS e parametrizações da NG, garantindo uma maior aderência da FIA NG à rede LoRa. Os programas do EPGS e o da LoRa rodam de forma independente, o que requer avaliação detalhada para definir qual deles será o principal. A LoRa será mais um serviço de comunicação para a NG, assim como hoje são o Wi-Fi e a Ethernet, desta forma, sendo definido o EPGS o programa principal.
Na sequência serão abordados as adequações e implementações que viabilizam esta prova de conceito.

#### 3.2.4.2.1 Adaptações no Código do EPGS

A versão do EPGS disponível em [58], foi utilizada como base de desenvolvimento. O primeiro desafio foi, conciliar a convivência de dois programas, o do EPGS e o do LoRa, rodando simultaneamente em um mesmo sistema operacional; mantendo e respeitando suas necessidades de interrupções e tarefas, sem trazer prejuízo às suas funcionalidades. O sistema operacional RTOS, teve papel importante neste desenvolvimento, uma vez que possibilita o gerenciamento das tarefas requeridas pelo dois programas, de forma

independente e harmônica.
O segundo desafio desta integração foi, encontrar os pontos do código que possibilitasse a integração dos dois programas por meio de interrupções..
Também foi necessário implementar semáforos que garantissem que o EPGS respeitasse as janelas de transmissão e recepção da LoRa, uma vez que o enlace LoRa precisa estar ativo para que o EPGS comece seu processo de inicialização.
As Figuras 3.4 e 3.5 ilustram alguns trechos de código inseridos no programa do EPGS para inter-funcionar com a LoRa.

```
EPGS_Controller

...
if (ng_strcmp (ngEPGS->MyNetInfo->Stack, NG_STACK_ETHERNET) == 0
            || ng_strcmp (ngEPGS->MyNetInfo->Stack, NG_STACK_WIFI) == 0
            || ng_strcmp (ngEPGS->MyNetInfo->Stack, NG_STACK_LORA) == 0)
...
```

Figura 3.4: *Inclusão da opção de LoRa no EPGS_Controller.*

```
EPGS_Defines

...
static const char SCN_NG_DOMAIN[] = "Intra_Domain";
static const char NG_STACK_ETHERNET[] = "Ethernet";
static const char NG_STACK_WIFI[] = "Wifi";
static const char NG_STACK_BLUETOOTH[] = "Bluetooth";
static const char NG_STACK_LORA[] = “Lora“;

#define NG_USE_ETHERNET 0
#define NG_USE_LORA 1
#define NG_USE_WIFI 0
#define NG_USE_BLE 0
...
```

Figura 3.5: *Inclusão da opção de LoRa no EPGS_Defines.*

Os trechos do código circulados em vermelho indicam algumas das linhas de comando inseridas no código do EPGS, incluindo a opção de LoRa.

#### 3.2.4.2.2 Parâmetros NG

Nos testes preliminares do EPGS já embarcado no ESP-32 LoRa, foi identificado que as tarefas que compõem o ciclo de vida do EPGS não alcançavam a publicação de dados.
Através de ensaios realizados no protótipo foi possível identificar os ajustes necessários nos parâmetros que definem os intervalos entre as tarefas a serem realizadas na inicialização do PGCS, foi possível garantir que o EPGS concluísse todo o processo, dando início à publicação de dados que contém medições de temperatura.
A Figura 3.6 ilustra os valores adotados para garantir a convivência da NG em um enlace LoRa.

Os parâmetros acima circulados em vermelho foram acrescentados no processo de inicialização do PGCS de forma a garantir os intervalo entre as

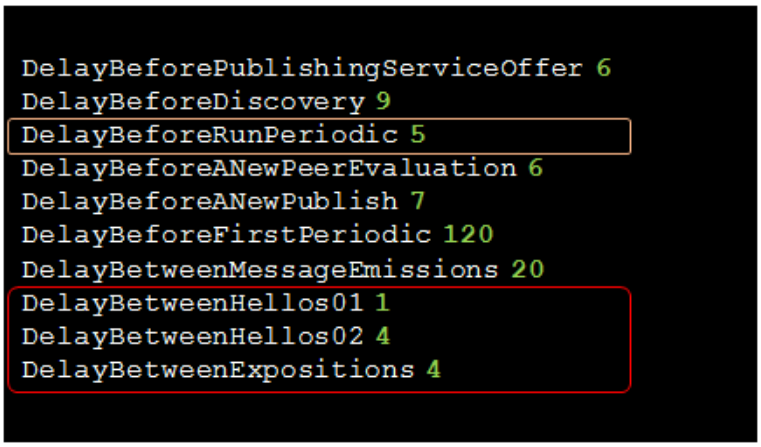



Figura 3.6: *Parâmetros de inicialização do PGCS.*

tarefas para um enlace LoRa. Ex., "DelayBetweenHellos01" indicam que o intervalo entre *Hellos* seja de 5 segundos. Ele é calculado multiplicando o valor 1 x 5, valor do "DelayBeforeRunPeriodic". O mesmo racional se replica para os demais parâmetros de tempo, com a diferença que o "DelayBetweenHellos02" é utilizado após o processo de exposição ter sido concluído.

#### 3.2.4.2.3 *Script* de inicialização da aplicação NG

E por último, foram definidos e ajustados o *script* que dá início *bootstrapping* da NG, garantindo que todos seus serviços internos estejam operacionais, e que a aplicação consumidora "IoTTestApp" interessada em assinar dados de medição de temperatura já tenha o contrato assinado com o PSS; aguardando apenas as notificações de um novo dado publicado pelo EPGS. A Figura 3.7 ilustra o *script* utilizado para a inicialização da NovaGenesis e da aplicação "IoTTestApp".

```
gnome-terminal
--tab --title="PGCS" -e "/bin/bash -c 'cd $BASE/cmake-build-debug;sh clean.sh;./PGCS $BASE/IO/PGCS/1
Intra_Domain -pc Wi-Fi Intra_Domain wlp18s0 3c:71:bf:fc:b8:c8 200;exec bash'" \
--tab --title="NRNCS" -e "/bin/bash -c 'cd $BASE/cmake-build-debug;sleep 10;./NRNCS $BASE/IO/NRNCS/;exec bash'" \
--tab --title="IoTTestApp1" -e "/bin/bash -c 'cd $BASE/cmake-build-debug;sleep 60;./IoTTestApp IoTTestApp1
$BASE/IO/IoTTestApp/;exec bash'"
```

Figura 3.7: *Script de inicialização para NG.*

Os elementos destacados em vermelho indicam o caminho para alcançar o EPGS, ou neste protótipo, o *Gateway* que fará a comunicação com o EPGS.

### 3.2.4.3 Desenvolvimento de um *Gateway* LoRa / Wi-Fi

Devido o ESP-32 LoRa, utilizado com a função de *Gateway*, não possuir interface Ethernet para conexão direta a rede local, foi necessário o desenvolvimento de um *Firmware* que possibilitasse o encaminhamento das mensagens oriundas do trecho LoRa para Wi-Fi e vice-versa, embarcado no próprio ESP-32 LoRa. Com a

implementação do GW foi possível viabilizar a comunicação integral da arquitetura proposta para esta prova de conceito, garantindo a comunicação em ambos sentidos, desde o *NÓ* EPGS até o núcleo da NovaGenesis.

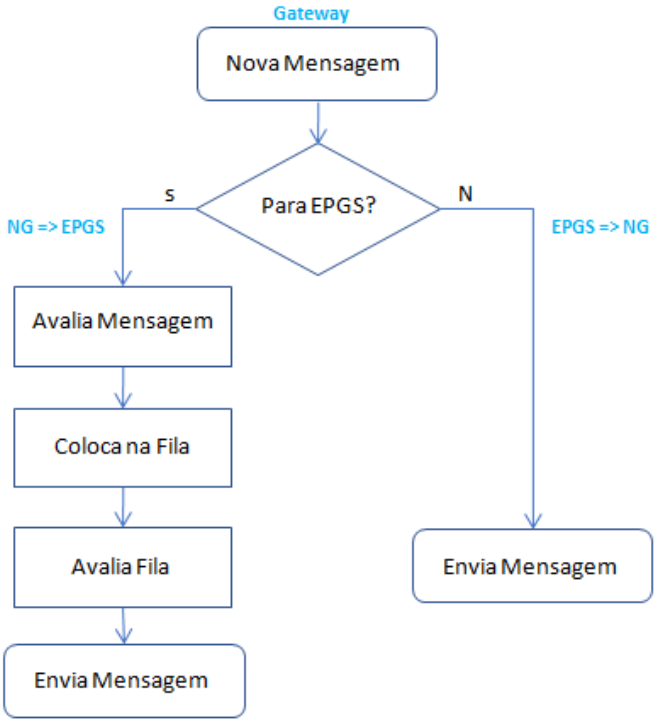



Figura 3.8: *Macro Fluxo Mensagens NG implementados no Gateway.*

No desenvolvimento do *Gateway* foram consideradas as premissas para obedecer os intervalos de transmissão disponíveis no *downlink*, garantindo que as mensagens sejam enviadas para o EPGS. A Figura 3.8 ilustra de forma macro a rotina criada para avaliar a disponibilidade de uma janela de transmissão em ambos sentidos de comunicação. Uma fila para armazenar as mensagens enviadas ao EPGS foi necessária, assegurando assim seu envio sempre que uma janela esteja habilitada, evitando colisão.
O método de controle de acesso ao meio não foi considerado na implementação do *Gateway*, o que ampliaria ainda mais sua capacidade em tratar mensagens para um número maior de *NÓS* EPGS, ou seja, neste protótipo, apenas um único *NÓ* é suportado. Mensagens envidas pelo EPGS para a NG são encaminhadas diretamente pelo GW para a transmissão em Wi-Fi, sem a necessidade de tratativa adicional para este sentido de tráfego.

Abaixo serão apresentados os fluxos e trechos de código criados para garantir esta interoperabilidade entre o LoRa e o Wi-Fi.

#### 3.2.4.3.1 Tráfego no sentido NG => EPGS

A figura 3.9 ilustra o macro fluxo desenvolvido no GW para realizar validação de um mensagem NG.

Com objetivo evitar congestionamento no *link* LoRa por mensagens enviadas pelo núcleo da NG para o *NÓ* EPGS, foram implementados no *firmware*

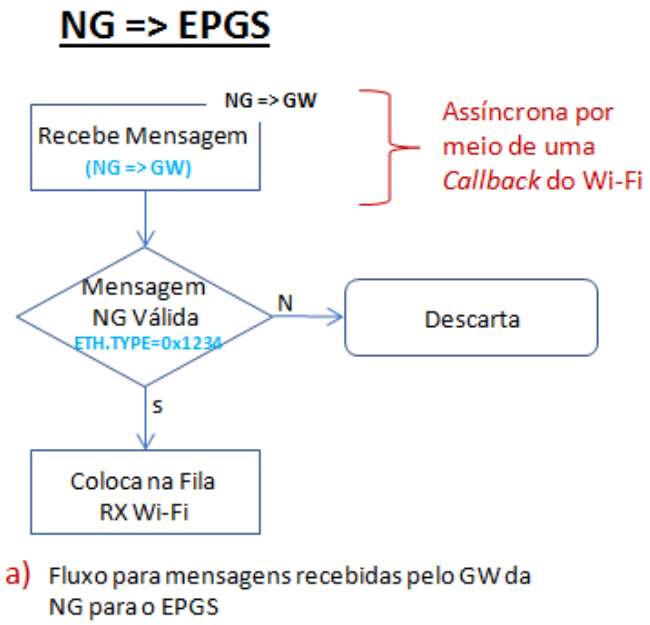



Figura 3.9: *Macro Fluxo Mensagens NG implementados no Gateway (NG => EPGS).*

do GW mecanismos que garantissem: a **legitimidade** de uma mensagem NG, e a **disponibilidade** de janela de transmissão para envio ao EPGS.
Toda vez que o GW receber uma mensagem oriunda da rede local, ele avalia se esta contem o "*Ethertype*=0x1234", o que indica ser uma mensagem NG. Se a mensagem for válida, esta é armazenada em uma fila "RX Wi-Fi". Caso não contenha o *Ethertype* válido a mensagem é descartada.

A figura 3.10 ilustra o macro fluxo desenvolvido no GW para envio das mensagens NG no enlace LoRa.

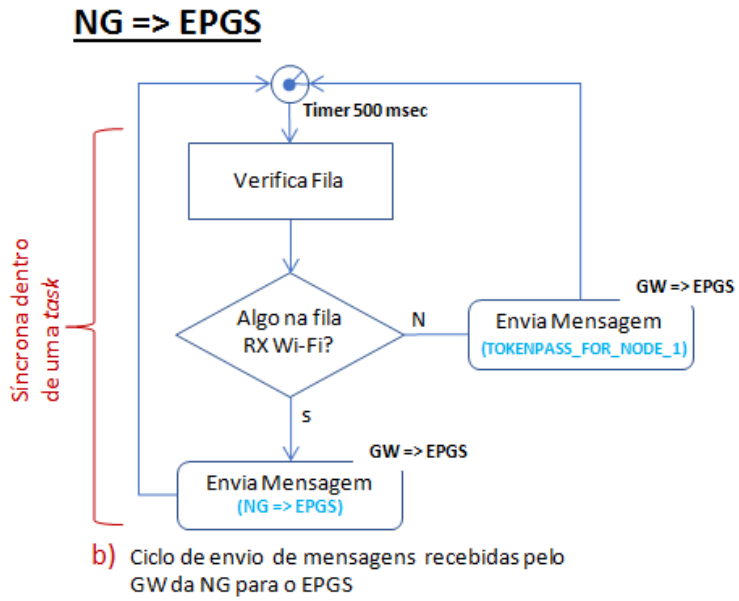



Figura 3.10: *Macro Fluxo Mensagens NG implementados no Gateway (NG => EPGS).*

Uma vez que o intervalo entre publicações de dados foi definido com 2 segundos, com o objetivo de minimizar possíveis colisões, foi estabelecido que a cada intervalo de 500 milissegundos uma *task* verifica se há mensagens disponíveis na fila "RX Wi-Fi". Caso haja, o GW envia para ser transmitida na interface do LoRa, caso contrário o GW envia uma mensagem de *token* para o EPGS com a informação "TOKENPASS FOR NODE 1" no *payload*, indicando que não há nenhuma mensagem NG para ser transmitida, disponibilizando assim o meio para envio pelo EPGS.
Este ciclo de transmissão em janelas ocorre no sentido do *downstream*, ou seja do GW para o EPGS devido o enlace LoRa exigir um maior controle, conforme suas limitações comentadas no **Capítulo 2**.

#### 3.2.4.3.2 Tráfego no sentido EPGS => NG

A Figura 3.11 ilustra o macro fluxo implementado no GW para encaminhamento de mensagens NG originadas no EPGS com destino a NG.

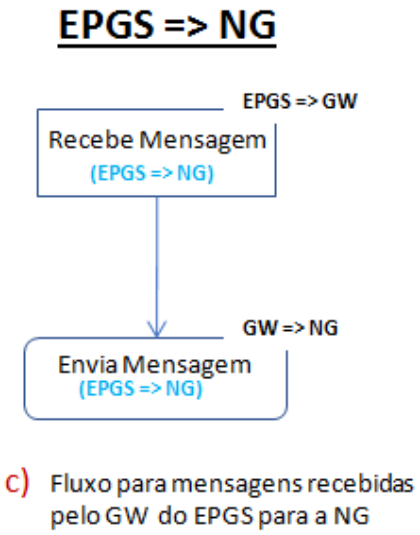



Figura 3.11: *Macro Fluxo Mensagens NG implementados no Gateway (EPGS => NG).*

Como no enlace Wi-Fi a vazão é maior, possuindo capacidade de tráfego em ambos sentidos sem necessidade de se preocupar com janelas de transmissão, não foi necessário a implementação de filas para armazenar mensagens NG. Não houve necessidade de criar um processo de validação das mensagens NG, já que apenas os *NÓS* EPGSs autenticados durante o processo de inicialização do LoRa irão transmiti-las.

**INFORMAÇÃO ADICIONAL**. Nos códigos do EPGS e do *Gateway* foram habilitados funções para impressão na porta serial das mensagens trocadas entre os dispositivos EPGS e *Gateway*, assim como entre o *Gateway* e núcleo da NG.

### 3.2.5 Experimentação - Teste de validação

Esta seção estará dividida em duas partes: uma que apresenta o passo a passo utilizado para realização dos teste em bancadas; e uma segunda que valida se o experimento contem registros/*logs* suficientes para análise.

#### 3.2.5.1 Passo a passo para realização dos teste

Todos os *software* listados em 3.3, foram instalados em seus devidos *hardware*. O ambiente foi preparado em bancada conforme ilustrado na Figura 3.12, de tal forma a possibilitar acompanhamento em tempo real.

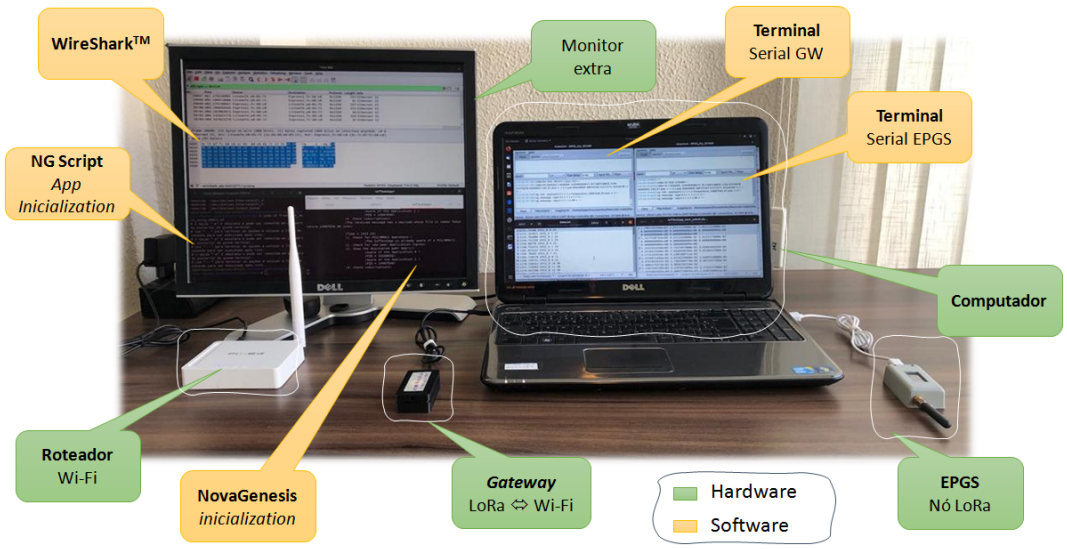



Figura 3.12: *Ambiente de teste em laboratório.*

A sequência descrita abaixo foi seguida para o sucesso do teste. Não serão relatados aqui os procedimentos de compilação dos *software* da NovaGenesis e do *firmware* do EPGS, mas somente a sequência de ações necessárias, desde a inicialização da NG até a coleta dos resultados dos testes.
A avaliação dos registros/*logs* coletados serão tratados no **Capítulo 4**.

- **Passo 1:**
  - Para garantir a coleta dos registros/*logs*, os *software* Wireshark™ e Teraterm devem estar operacionais antes de iniciar os testes, independente da sequência de inicialização.
  - Duas janelas do emulador de terminal (Teraterm) deverão ser abertas para coletar registros/*logs* do EPGS e o *Gateway*.
  - A rede local Wi-Fi deve estar operacional e com o computador registrado no SSID criado para este experimento.
  - No intuito de evitar possíveis tráfegos indesejados oriundos da *Local Area Network* (LAN) ou da internet *Wide Area Network* (WAN), todos os cabos de rede do roteador foram removidos, permanecendo apenas a rede Wi-Fi operacional.

- **Passo 2:**
  - Com o notebook conectado à rede Wi-Fi, executar o *script* de inicialização da NG, definindo sua sequência correta e os temporizadores necessários entre cada etapa.
  - No diretório onde foi instalado a NG, acessar a pasta "`...\ng\Scripts\Simple`" e abrir o terminal. Executar o *script* utilizando a sequência de comandos: "`sudo sh Clean.sh`" para limpar registros de testes anteriores e o "`sudo sh frodo_iot_test_using_NRNCS.sh`" que executa o *script*.
  - Automaticamente uma nova tela do terminal será aberta apresentando os serviços que serão inicializados.
  - Aguardar até que todos os serviços sejam descobertos pela NG. Isso acontecerá quando a tela do terminal "IoTTestApp1" imprimir os dados. Tempo estimado de 2 minutos.
- **Passo 3:**
  - Conectar o ESP-32 LoRa com função de *Gateway* à porta serial-USB do computador, que além de alimentar o dispositivo, é utilizada como interface para coleta de registros/*logs*.
  - Iniciar a coleta pelo emulador de terminal correspondente a porta serial indicada na aplicação. Parte-se do pressuposto que há conhecimento da utilização de ferramentas de emulação de terminal.
  - Vale ressaltar que as configurações da rede para acesso ao Wi-Fi, como SSID e *Password*, foram previamente configuradas no código do *Gateway*.
  - Informações de inicialização do *hardware* assim como mensagens NG enviadas pelo PGCS, serão apresentadas na tela do emulador de terminal.

- **Passo 4:**
  - Por último, o *NÓ* EPGS é conectado a outra porta serial-USB, que alimentará o dispositivo e servirá para coletar os registros/*logs*.
  - Deverá ser iniciado o emulador de terminal selecionando a porta serial correspondente a este novo dispositivo. Neste momento é possível verificar a inicialização do *hardware* do ESP-32 LoRa, com função de EPGS. Em seguida são apresentadas na tela as trocas de mensagens entre o EPGS e o PGCS.

É importante observar se as ferramentas, Wireshark™ e Teraterm estão operacionais e coletando registros/*logs* das mensagens trocadas entre o EPGS e o núcleo da NovaGenesis.
Ao finalizar o teste, os registros/*logs* coletados pelas ferramentas deverão ser salvos em padrão ".txt" ou ".csv", para posterior tratativa no Excel.

Estas informações coletadas e salvas das portas seriais pelo emulador de terminal, bem como os registros salvos do Wireshark™, nortearão as avaliações comprobatória da hipótese dessa Dissertação de Mestrado. Também auxiliarão na identificação de

problema durante os testes.
Importante que estes passos sugeridos sejam seguidos para possibilitar a coleta dos registros/*logs* gerados por todos os elementos da topologia de teste, garantindo ao EPGS concluir todas etapas do ciclo de vida, até iniciar a publicação dos dados de medição de temperatura que deverão ser contínuos.

#### 3.2.5.2 Registros e *Logs* dos teste

Com todos os recursos devidamente operacionais, espera-se coletar o máximo de registros/*logs* em todas as etapas do ciclo de vida da NG. Caso não se tenha amostras suficientes, conforme definido na subseção 3.2.3, o teste deverá ser refeito iniciando sempre do passo 1.

Para uma melhor compreensão dos resultados a serem apresentados no **Capítulo 4**, se faz necessário um melhor entendimento dos arquivos gerados contendo os registros/*logs* coletados durante os testes.
No decorrer desta seção serão detalhados os arquivos e os campos.

##### 3.2.5.2.1 Sobre o arquivo "data.txt"

O arquivo "data.txt", é gerado pela aplicação "IoTTestApp" no processo de publicação de dados pelo EPGS e armazena as seguintes informação: (a) o registro do ***Timestamp*** de quando as publicações foram gravadas; (b) o **nome do *NÓ*** IoT que publicou a medida; (c) o **número de sequência** da publicação; e (d) a **medida instantânea da temperatura** coletada.
Um exemplo do arquivo é ilustrado na 3.13, sendo que as letras sinalizadas em cada coluna representam as informações detalhadas acima.

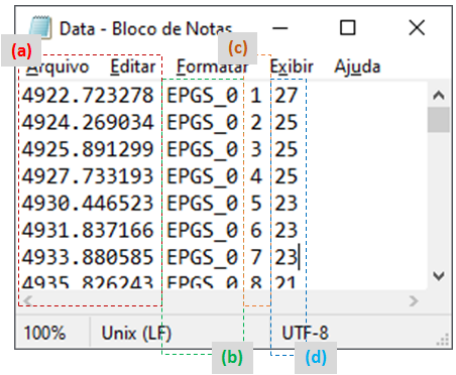



Figura 3.13: *Recorte do arquivo data.txt na aplicação IoTTestApp da NovaGenesis.*

##### 3.2.5.2.2 Sobre o arquivo "IoTTestApp_Core_SubRTT.dat"

O arquivo "IoTTestApp_Core_SubRTT.dat" também é gerado pela aplicação "IoTTestApp" e mede indicadores de performance de serviço. São calculados com base no tempo de entrega de uma nova publicação de dados, enviadas pelo PSS para aplicação consumidora "IoTTestApp". O tempo entre o recebimento de uma notificação envida pelo PSS para a aplicação "IoTTesteApp" e o recebimento do dado publicado, é denominado como *Round Trip Time* (RTT).

A Figura 3.14 ilustra as premissas da aplicação "IoTTestApp" para cálculo dos indicadores.

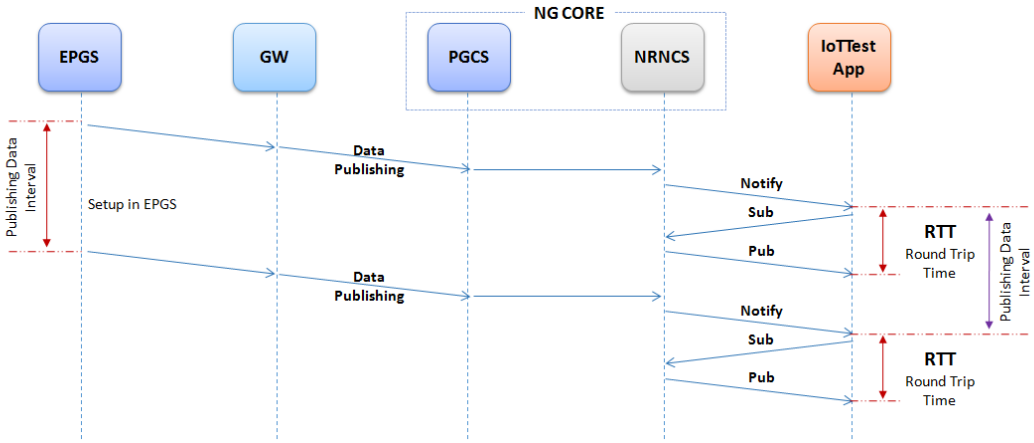



Figura 3.14: *Fluxo de mensagens NG para cálculo do RTT*

Ele armazena as seguintes métricas: (a) o ***Timestamp*** registra o momento em que cada amostra de medida foi recebida; (b) o **RTT instantâneo** de cada mensagem de publicação de dados; (c) a **Média aritmética do RTT** de todas publicação; (d) o **Desvio padrão**, é uma medida estatística da variação ou dispersão de cada RTT; (e) o **Erro padrão**, representa uma medida estatística de desvio entre cada amostra e a média de todas amostras; (f) o **Intervalo de confiança (CI)**, é uma medida estatística que estabelece uma faixa onde uma amostra pode ser encontrada; (g) o **Limite mínimo** define o menor valor para para CI; e por ultimo (h) o **Limite máximo** o maior valor para um CI.

O indicador de **RTT instantâneo**, informa o tempo medido desde o instante em que a aplicação recebeu uma mensagem de notificação até o recebimento da publicação do dado, contudo esta medição não reflete o ocorrido durante todo o tempo do experimento, desta forma, o outro índice calculado com base na **Média aritmética do RTT** das amostras instantâneas, demonstra qual é a tendência das publicações ao longo do experimento.
Com as variações entre estas duas medidas, RTT Instantâneo e a Média Aritmética, calcula-se o **Desvio padrão** utilizando métodos estatísticos, assim como o **Erro padrão** destas medidas.
A aplicação "IoTTestApp" calcula o intervalo de confiança, indicando uma faixa onde uma próxima medida de RTT pode ser encontrada, apontando para uma tendência. Desta forma, a aplicação calcula os **Limites mínimos e máximos** de cada publicação, assim como seu **intervalo de confiança**, representado como "***Low Limit***", "***Upper Limit***" e "***Confidence Interval***".
As fórmulas de cálculo destes indicadores podem ser melhor entendidas em [41].

A Figura 3.15 ilustra estes indicadores, sendo que as letras sinalizadas em cada coluna representam as informações detalhadas acima.

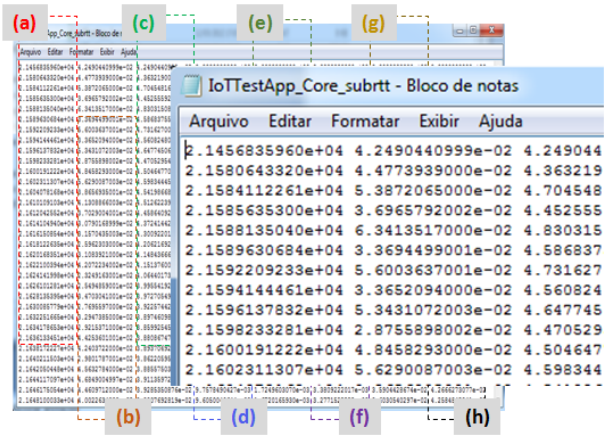



Figura 3.15: *Recorte do arquivo data.txt na aplicação IoTTestApp da NovaGenesis.*

#### 3.2.5.2.3 Sobre os pacotes *Ethernet* coletados na rede local

O Wireshark™ instalado em um computador/notebook conectado à rede local tem visibilidade a todos os pacotes *Ethernet* trafegados na rede, não gerando nenhuma interferência ou alteração dos pacotes. Nesta prova de conceito o Wireshark™ foi configurado com um filtro para apresentar apenas os pacotes NG que utilizam o"*Ethertype*=0x1234", minimizando a quantidade de registros a serem visualizados e analisados posteriormente.
A Figura 3.16 ilustra uma tela do Wireshark™ apresentando uma mensagem de publicação de medição de temperatura.

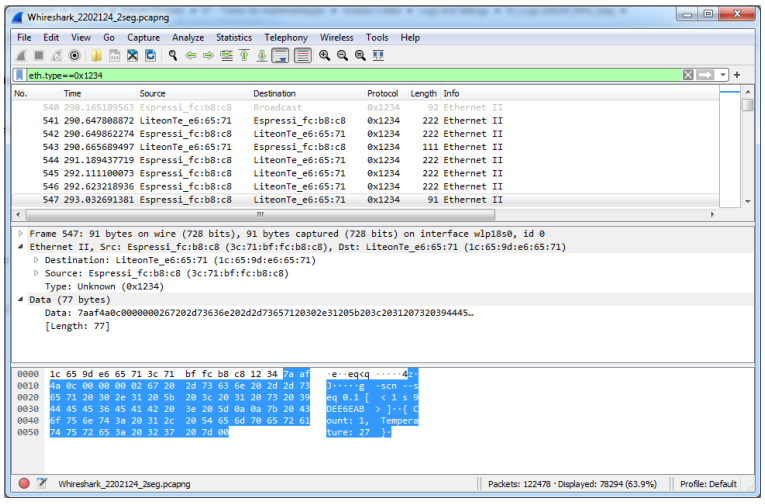



Figura 3.16: *Recorte do arquivo data.txt na aplicação IoTTestApp da NovaGenesis.*

Os registros/*logs* são exportados para um arquivo ".csv" que posteriormente serão trabalhados. Para facilitar o processo de busca pelas informações desejadas e a correlação com outros arquivos, por meio de campos chaves, este arquivo ".csv" é importado para o Excel dando origem a um novo arquivo formado por colunas e linhas que serão apresentadas na sequência. A coluna (A) contem um número de sequência, a coluna (B) o *Timestamp* gerados pela aplicação Wireshark™, as colunas (C) e (D) indicam a origem

e o destino dos pacotes coletados respectivamente. As colunas (E) e (F) apresentam o"*Ethertype*=0x1234" e o tamanho do pacote, e a coluna (G) a informação da interface utilizada.
Este campos auxiliam na descendência de outras colunas (H. I, J, K e L), pós processadas de forma manual, que subsidiarão a análise comprobatória deste trabalho. É possível observar na linha 27, destacada em amarelo, que foi identificado que o terceiro fragmento da segunda publicação de medição de temperatura foi perdido. As colunas descritas acimas são ilustrados na Figura 3.17.

| A | B | C | D | E | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|
| No. | Time | Source | Destination | Protocol | Length | Info | Intervalo | Nº Amost | Etapa / Fragmento | Tempo de execução de ca | Tempo total/parcial d |
| 292 | 204,9420865 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,407777 | | Service Offering | 1,844105051 | |
| 311 | 223,0679068 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 103 | Ethernet II | 18,12582 | | Service Acceptance | | |
| 312 | 223,5849355 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,517029 | | Service Acceptance | 0,517028672 | |
| 346 | 266,1793844 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 198 | Ethernet II | 42,59445 | | Broadcast | | |
| 347 | 266,5876561 | Espressi_fc:b8:c8 | Broadcast | 0x1234 | 222 | Ethernet II | 0,408272 | | Broadcast | 0,4082717 | |
| 348 | 266,9981343 | Espressi_fc:b8:c8 | Broadcast | 0x1234 | 92 | Ethernet II | 0,410478 | 0 | Data Publishing - Frag1 Temperature | | 83,86701095 |
| 349 | 267,5187823 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,520648 | | Data Publishing - Frag2 Temperature | | |
| 350 | 267,9205196 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,401737 | | Data Publishing - Frag3 Temperature | 0,922385282 | |
| 351 | 268,5343718 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,613852 | 1 | Data Publishing - Frag1 Temperature | | 1,536237478 |
| 352 | 268,9417369 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,407365 | | Data Publishing - Frag2 Temperature | | |
| 353 | 269,4553462 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 91 | Ethernet II | 0,513609 | | Data Publishing - Frag3 Temperature | 0,920974378 | |
| 356 | 270,0680852 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,612739 | 2 | Data Publishing - Frag1 Temperature | | 1,533713393 |
| 359 | 271,0959942 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 1,027909 | | Data Publishing - Frag2 Temperature | | |
| | 271,555414 | | | | | | | | Data Publishing - Frag3 Temperature | 1,487328803 | |
| 360 | 272,0148338 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 91 | Ethernet II | 0,91884 | 3 | Data Publishing - Frag1 Temperature | | 1,946748607 |
| 361 | 272,5283978 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,513564 | | Data Publishing - Frag2 Temperature | | |
| 362 | 272,9357355 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,407338 | | Data Publishing - Frag3 Temperature | 0,920901656 | |
| 365 | 273,5510909 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 91 | Ethernet II | 0,615355 | 4 | Data Publishing - Frag1 Temperature | | 1,53625712 |
| 366 | 274,0703594 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,519269 | | Data Publishing - Frag2 Temperature | | |
| 367 | 274,4746178 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 222 | Ethernet II | 0,404258 | | Data Publishing - Frag3 Temperature | 0,923526859 | |
| 372 | 276,1098556 | Espressi_fc:b8:c8 | LiteonTe_e6:65:71 | 0x1234 | 91 | Ethernet II | 1,635238 | 5 | Data Publishing - Frag1 Temperature | | 2,558764653 |

Figura 3.17: *Recorte do arquivo pós processado do Wireshark*$^{TM}$.

#### 3.2.5.2.4 Sobre os registros/*Logs* da porta serial do EPGS e do GW

Como objetivo de ter um acompanhamento em tempo real e guardar registros de ações executadas pelo programa em partes estratégicas do código do EPGS e do GW, foram habilitados funções de impressão (comando printf) de mensagens para uma porta de saída, no ESP-32 a porta USB além alimentar o dispositivo é utilizada como interface serial para imprimir os dados.
Neste experimento, a aplicação Teraterm gera o *log* contendo as impressões que são salvas em um arquivo ".txt". Cada arquivo gerado pode conter algumas milhares de linhas de impressão.
Para facilitar a tratativa destes arquivos, eles são importados para o Excel e depois convertidos no padrão de planilha, o que possibilita uma forma mais fácil para trabalhar os registros que subsidiarão a análise dos experimentos. Importante ressaltar que os registros trabalhados não foram modificados, mas mantidos em sua forma original, possibilitando o rastreio das informações.
A Figura 3.18 e 3.19 ilustram exemplos de linhas de impressão dos arquivos ".txt". Nela é possível observar que cada linha é precedida por um *Timestamp*, que será de fundamental importância para identificação e correlação entre os diferentes arquivos a serem processados.

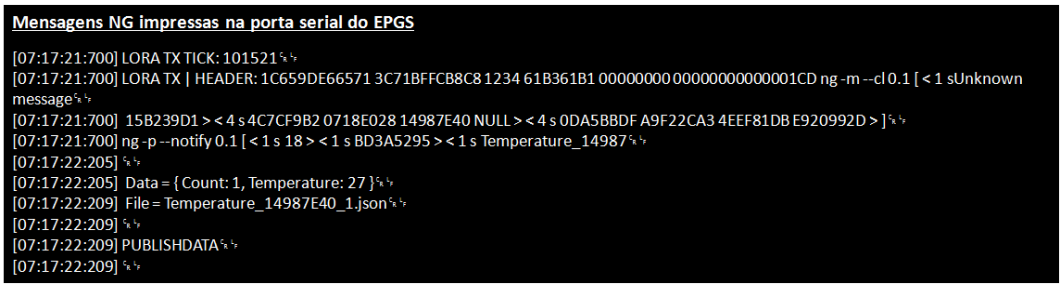



Figura 3.18: *Recorte do arquivo gerado pelo Teraterm com os logs de impressão na porta serial do EPGS.*

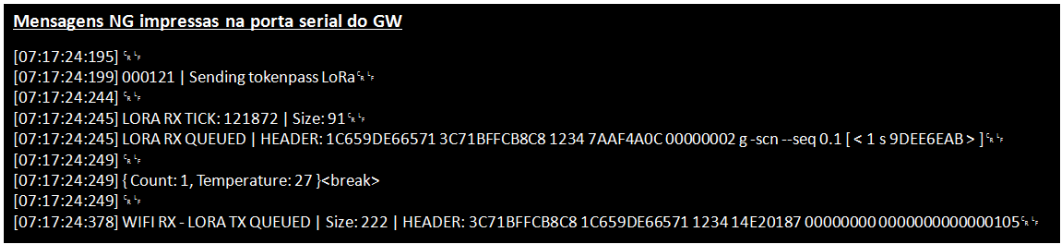



Figura 3.19: *Recorte do arquivo gerado pelo Teraterm com os logs de impressão na porta serial do GW.*

### 3.2.6 Resumo

Neste capítulo foi definido a metodologia adotada para viabilizar os testes em laboratório (bancada), que comprovará a viabilidade de integração da NG à LoRa, apresentando as etapas definidas desde o planejamento até a realização dos testes.
Foi estabelecida uma topologia de teste para prova de conceito, considerando coletas de registros/*logs* em diversos pontos de forma a obter o máximo de dados para a comprovação da hipótese desta Dissertação de Mestrado.
Foram apresentadas as dificuldades encontradas para a integração destas duas arquiteturas, demonstrando os pontos de ajustes na versão atual da NG e do EPGS para operar em uma rede LoRa. Também foi exposto sobre o *Gateway* desenvolvido utilizando o *hardware* do ESP-32 LoRa, interligando as redes de comunicação LoRa a Wi-Fi.
Para um melhor entendimento dos resultados obtidos das análises dos dados processados que serão apresentados no próximo capítulo, foram detalhados os arquivos gerados das coletas de registros/*logs* dos diversos pontos de monitoração.

# Capítulo 4

# Análise dos dados

NESTE capítulo serão abordados os resultados obtidos da análise das amostras coletadas dos testes realizados seguindo a metodologia definida no Capítulo 3, que serão apresentados de forma estruturada.

Os resultados dos testes demonstraram a viabilidade de implementar uma arquitetura FIA NG utilizando uma rede LoRa; embora no segmento da rede Wi-Fi tenha sido observado um resultado diferente do esperado. Fato este que será melhor detalhado no decorrer do capítulo.

Os seguintes pontos serão abordados adiante:

- A **performance** de toda solução analisada, a perda de mensagens e fragmentos NG, fragmentação e remontagem de mensagens NG;
- Validação de todo **Ciclo de Vida** do EPGS, incluindo a **continuidade do serviço**;
- O **nível de serviço** entregue pela NovaGenesis para uma aplicação que possui um contrato assinado com NG.

## 4.1 Resultado das coletas de registros/*logs*

A comprovação da hipótese desta Dissertação de Mestrado está baseada em: (a) amostragem de **registros/*logs* na interface serial** do segmento, que conecta o *NÓ* EPGS ao GW, indicados pelos componentes 1 e 2 da Figura 3.2; (b) amostragem de **pacotes *Ethernet*** trocados no segmento que conecta o *Gateway* LoRa/Wi-Fi ao núcleo da NG, onde também encontra-se a aplicação "IoTTestApp", sendo representados pelos componentes 3 e 4 na Figura 3.2, onde um filtro para "*Ethertype*=0x123" no Wireshark™ facilita a visualização dos pacotes NG; (c) no **arquivo "data.txt"** gerado pela aplicação "IoTTestApp" contendo as medições de temperatura publicadas pelo EPGS; e, (d) o **arquivo "IoTTest_Core_subRTT.dat"** também gerado pela aplicação "IoTTestApp", que registra os indicadores de performance relativos a assinatura de uma amostra de temperatura, armazenados no cache de rede NRNCS.

## 4.2 Metodologia de análise dos dados

Após importados os arquivos brutos, são realizados filtros para obter apenas os dados a serem moldados em um formato útil para analise. O resultado é, um arquivo único com diferentes planilhas, sendo que cada uma representa seus arquivos brutos originais.
As planilhas geradas possuem campos em comum que facilitam a correlação entre elas, por exemplo, o ***timestemp*** inseridos pelos programas de coleta dos registros/*logs* e o "**campo de numeração de sequência**" que é enviada pelo EPGS durante a publicação de dados e identificado como *Count*, como exemplo "$[07 : 17 : 24 : 249]\{$ *Count: 1, Temperature: 27* $\}$".
Os registros/*logs* foram coletados nos *software* instalados em um mesmo computador facilitando a correlação entre as planilhas, mesmo com pequenas variações de tempo no *timestemp*. Essas variações se dão devido ao tempo de transmissão ou processamento de cada fase ou segmento do teste realizado.
De posse das planilhas estruturadas com os dados selecionados, foram avaliadas as informações, possibilitando elaborar e apresentar relatórios e gráficos que comprovarão a hipótese.
Pode-se separar os resultados gerados após este processamento no Excel em dois grupos de acordo com seus arquivos de origem: Um que apresenta informações que possibilitam a analise do **comportamento e a performance da arquitetura** implementada para comprovação dessa hipótese, e um outro que demonstra medições da **performance da NovaGenesis** na entrega de dados publicados pelo EPGS, via PGCS, para a aplicação "IoTTestApp".
A Figura 4.1 ilustra, de forma macro, todo o processo utilizado. Desde a importação dos dados brutos, até o processamento que torna as informações contextualizadas, que subsidiarão as análises apresentadas nesta seção.

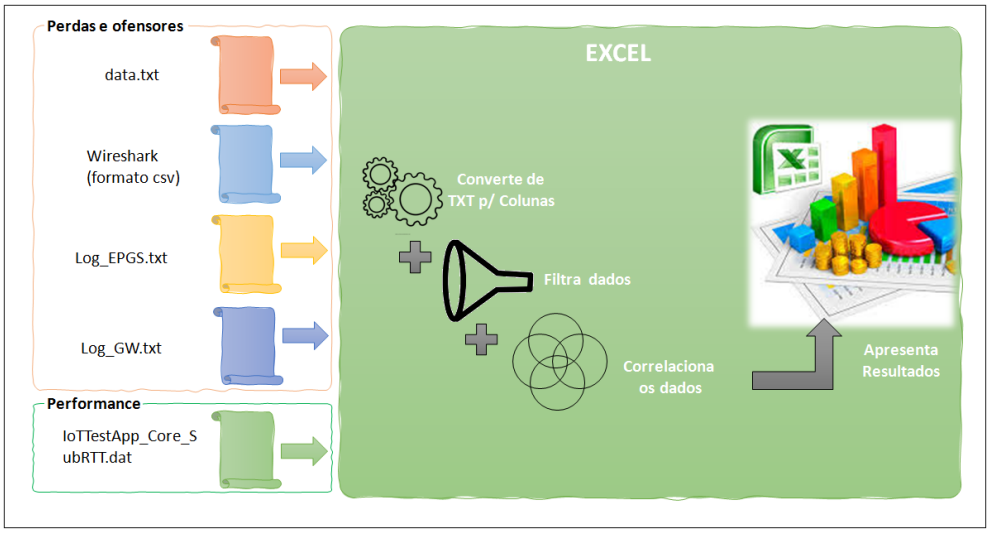



Figura 4.1: *Metodologia de análise dos dados/logs coletados.*

## 4.3 Apresentação dos resultados

Os testes foram realizados em ambiente controlado e isolado de outros elementos, sem tráfego externo que pudesse inserir atrasos ou interferir nas medições; havendo apenas tráfegos da rede local e da NovaGenesis. O único elemento que não está em nosso controle para este teste é a interferência externa no âmbito da rádio frequência. Como premissa inicial, foi considerado que toda e qualquer variação entre medições e possíveis perdas, estejam associadas à influência do segmento da comunicação LoRa, processamentos interno do GW ou da NG. Isso, devido o Wi-Fi ter sido prova de conceito em [7], não sendo ofensor para implementação da FIA NG em cenários de IoT.
Quatro grandezas foram analisadas: (a) Perda de mensagens NG em toda arquitetura proposta para teste; (b) Perda de fragmentos de pacotes; (c) Mensagens entregues fora de ordem; (d) Performance na entrega dos dados publicados para a aplicação NG.

Vários experimentos foram realizados seguindo o procedimento indicado no Capítulo 3. Os testes somente foram interrompidos quando, pelo menos uma das premissas definidas na subseção 3.2.3 deixou de ser atendida.
Um ponto observado durante os testes, foi que por algum motivo a memória dinâmica do EPGS excede o seu limite máximo, forçando sua reinicialização. Este comportamento foi identificado em vários experimentos e a comprovação está baseada nos registros/*logs* gerados na porta serial do EPGS. Não foi feito nenhuma intervenção no código do EPGS para identificar e corrigir esta falha. Fato que requer avaliação futura.
Na Tabela 4.2 ilustra os testes válidos e os resultados obtidos, com base na análise dos registros/*logs* (Amostras).

| Teste ID | Tempo (h) | Amostra | | | | Avaliação de perdas nos trechos | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Qtde | OK | Perda | | EPGS | | Gateway | | Wireshark | | data.txt | |
| | | | | Qtde | % | Qtde | % | Qtde | % | Qtde | % | Qtde | % |
| 220312 | 3,00 | 5402 | 5171 | 231 | 4,28% | 0 | 0,00% | 78 | 33,77% | 152 | 65,80% | 1 | 0,43% |
| 220224 | 5,56 | 9999 | 9922 | 77 | 0,77% | 0 | 0,00% | 25 | 32,47% | 51 | 66,23% | 1 | 1,30% |
| 220523 | 2,11 | 3806 | 3707 | 99 | 2,60% | 0 | 0,00% | 42 | 42,42% | 56 | 56,57% | 1 | 1,01% |
| 220529 | 1,72 | 3103 | 3086 | 17 | 0,55% | 0 | 0,00% | 1 | 5,88% | 15 | 88,24% | 1 | 5,88% |
| Total * | | 12311 | 11964 | 347 | 2,82% | 0 | 0,00% | 121 | 34,87% | 223 | 64,27% | 3 | 0,86% |
| Média * | | 6870 | 6761 | 110 | 1,60% | 0 | 0,00% | 37 | 34,09% | 71 | 65,00% | 1 | 0,91% |

* Considera apenas testes válidos. O teste em destaque vermelho não coletou todos os registros (desconsiderado na análise.

Figura 4.2: *Resultado consolidado das análises dos testes válidos realizados.*

Para um maior entendimento da análise e demonstração dos resultados, será utilizado o "Teste ID 220312". Estes resultados contribuirão para a conclusão dessa Dissertação de Mestrado.
A escolha desse teste foi motivada por ele possuir o maior número de registros/*logs* coletados, válidos e completos, em todos os pontos monitorados, além de ter apresentado o maior índice de perda (Erro).

O "Teste 220224", apesar de conter o maior número de amostras não foi escolhido, pois a aplicação de coleta dos dados da porta serial onde estava conectado o *Gateway* travou, ou seja, parou de guardar os registros/*logs* durante os teste, não salvando todos

os dados comprobatórios. Os dados indicados na Tabela 4.2 em vermelho foram analisados com base dos registros do Wireshark™, seguindo o comportamento observado nos demais testes válidos. Toda mensagem de publicação de dados que perde o terceiro fragmento, está associado à perda no trecho LoRa (EPGS e GW).

Importante atentar que, para se obter os registros de publicação de dados enviado pelo EPGS para a NG, contendo as medições de temperatura, todos os estágios anteriores incluindo a inicialização do LoRa e as demais etapas do ciclo de vida da Nova-Genesis foram concluídas com sucesso. O que comprova a capacidade da NG em se adequar ao meio LoRa para garantir sua comunicação entre entidades.

### 4.3.1 Medidas de Perda de Mensagens e Fragmentos

Por meio da avaliação do campo de numeração de sequência (*count*) contido no arquivo "data.txt", que é registrado pela aplicação "IoTTestApp", foi possível identificar as mensagens NG perdidas no percurso entre o EPGS e a aplicação, durante o processo de publicação de dados.
Neste experimento, cerca de 231 fragmentos de pacotes foram perdidos de um total de 5402 pacotes enviados. Isso impacta em **4,28%** do geral de perdas de pacotes. Cada mensagem de publicação de dados NG possui três fragmentos, conforme Figura 2.5.

Analisando os registros/*logs* da rede Ethernet coletados no Wireshark™, pode-se verificar que, cada mensagens NG perdida está associada a perda de um (1) único fragmento da mensagem. Isso significa que a rede LoRa entregou uma disponibilidade de **98,56%** dos fragmentos enviados pelo EPGS para o GW, representando uma perda de **1,44%**, conforme ilustrado na Figura 4.3 e calculado pela formula abaixo.

$$Disponibilidade = \left( \frac{QtdePerda}{(QtdeAmostras)(3Fragmentos)} \right) 100$$

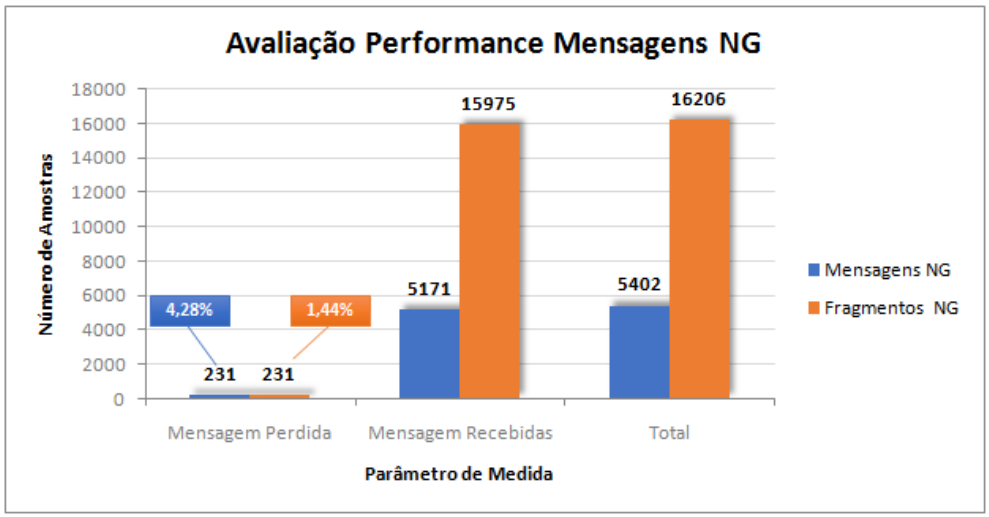



Figura 4.3: *Perda de mensagens NG, fragmentos e mensagens fora de ordem.*

Confrontando o "campo de numeração de sequência" das planilhas geradas dos arquivos brutos, foi possível elaborar uma tabela no Excel, contendo a correlação das

leituras dos diferentes arquivos. Baseado na análise das informações apresentadas por essa tabela, foram identificados os trechos e a relevância de cada um dos ofensores de perda, possibilitando chegar a um nível de análise para identificação do fragmento perdido de uma mensagem de publicação de dados.
Embora inicialmente o Wi-Fi ter sido considerado como elemento neutro neste experimento, não gerando perdas de pacote, foi verificado que esse segmento se demonstrou o maior ofensor, representando **65,80%** do total de mensagens NG perdidas. Este elevado índice de perda levou à uma analise mais profunda dos possíveis motivadores deste resultado. Os Gráficos ilustrados na Figura 4.4 apresentam os resultados obtidos da análise dos registros/*logs* coletados, confirmando que apesar de toda complexidade para implementação da FIA NG em uma rede LoRa, as entidades EPGS e o Núcleo da NG não impactaram aos índices de perdas nesta arquitetura, sendo estes responsáveis por **0,00%** e **0,43%** respectivamente. Já o segmento LoRa, entre o EPGS e o GW apresentou **33,77%** do total de perdas, ou seja das 231 perdas identificadas, 78 estão relacionadas ao LoRa.

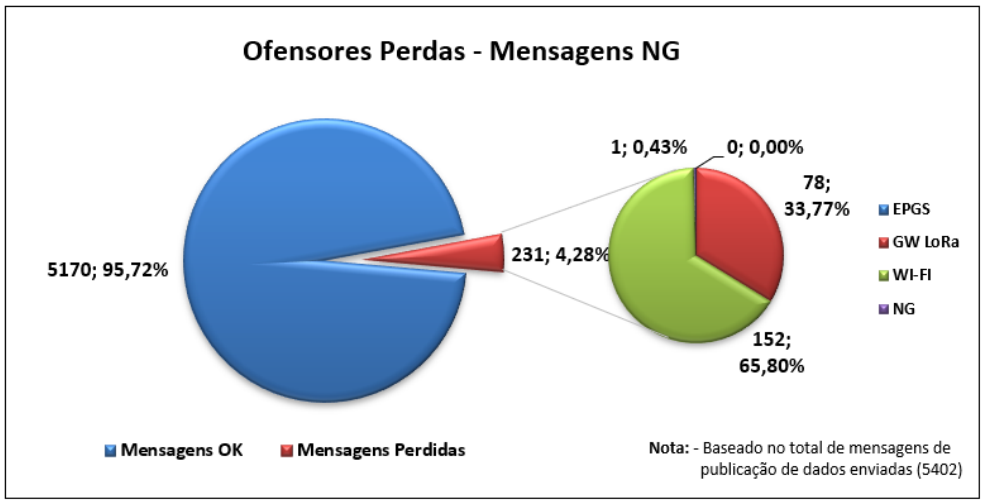



Figura 4.4: *Ofensores de Perda de mensagens NG em uma Arquitetura NG sobre uma rede LoRa*

#### 4.3.1.1 Entendimento dos ofensores de Perda

Conforme observado na Tabela 4.2, o mesmo comportamento de perda visto no "Teste 220312" se repete nos demais testes realizados, servindo como motivador para investigação e entendimento do ocorrido. Devido o Wi-Fi ter sido o maior ofensor de perda, contradizendo a premissa inicial adotada, pesquisas para identificar causas que pudessem influenciar na ocorrência deste prejuízo significativo foram requeridas.

Os testes foram realizados em uma região próxima à Av. Paulista - São Paulo - SP (Lat/Long 23º34'52"S 46º39'09"W). A comunicação no segmento Wi-Fi foi estabelecida utilizando o padrão 802.11/n em uma frequência de 2.4GHz no canal 11.
É sabido que esta faixa de espectro, por não ser licenciada pelos órgãos reguladores, está sujeita a interferência devido a grande quantidade de dispositivos que operam nesta faixa, como por exemplo, telefones sem fio, *Bluetooth*, Microondas, etc.

Na busca dos motivos que levaram ao grande volume de perdas no Wi-Fi, foi avaliado o uso do espectro ao arredor do local onde os testes foram realizados. Segundo [59], esta região é considerada como local com o maior índice de interferência de RF no país.

Testes complementares, com objetivo de comprovar se realmente esta suposição poderia ser a causa, foram realizados.
Utilizando um *Access Point* (AP) Aruba, modelo IAP-205RW [60] na versão de *firmware* 6.5.4.22 configurado no modo *Spectrum Monitor*, modo este onde o AP funciona como um analisador de espectro para as frequências onde trabalha, foi possível avaliar o nível de interferência no Wi-Fi para as frequências 2.4 GHz e 5.8 GHz.
A Figura 4.5 ilustra o cenário de investigação do espectro ao arredor do local onde o teste foi realizado e os principais números encontrados que serão detalhados a seguir.

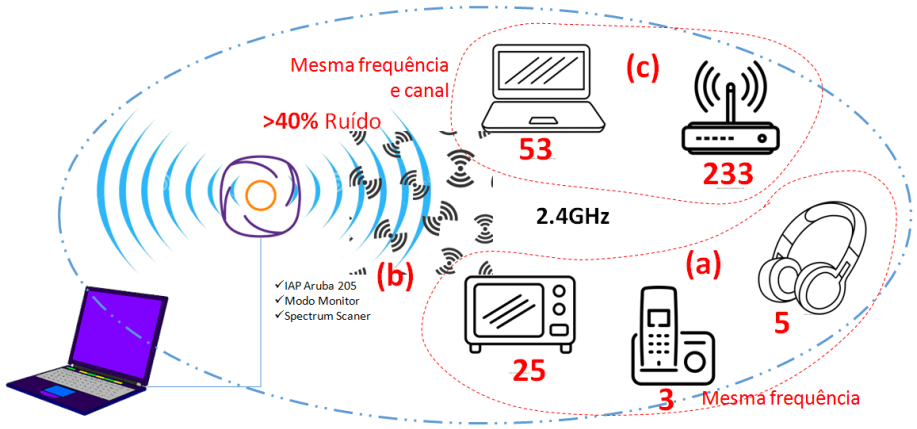



Figura 4.5: *Cenário de investigação de RF e resultados obtidos.*

O resultado desta varredura de espectro, trouxe informações relevantes para esta avaliação. A Figura 4.6 ilustra recortes da página WEB de gerenciamento do AP, onde cada imagem é sinalizada por uma letra detalhada a seguir:

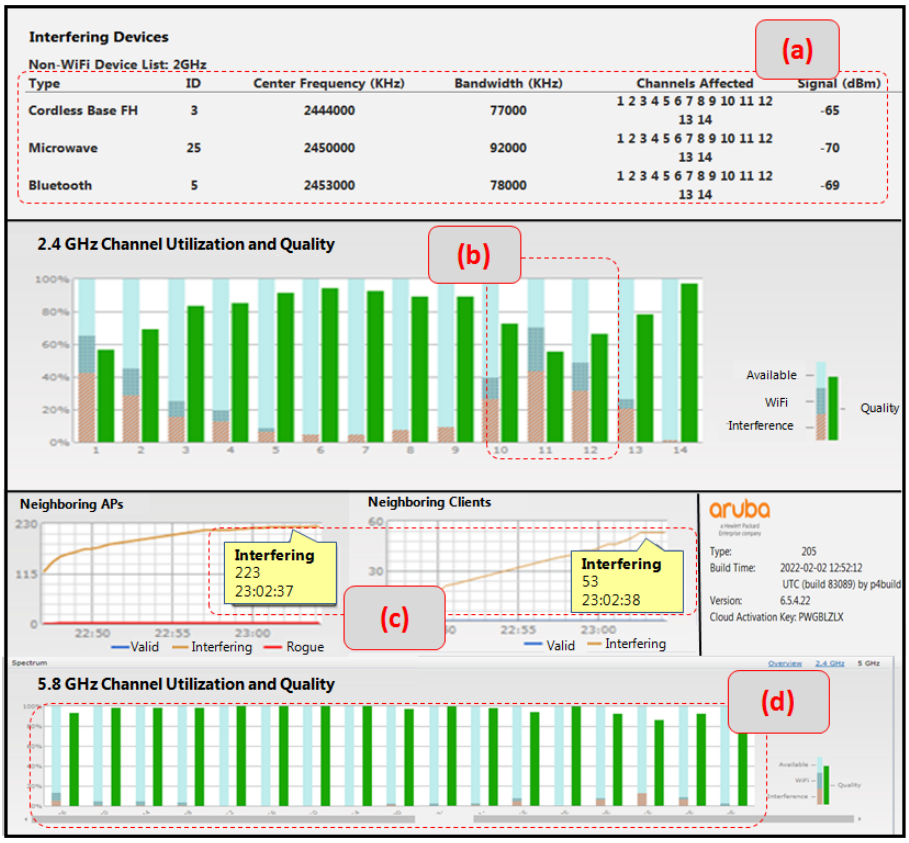



Figura 4.6: *Nível de interferência RF no local de teste.*

*a*) Nesta tela são apresentados todos os dispositivos irradiantes identificados no raio de cobertura do AP, que operam na frequência de 2.4 GHz, e que possam estar gerando interferência.

*b*) Este gráfico ilustra a qualidade dos canais e seu nível de ruido para a frequência de 2.4 GHz. É possível observar que, **mais de 40%** do canal 11 sofre com problemas de ruído e interferências, podendo ocasionar perdas de pacotes.

*c*) O *Access Point* tem capacidade para quantificar os dispositivos identificados dentro do raio de cobertura divididos em dois grupos: um enumerando **os APs** que estão gerando interferência na vizinhança e outro que indica a quantidade de **clientes** que também geram interferência na rede, representados pelas quantidades de **223 APs** e **53 Clientes**, respectivamente. .

*d*) E por último, analisando o gráfico gerado pelo AP na frequência de **5.8 GHz** é possível identificar um **nível bem inferior** de interferência.

Com base na análise dessas medidas, pode-se afirmar que a expressiva quantidade de dispositivos irradiantes na frequência de 2.4 GHz impactaram diretamente na perda de pacotes durante o experimento.

Teste em um ambiente com menor índice de interferência objetivando justificar o pressuposto nessa subseção, foi realizado e demonstrou uma redução significativa das perdas de pacotes/mensagens no Wi-Fi. Contudo, este resultado não foi conclusivo por exigir um número maior de experimentos para sua validação, por esse motivo, não será abordado nesta Dissertação de Mestrado.

Assim como para o Wi-Fi, análise detalhada das perdas no segmento LoRa são requeridas visto que, este representou o segundo maior índice de perdas nesses experimentos. Devido a indisponibilidade de equipamento que possibilitasse a inspeção do espectro na frequência de 915 MHz e que pudesse justificar os prejuízos nesse segmento, não foi possível apresentar nessa Dissertação de Mestrado o mesmo nível de detalhamento obtido no Wi-Fi. Ficando como sugestão para trabalhos futuros.

#### 4.3.1.2 Proposta para minimizar as perdas

Essa subseção tem como objetivo levar sugestões para projetos futuros minimizando as perdas nos trecho LoRa e Wi-Fi. Para reduzir os impactos com perdas de pacotes ou mensagens NG nestas faixas de frequência, uma opção seria se utilizar de técnicas de múltiplas transmissões dos pacotes como implementado em alguns cenários no CAT-M e NB-IoT [22].
No protocolo do código atual do EPGS não é previsto a retransmissão de pacotes/mensagens NG perdidos, devido a necessidade de preservar a vida útil das baterias. A implementação de múltiplas transmissões, aumentaria a chance de um pacote chegar ao seu destino, porém reduzindo a eficiência energética do *NÓ* IoT. Para medir o aumento da probabilidade de sucesso de um pacote com base a sugestão acima, requer a implementação desta função na NG e no EPGS, a qual não é suportada no código atual.

Uma outra opção é tratar os pacotes perdidos na camada de aplicação, calculando-se um valor médio, uma vez que as medidas de temperatura são valores estáveis e não oscilam repentinamente.
Um ponto que reforça a esta sugestão de cálculo médio é, a quantidade de perdas de mensagens NG consecutivas (duas medidas simultâneas) foi relativamente baixa conforme apresentado na Tabela 4.7. A única exceção é o "Teste 220224", que teve das 77 mensagens NG perdidas sendo 26 relativas a 13 eventos consecutivos. Deste 13 eventos foi observado que, 8 deles ocorreram em sequência contínua, algo não percebido nos demais testes. A Tabela 4.7 ilustra a identificação dos pacotes perdidos em cada teste analisado.

| Teste ID | Perda | | Perdas de fragmento | | | | | | Eventos consecutivos de perda | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Perda | % | Fragmento 1 | | Fragmento 2 | | Fragmento 3 | | | |
| | | | Perda | % | Perda | % | Perda | % | Qtde | % |
| 220312 | 231 | 4,28% | 71 | 30,74% | 82 | 35,50% | 78 | 33,77% | 10 | 4,33% |
| 220224 * | 77 | 0,77% | 1 | 1,30% | 51 | 66,23% | 25 | 32,47% | 13 | 16,88% |
| 220523 | 99 | 2,60% | 24 | 24,24% | 33 | 33,33% | 42 | 42,42% | 1 | 1,01% |
| 220529 | 17 | 0,55% | 5 | 29,41% | 11 | 64,71% | 1 | 5,88% | 0 | 0,00% |
| Total | 424 | 2,82% | 101 | 23,82% | 177 | 41,75% | 146 | 34,43% | 24 | 5,66% |

* Foi observado que dos 13 eventos 8 ocorreram sequenciais. Diferente dos demais, sempre espassados.

Figura 4.7: *Detalhamento dos Fragmentos perdidos.*

Vale relembrar que os testes foram realizados com uma cadência de envio de publicação de dados (medições de temperatura) a cada 2 segundos.
Para casos onde a frequência de transmissão são espaçadas, por exemplo, medição de temperatura em uma estufa de plantação de morangos, que pode ser enviada a cada hora ou intervalo maiores, a implementação de múltiplas publicações em sequência

pode ajudar a reduzir ou até mesmo eliminar a possibilidade de não se ter o dado no tempo desejado. A definição do número de múltiplas transmissões podem variar de acordo com o cenário.
A identificação de pacotes duplicados ou utilização do que contém a mensagem completa pode ser motivo de implementação na própria NG, similar aos tipos de classes de rede suportado na LoRaWAN [R].

### 4.3.2 Mensagens NG Fora de Ordem

Analisando as planilhas individuais do arquivo único geradas após processamentos dos registros/*logs* do EPGS, GW, Wireshark™ e "data.txt", foi possível observar se ocorreram inversão de mensagens NG, fato este observado somente na planilha gerada do "data.txt".

Verificou-se que apenas 31 das 5402 mensagens de publicação de dados tiveram pelo menos um fragmento de mensagem NG chegando no Núcleo da NovaGenesis fora de ordem, representando **0,57%** do total de amostras conforme ilustrado na Figura 4.8. Esta identificação somente foi possível pela análise detalhada dos *logs* do Wireshark™ visualizando os pacotes trocados na rede Ethernet.

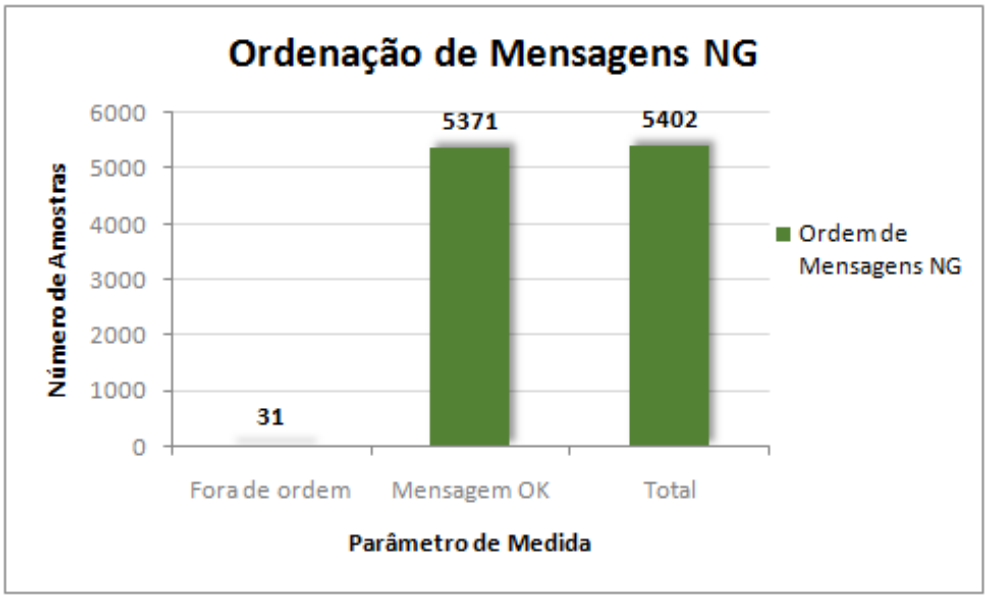



Figura 4.8: *Perda de mensagens NG, fragmentos e mensagens fora de ordem.*

Os atraso nos fragmentos de mensagem NG, fazem com que as publicações de dados ocorram fora de ordem. Na planilha processada do arquivo "data.txt" é possível identificar estas publicações, uma vez que, para cada registro é salvo o contador de número de sequência (*count*) enviado pelo EPGS.
Isso demonstra a capacidade da NG em tratar sequenciamento de fragmentos da NG recebidos desordenados.

Outro ponto observado foi a flexibilidade da NG e do EPGS em se adequar a outros meios de enlace, como por exemplo a rede LoRa que restringe o tamanho da *Protocol Data Unit* (PDU) a 222 bytes. Na experimentação anterior utilizando Wi-Fi, o tamanho da PDU pode acomodar toda a mensagem NG, conforme comprovado em [7].

Não foi possível identificar os fatores que levaram à inversão dos fragmentos. No entanto, estes não foram relevantes para acarretar impacto no serviço de publicação de dados, uma vez que após o recebimento dos fragmentos e a remontagem dos pacotes/mensagens pela NG o dado é entregue ao destinatário assinante do serviço, mesmo que atrasado. A investigação deste problema pode ser um motivo de estudo para futuros trabalhos.

### 4.3.3 Indicadores de performance de serviço

Os indicadores de performance do serviço entregues pela NG registrados no arquivo "IoTTestApp_core_SubRTT.dat", são calculados pela diferença dos tempos de entrega de uma nova publicação de dado, recebida pelo PSS e notificadas para aplicação consumidora "IoTTestApp", conforme apresentado em **3.2.5.2.2**.
Utilizando as informações disponíveis no arquivo "IoTTest_Core_SubRTT.dat", processado no Excel, foi verificado que a média aritmética do RTT tende para um valor de **38,02 milissegundos**, conforme ilustrado na Figura 4.9 indicado pela linha azul com asteriscos denominada "Tendência" no gráfico. Um tempo relativamente elevado comparado com a comprovação anterior utilizando Wi-Fi, e acima do esperado por ser processado internamente no mesmo computador, conforme descrito na subseção 3.2.2.2.
Durante todo período de teste os *software* da NovaGenesis, Wireshark™ e o Teraterm são executados concomitantemente. Foi observado que o processamento do notebook atinge 100% após a NG estar operacional e permanecendo assim em todo período de realização do teste, este é um fato relevante requerendo futura análise para justificativa do tempo elevado medido.

Para o entendimento de como foi a performance deste experimento, foram selecionadas 100 amostras, do total de 5042, equidistantes do conjunto total de medidas coletadas. Cada amostra representa uma linha da planilha processada do arquivo "IoTTestApp_Core_SubRTT.dat". Estas amostras foram consolidadas e o seu resultado é apresentado em um gráfico ilustrado na Figura 4.9. A definição de 100 amostras foi motivada com o objetivo de apresentar, de forma visual, os indicadores e as informações que podem ser obtidas a partir deste arquivo, sem perder sua essência ou informação. A representação com um número elevado de amostras, inviabiliza sua visualização no modelo do gráfico sugerido.

No gráfico os retângulos indicam a faixa em que uma medida instantânea do RTT variou em relação a média aritmética. Quando sua cor de preenchimento é verde indica que a medida instantânea foi maior que a média aritmética, e quando sua cor for preenchida com vermelho indica que a média aritmética está acima da instantânea. As linhas pretas com setas em suas extremidades representam os limites máximos e mínimos onde um valor de rtt pode ser encontrado. As suas medidas são representadas pelo eixo vertical a esquerda em segundos.
Já as linhas verde com triangulo, vermelho com bolas e azul com asteriscos apresentadas no gráfico, se referenciam as medidas máximas e mínimas e sua média aritmética (Tendência) respectivamente, e são apresentadas em segundos no eixo vertical a direita.
É possível observar uma convergência do tempo do intervalo de publicação a medida

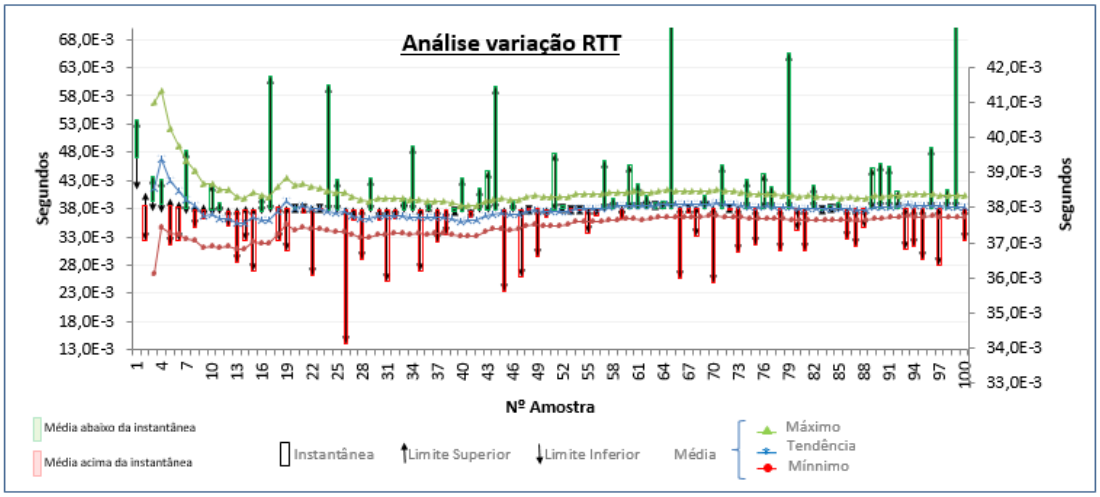



Figura 4.9: *RTT medido na Aplicação IoTTestApp da NG.*

que se tem um número maior de amostras, tendendo os limites máximos e mínimos ficarem cada vez mais próximos a média aritmética.

Quando analisado os picos extremos apresentados no gráfico, como por exemplo as amostras 16, 23, 26, 44, 65,.., elas indicam que estão precedidos de um evento de perda de mensagem. Por este motivo um indicador de tendência com valores médios, erro padrão e limites de confidência são imprescindíveis na avaliação do nível de serviço entregue.
Os indicadores gerados demonstram a capacidade da NovaGenesis e/ou aplicações em entregar informações relevantes aos serviços contratados, sendo esta função intrínseca à sua arquitetura.

## 4.4 Resumo

No início deste capítulo, foi abordado a metodologia utilizada para transformar os arquivos de registros/*logs* (contendo dados brutos), coletados em diferentes pontos da arquitetura implementada, em um arquivo com informações contextualizadas para subsidiar as análise dos resultados desta prova de conceito.
No decorrer do capítulo, foram analisados e apresentados os resultados de perdas e ordenação de pacotes/fragmentos.
Uma vez que os resultados de perdas apresentaram uma contradição à premissa adotada inicialmente sobre o Wi-Fi, investigações adicionais foram necessárias com objetivo de identificar os ofensores das perdas. De acordo com os resultados das pesquisas, existe grande chance das interferências geradas por dispositivos externos terem influenciado nos resultados dos testes, os quais não puderam ser replicados em local de menor interferência de RF para reforçar nossa desconfiança. Também foi abordado a impossibilidade de investigação no trecho LoRa.
Os números apresentados demonstram a viabilidade de uma Arquitetura FIA Nova-Genesis utilizando uma rede LoRa. Não se observou resultados relevantes que inviabilizassem esta implementação, principalmente do ponto de vista do EPGS e da NG que tiveram êxito em executar todas as etapas do ciclo de vida do serviço, desde sua inicialização até a publicação, respeitando os limites da rede LoRa.
Também foram apresentados os indicadores de performance de serviço que demonstram a capacidade da NG em notificar e publicar dados para uma aplicação que assinou o serviço. Em adicional a NG possibilita a medição de tempos RTT e suas variações que representam a performance de como estes dados são entregue, servindo assim com indicador de qualidade de nível de serviço.
A Figura 4.10 resume os resultados apresentados neste capítulo, os quais subsidiam e reforçam a conclusão deste trabalho.

| | Item | | Valor | % | | | |
|---|---|---|---|---|---|---|---|
| Teste ID 220312 | Duração (horas) | | 3,00 | | | | |
| | Nº Amostras | | 5402 | 100,00% | | | |
| | Amostras OK | | 5171 | 95,72% | | | |
| Perdas (Pacotes / Mensagens) | ***Total Perdas*** | | ***231*** | ***4,28%*** | ***Frag 1*** | ***Frag 2*** | ***Frag 3*** |
| | No EPGS | | 0 | 0,00% | 0 | 0 | 0 |
| | Trecho LoRa | | 78 | 33,77% | 0 | 0 | 78 |
| | Trecho WiFi | | 152 | 65,80% | 152 | | 0 |
| | Na NG | | 1 | 0,43% | 0 | 0 | 0 |
| Ordenação (Mensagens) | ***Fora de Ordem*** | | ***31*** | ***0,57%*** | | | |
| Performance (Milisegundos) | ***Média*** | | ***38,02E-3*** | | | | |
| | Limites | Máximo | 38,33E-3 | | | | |
| | | Mínimo | 37,72E-3 | | | | |

Figura 4.10: *Resumo dos resultados de análise de experimento.*

No próximo capítulo, serão apresentados as impressões deste trabalho, conclusões e sugestões para projetos futuros.

# Capítulo 5

# Conclusões e Propostas Para Novas Pesquisas

NESSE capítulo será apresentado a conclusão final desta Dissertação de Mestrado e quais pontos ainda ficaram em aberto que podem ser objeto de novos estudos.

## 5.1 Considerações finais

Essa seção será apresentada em três subdivisões. Uma fará a revisão dos objetivos deste trabalho, a outra apresentará as conclusões obtidas e a última, dará sugestões para o seguimento de futuros trabalhos relacionados à pesquisa em questão.

### 5.1.1 Revisão dos objetivos

Este trabalho propôs a expansão da arquitetura NovaGenesis em cenários de *Internet of Things* (IoT), utilizando meio de comunicação de longo alcance *Longe Range* (LoRa).
No decorrer desta Dissertação de Mestrado foram:

- Apresentados os desafios para a Internet do Futuro e como Órgãos Internacionais têm contribuído para trilhar esta jornada.
- Importantes projetos voltados a este "Repensar da Internet" foram apresentados, dando maior ênfase para a NovaGenesis.
- Em seguida foram apresentados os principais problemas enfrentados com a arquitetura da Internet atual e como a NovaGenesis contribui e resolve estas questões em direção a uma *Future Internet Architecture* (FIA).
- Foi apresentado um comparativo entre tecnologias de rede *Low Power Wide Area Network* (LPWAN) com maior foco para a LoRa.
- Conhecidas as dimensões do desafio para integração da FIA NovaGenesis e a LoRa, foi definida metodologia e premissa de teste visando obter o maior número de amostras que suportassem a validação desta hipótese.

- Utilizando-se do cenário proposto para validar esta hipótese, sequências de testes foram realizados utilizando o protótipo.
- De posse das amostras coletadas e processadas, sem perder sua rastreabilidade, foram gerados planilhas, relatórios e gráficos que pudessem comprovar e fundamentar a hipótese desta Dissertação de Mestrado.
- Ao longo da pesquisa, premissas tiveram que ser revistas, uma vez que se demonstraram opostas ao definido inicialmente (citando como exemplo o Wi-Fi).

A jornada trilhada até aqui proporcionou subsídios importantes para concluir esta Dissertação de Mestrado, assim como sugerir futuros trabalhos que certamente ampliarão ainda mais a abrangência da NovaGenesis.

### 5.1.2 Conclusões obtidas

Com base nos resultados obtidos durante os experimentos em laboratório e análise dos registros/*logs* resumidos e ilustrados na Figura 4.10, podemos afirmar:

1. Foi possível comprovar que as **funcionalidades NovaGenesis** em um **cenário de IoT utilizando redes LPWAN** foram suportadas. Dentre elas destacam-se nomes auto-verificáveis, ligações de nomes, auto-descoberta, estabelecimento de contratos, cache de rede e ciclo de vida do serviço, pré requisitos para publicação de dados pelo *Embedded Proxy Gateway Service* (EPGS);
2. A NovaGenesis e o EPGS **não foram ofensores** de entrega do serviço conforme demonstrado nas tabelas e gráficos no Capítulo 4 e resumido na Figura 4.10;
3. A NovaGenesis se **demonstra flexível** o suficiente para se adequar ao novo meio e as suas características, podendo evoluir para suportar novos serviços e assumir funcionalidades implementadas na camada de aplicação do *Longe Range WAN* (LoRaWAN $^{R}$) (tipos de classes);
4. **A NovaGenesis** não enfrentou dificuldades em operar com **mensagens de *Protocol Data Unit* (PDU) limitadas no LoRa**, comprovando a capacidade da NG e do EPGS em se adaptar a distintos meios físicos, tratando fragmentação, remontagem e ordenação de pacotes;
5. A aplicação "IoTTestApp" que segue as mesmas características da NG **foi capaz de medir o nível de serviço entregue pela NovaGenesis** com ricos indicadores de performance, podendo subsidiar novos modelos de negócios, como a remuneração variável, de acordo com o nível de serviço entregue;
6. A plataforma aberta do **ESP-32 LoRa** da Heltec, se demonstrou uma boa ferramenta para desenvolvimentos em cenários de IoT, mesmo em arquiteturas FIA. Ela se mostrou flexível, possibilitando a **implementação de um *Gateway*** tratando mensagens NG;

De posse das afirmações acima, pode-se concluir: é totalmente viável implementar uma arquitetura FIA NovaGenesis em uma rede LoRa, expandindo assim sua abrangência para cenários de IoT com longas áreas de cobertura, atendendo as demandas como agronegócio, logísticas, rastreamentos, redes de monitoramento inteligentes, entre outros cenários.

Para cenários onde o tempo de vida da bateria é relevante, como é o exemplo do agronegócio, industrias, aplicações em cidades inteligentes, etc sugere-se a avaliação de múltiplas transmissões durante o envio de uma publicação, aumentando assim a chance da entrega dos dados publicados.

Também suportados pelas análises e investigações realizadas para identificar o ofensor da rede Wi-Fi, levanta-se a questão de se ter dispositivos que trabalhem em faixas de frequência com menor interferência, por exemplo utilizando 5.8 GHz, principalmente para os casos de uso em aplicações críticas.

### 5.1.3 Sugestões para futuros trabalhos

Apesar dos esforços empreendidos ao longo das pesquisas realizadas, alguns pontos não foram possíveis de serem abordados durante a evolução desta Dissertação de Mestrado. Serão apresentados abaixo os pontos em aberto que abrem oportunidades de novos trabalhos de pesquisa, expandindo ainda mais os cenários de IoT considerando a FIA NG utilizando uma rede LoRa.

1. **Múltiplas transmissões** - Implementar no EPGS e na NG a possibilidade de envio e tratativa de múltiplas transmissões, reduzindo assim a probabilidade de perda de uma mensagem NG;
2. **Controle de Acesso** - Implementar no *Gateway* métodos para suportar vários *NÓS* simultâneos, considerando controle de acesso e gestão das janelas de transmissão;
3. **Tipos de Classes de aplicações para IoT** - Desenvolver diretamente na NovaGenesis tipos de classes de rede similares ao implementado na LoRaWAN $^{R}$, como um novo serviço NG, dando autonomia para a NG controlar a totalidade dos fluxos otimizando o uso dos recursos energéticos;
4. **Múltiplos *NÓS* / Múltiplos *Gateway*** - Implementar e validar cenários de escalabilidade gerenciados pela NovaGenesis, verificando a performance do meio e avaliando os impactos em seu núcleo;
5. **Mobilidade do EPGS** - Validar cenários de **mobilidade de *NÓS* IoT EPGS** em uma arquitetura FIA NG com múltiplos *Gateway* em uma rede LoRa;
6. **Otimização das mensagens NG** - Avaliar possibilidade de otimizar as mensagens NG para caber em um único pacote, aumentando assim a eficiência da arquitetura proposta em transmissão LoRa ou outra tecnologia LPWAN que possui *payload* reduzido.

A Figura 5.1 ilustra essas sugestões para futuras pesquisas.

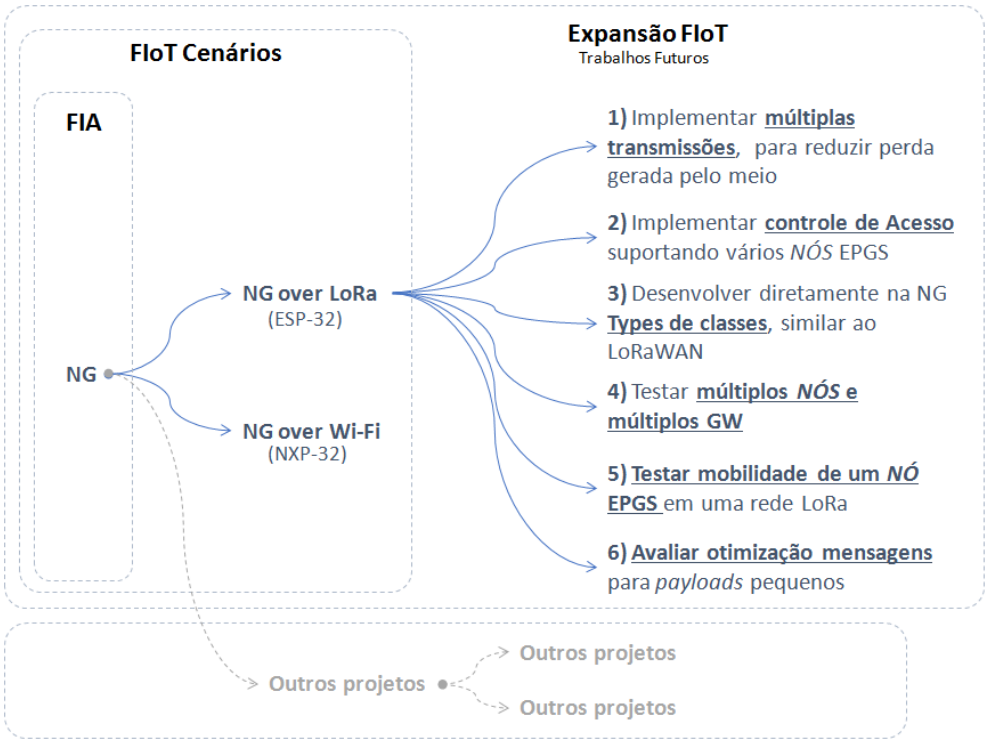



Figura 5.1: *Proposta para projetos futuros de NG utilizando LoRa.*

### 5.1.4 Repensando as conclusões do trabalho de pesquisa

Ao final deste trabalho de pesquisa, algumas considerações precisam ser feita: a) que o conhecimento obtido através dos estudos, testes, análises, etc, contribuíram para o desenvolvimento de um senso crítico mais apurado; b) que no afã de realizar as tarefas, passou desapercebido uma gama de conhecimento que teria permitido a inserção de novos elementos que ampliariam ainda mais a abrangência dos resultados alcançados para comprovação das hipóteses; que se fosse possível recomeçá-lo, provavelmente sua conclusão traria uma contribuição mais enriquecedora para a comunidade científica, apresentando melhores resultados com maior aplicabilidade e abrangência do até então realizado. Assim o excedente de resultados que não foi possível ser utilizado no decorrer desse estudo, fica como legado para futuros trabalhos de pesquisas, reforçando a viabilidade da implementação FIA NG em uma rede LoRa, desmistificando suspeitas que ainda nos restam.

Contudo, estes conhecimentos somente foram se consolidando a proporção que foi possível entender e analisar de forma crítica os resultados obtidos na finalização do trabalho de pesquisa.

Desta reflexão, surgem novos temas de pesquisas com objetivo de reforçar ainda mais as conclusões obtidas neste trabalho até o momento, que são listados abaixo:

- **Interferência de RF** - Repetir os testes em local com um nível menor de interferência externa para validar a desconfiança de que esse nível foi o maior ofensor de perdas no Wi-Fi, assim como avaliar se existe algum outro ofensor associado;
- **Variação de distância** - Repetir os testes utilizando outras *Spread Factor* (SF) e avaliar o comportamento da NG em cenários com maior espalhamento espectral;

- **Avaliação de perdas na LoRa** - Executar teste similares ao realizado para o Wi-Fi buscando identificar possíveis ofensores que levaram a perda de fragmentos de pacotes na transmissão LoRa;
- **Inversão de pacotes** - Avaliar os motivos que ocasionaram o atraso de fragmento de pacotes que levaram a inversão de mensagens NG;
- **Alocação de memórias do EPGS** - Avaliar, identificar e corrigir no código do EPGS a alocação de memória dinâmica sem liberação após o uso;
- **Elevado processamento** - Refazer os testes em uma máquina com maior capacidade de processamento e memória para avaliar se o tempo médio de *Round Trip Time* (RTT) é influenciado.

## 5.2 Reflexão

A evolução é um processo contínuo e infinito, pois a cada passo dado, um nova oportunidade se abre para ser explorada. Este trabalho contribui na evolução do Estado da Arte no repensar da Internet, tal qual foram explorados nos capítulos 1 e 2. Cabe a nós, pesquisadores, cientistas, mercado, indústria e sociedade ajustar a direção e priorizar a evolução. No "Repensar da Internet" muito já foi feito até aqui pela comunidade acadêmica, contudo, existe um caminho ainda desconhecido a ser explorado. Desejo humildemente com esta Dissertação de Mestrado ter contribuído com mais um passo em direção a este futuro ainda desconhecido, porém já idealizado por pesquisadores em projetos inovadores como [7, 10, 12, 61].

Finalizo aqui esta Dissertação com uma frase de **"Duílio Alves de Moraes"**.

"A evolução é um processo contínuo e só se obtém por meio do constante auto questionamento. Aquele que se crê conhecedor da verdade constrói um muro diante de si mesmo. Assim também é com qualquer grupo ou sociedade que se veste da soberba."

# Capítulo 6

# Contribuições para a Comunidade Científica

ESSA Dissertação de Mestrado segue em linha ao artigo publicado no "XIII Workshop de Pesquisa Experimental da Internet do Futuro (WPEIF 2022)", intitulado por "NovaGenesis Over LoRa in an IoT Scenario" [62], ampliando sua abrangência introduzindo novos indicadores.
No artigo [62] as dimensões de perdas de pacote e fragmento foram abordadas. Já, nessa Dissertação de Mestrado, os indicadores de ordenação dos pacotes e performance de nível de serviço entregues pela NovaGenesis à aplicação NG foram inseridos ampliando sua abrangência.
Também são detalhados as metodologias utilizadas para planejar/executar os teste, bem como transformar dados brutos em informações contextualizadas que serviram de base para análise que contribuíram para a defesa da hipótese deste trabalho.

## 6.1 Publicações e Premiações

O Prêmio de melhor artigo no XIII Workshop de Pesquisa Experimental sobre Internet do Futuro (WPEIF 2022). Autores: Epper Bonomo, Rodrigo Hilário do Santos, Antônio Marcos Alberti.


FORTALEZA - CE

ANOS SBRC

XL SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS

Certificado

Certificamos que o artigo intitulado "**NovaGenesis Over LoRa in an IoT Scenario**" dos autores **Epper Bonomo, Antonio Marcos Alberti e Rodrigo Santos** recebeu o prêmio de Melhor Artigo no XIII Workshop de Pesquisa Experimental da Internet do Futuro (WPEIF) do XL Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, que ocorreu no período de 23 a 27 de maio de 2022.

Fortaleza, 27 de Maio de 2022.

**Rafael Lopes Gomes**
Coordenador Geral do SBRC 2022

**Rossana Maria de Castro Andrade**
Coordenadora Geral do SBRC 2022

ORGANIZAÇÃO: REALIZAÇÃO: SECRETARIA EXECUTIVA:

Figura 6.1: *Certificado de melhor artigo do XIII Workshop de Pesquisa Experimental sobre Internet do Futuro (WPEIF 2022).*

# Referências Bibliográficas


[1] D. Evans, "The future of iot miniguide: The burgeoning iot market continues," *Cisco Newsletter*, July 2019. [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/future-of-iot.html?dtid=osscdc000283

[2] STADISTA, "Internet of things (iot) connected devices installed base worldwide from 2015 to 2025," *Statista Research Department*, p. 5, November 2016. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] V. P. Kafle, Y. Fukushima, and H. Harai, "Internet of things standardization in itu and prospective networking technologies," *IEEE Comm. Magazine*, vol. 54, no. 9, pp. 43–49, September 2016. [Online]. Available: https://www.researchgate.net/publication/308276472_Internet_of_things_standardization_in_ITU_and_prospective_networking_technologies

[4] S. L. . L. D. X. . S. Zhao, "The internet of things: a survey," *Springer*, no. 17, p. 243–259, April 2015.

[5] H. Saadeh, W. Almobaideen, and K. E. Sabri, "Internet of Things: A review to support IoT architecture's design," *IEEE Magazine*, December 2017.

[6] G. Mulligan, "The 6LoWPAN architecture," *ACM Journals*, June 2007. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1278972.1278992

[7] A. M. Alberti, G. D. Scarpioni, V. J. Magalhaes, A. C. S. Jr., J. J. P. C. Rodrigues, and R. da R. Righi, "Advancing novagenesis architecture towards future internet of things," *IEEE Internet of Things Journal*, vol. 6, pp. 215 – 229, Jully 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7970111/keywords#keywords

[8] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, kc claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM Journals*, pp. 66 – 73, 2014. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2656877.2656887

[9] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," *ACM Journals*, pp. 1 – 12, 2009. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1658939.1658941

[10] P. J. H. d. S, "Title model ontology for future internet networks. in: Future internet assembly 2011: Achievements and technological promises," *The Future Internet*, 2011. [Online]. Available: https://library.oapen.org/bitstream/handle/20.500.12657/27702/1002304.pdf?sequence=1#page=117

[11] D. Naylor, M. K. Mukerjee, P. Agyapong, R. Grandl, R. Kang, and M. Machado, "Xia:architecting a more trustworthy and evolvable internet," *ACM Journals*, pp. 50 – 57, 2000. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2656877.2656885

[12] A. Anand, F. Dogar, D. Han, B. Li, H. Lim, M. Machado, W. Wu, A. Akella, D. G. Andersen, J. W. Byers, S. Seshan, and P. Steenkiste†, "Xia: an architecture for an evolvable and trustworthy internet," *ACM Journals*, pp. 1 – 6, 2000. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2070562.2070564

[13] A. Alberti, M. Aurelio Favoreto Casaroli, R. Righi, and D. Singh, *Introducing NovaGenesis as a Novel Distributed System-Based Convergent Information Architecture*. Future Generation Computer Systems, 03 2018.

[14] G. Pottie, "Wireless sensor network," *IEEE Comm. Magazine*, vol. 54, no. 131, pp. 139–140, June 1998. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/706478/metrics#metrics

[15] E. Khorov, A. Kiryanov, A. Lyakhov, and G. B. M. Russia, "A tutorial on ieee 802.11ax high efficiency wlans," *IEEE*, pp. 197 –216, 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8468986

[16] P. Bhagwat, "Bluetooth technology for short-range wireless app," *IEEE Internet Computing*, 2001. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/935183/authors#authors

[17] S. Safaric, K. Malaric, and Z. Croatia, "Zigbee wireless standard," *IEEE Xplore*, 2006. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4127535

[18] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of lorawan," *IEEE Communications Magazine*, September 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8030482

[19] L. le Moan CEO, A. L. Chairman, and C. F. S. Director, "Sigfox," *Wikipedia*, 2010. [Online]. Available: https://en.wikipedia.org/wiki/Sigfox

[20] W.-F. Alliance, "Wi-fi halow technology overview," *IEEE*, 2020. [Online]. Available: https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_HaLow_Technology_Overview_20200518_0.pdf/36879

[21] M. C. S. M. IEEE, Y. Miao, Y. H. S. M. IEEE, K. Hwang, and L. F. IEEE, "Narrow band internet of things," *IEEE Access*, pp. 20 557 – 20 577, 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8038776

[22] B. S. Propietary, "Lte-m deployment guide to basic feature set requirements," *GSMA*, 2019. [Online]. Available: https://www.gsma.com/iot/resources/ltem-deployment-guide-v3/

[23] M. D. D. Moreira, N. C. Fernandes, and L. H. M. K. C. e Otto Carlos M. B. Duarte, "Internet do futuro: Um novo horizonte," *27º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, 2009. [Online]. Available: http://ce-resd.facom.ufms.br/sbrc/2009/080.pdf

[24] S. E. Deering and R. M. Hinden, "Internet protocol, version 6 (ipv6) specifica-

tion," *Internet Engineering Task Force (IETF)*, 1998. [Online]. Available: https://dl.acm.org/doi/pdf/10.17487/RFC2460,http=//www.rfc-editor.org/info/rfc8200

[25] M. S. B. D. D. CLARK, "Rethinking the design of the internet: The end-to-end arguments vs. the brave new world," *ACM Journals*, pp. 70–109, 2001. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/383034.383037

[26] C. D., B. R., S. K., W. J., K. D., K. J., Y. X., F. T., F. A., P. V., and H. M. e Chiappa, "New arch: Future generation internet architecture," *MIT Laboratory for Computer Science and International Computer Science Institute (ICSI)*, 2004. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA426770

[27] I. T. Union, "Imt traffic estimates for the years 2020 to 2030," *ITU-R*, 2015. [Online]. Available: https://www.itu.int/pub/R-REP-M.2370-2015

[28] H. G. e Vaidya N., "Analysis of tcp performance over mobile ad hoc networks," *Springer Wireless Network*, pp. 275–288, 2002. [Online]. Available: https://link.springer.com/article/10.1023/A:1013798127590

[29] I. T. Union, "Cisco annual internet report (2018–2023)," *Cisco Anual Report*, 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[30] Bellovin, S. Michael, C. D. D. P. Adrian, and S. Dawn, "A clean-slate design for the next-generation secure internet," *Computer Science*, 2006. [Online]. Available: https://academiccommons.columbia.edu/doi/10.7916/D8BV7PCM

[31] J. Haworth, "Cyber-attack at vodafone portugal knocks mobile network services offline," *The Daily Swig*, 2022. [Online]. Available: https://portswigger.net/daily-swig/cyber-attack-at-vodafone-portugal-knocks-mobile-network-services-offline

[32] TelecomLead, "T-mobile faces cyber attack by lapsus$ hacking group," *TelecomLead*, 2022. [Online]. Available: https://www.telecomlead.com/telecom-services/t-mobile-faces-cyber-attack-by-lapsus-hacking-group-104460

[33] M. J. e Reiher P., "Building accountability into the future internet," *IEEE Access*, 2008. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4664880

[34] Netscout, "The long tail of attacker innovation," *Netscout therat intelligence report*, 2021. [Online]. Available: https://www.netscout.com/threatreport/conclusion/

[35] L. C., A. A., and B. A. e Jahanian F., "Delayed internet routing convergence," *ACM Journals*, pp. 175 – 187, 2000. [Online]. Available: https://academiccommons.columbia.edu/doi/10.7916/D8BV7PCM

[36] M. J. e Reiher P, "Overcoming the internet impasse through virtualization," *IEEE Access*, pp. 34 – 41, 2005. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1432642

[37] J. F. Kurose and K. W. Ross, *Computer Networking A Top-Down Approach Featuring the Internet*. Pearson Education India, 2004.

[38] A. M. Alberti, "Novagenesis: Convergent information architecture," *Ina-*

*tel*, December 2012. [Online]. Available: https://www.inatel.br/novagenesis/specifications

[39] A. M. Alberti, M. A. F. Casaroli, D. Singh, and R. da Rosa Righi, "Naming and name resolution in the future internet: Introducing the novagenesis approach," *Elsevier*, vol. 67, pp. 163–179, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X16302643

[40] J. A. T. Gavazza, J. C. Melo, T. B. da Silva, A. M. Alberti, P. F. Rosa, F. de Oliveira Silva ane Fábio L. Verdi, and J. A. Suruagy, "Future Internet Exchange Point (FIXP): Enabling Future Internet Architectures Interconnection," *Springer, Cham*, 2020. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-44041-1_62

[41] T. B. da Silva, "Novagenesis control agent for future internet exchange point," *Tese de Mestrado*, December 2021. [Online]. Available: https://inatel.br/biblioteca/dissertacoes-mestrado

[42] A. M. Alberti, V. H. d. O. Fernandes, M. A. F. Casaroli, L. H. d. Oliveira, F. M. P. Júnior, and D. Singh, "A novagenesis proxy/gateway/controller for openflow software defined networks," *IEEE Internet of Things Journal*, pp. 394–399, 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7014201

[43] S. P. S. M. IEEE, R. K. J. S. M. IEEE, and I. Sanjeev Jain Member, "A survey on energy efficient narrowband internet of things (nbiot): Architecture, application and challenges," *IEEE Access*, no. 7, pp. 2169–3536, November 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/853638

[44] R. S. Sinha, Y. Wei, and S.-H. Hwang, "survey on lpwa technology: Lora and nb-iot," *Elsevier - Science Direct*, March 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959517300061

[45] M. C. S. M. IEEE, Y. Miao, Y. H. S. M. IEEE, and K. H. L. F. IEEE, "A survey on energy efficient narrowband internet of things (nbiot): Architecture, application and challeng," *IEEE Access*, pp. 16 739 – 16 776, 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8536384

[46] I. T. Unnion, "Minimum requirements related to technical performance for imt-2020 radio interface," *ITU-R*, 2017. [Online]. Available: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf

[47] R. Ratasuk, N. Mangalvedhe, D. Bhatoolaul, and A. G. N. B. L. A. H. I. USA, "Lte-m evolution towards 5g massive mtc," *IEEE Access*, 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8269112

[48] J. de Carvalho Silva, J. J. P. C. Rodrigues, A. M. Alberti, P. Solic, and A. L. L. Aquino, "Lorawan - a low power wan protocol for internet of things: a review and opportunities," *Resource Gate*, no. 5, pp. 1–7, Jully 2017. [Online]. Available: https://www.researchgate.net/publication/318866065_LoRaWAN_-_A_Low_Power_WAN_Protocol_for_Internet_of_Things_a_Review_and_Opportunities

[49] N. S. (Semtech), M. L. (Semtech), T. E. (IBM), T. K. (IBM), and H. (Actility), "Lorawan specification," *LoRa Alliance*, January 2015. [Online]. Available: https://lora-alliance.org/resource_hub/lorawan-specification-v1-1/

[50] L. Vangelista1, A. Zanella, and M. Zorzi, "Long-range iot technologies: The dawn of lora," *Springer, Cham*, December 2015. [Online]. Available: https://lora-alliance.org/resource_hub/lorawan-specification-v1-1/

[51] R. A. B. Kpadonou, T. Owiyo, B. Barbier, F. Denton, F. Rutabingwa, and A. Kiema, "Advancing climate-smart-agriculture in developing drylands: Joint analysis of the adoption of multiple on-farm soil and water conservation technologies in west african sahel," *Land Use Policy*, vol. 61, pp. 196–207, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0264837716300187

[52] T. B. V. Blok and I. Coninx, "Barriers to the adoption and diffusion of technological innovations for climate-smart agriculture in europe: evidence from the netherlands, france, switzerland and italy," *Journal of Cleaner Production*, vol. 112, pp. 9–21, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0959652615007738

[53] H. Neufeldt, M. Jahn, B. M. Campbell, J. R. Beddington, F. DeClerck, A. D. Pinto, J. Gulledge, J. Hellin, M. Herrero, A. Jarvis, D. LeZaks, H. Meinke, T. Rosenstock, M. Scholes, R. Scholes, S. Vermeulen, E. Wollenberg, and R. Zougmoré, "Beyond climate-smart agriculture: toward safe operating spaces for global food systems," *Agriculture and Food Security*, vol. 2, 2013. [Online]. Available: https://agricultureandfoodsecurity.biomedcentral.com/articles/10.1186/2048-7010-2-12#citeas

[54] J. Hammonda, S. Fraval, J. van Etten, J. G. Suchini, L. Mercado, T. Pagella, R. Frelat, M. Lannerstad, S. Douxchamps, N. Teufel, D. Valbuena, and M. T. Wijk, "The rural household multi-indicator survey (rhomis) for rapid characterisation of households to inform climate smart agriculture interventions: Description and applications in east africa and central america," *Agricultural Systems*, vol. 151, pp. 225–233, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0308521X16301172

[55] N. Alexandratos and J. Bruinsma, "World agriculture towards 2030/2050," *ESA Working Paper No. 12-03*, June 2012.

[56] ——, "Overview of smart farming based on networks - recommendation itu-t y.2238," *ITU-T*, June 2015.

[57] H. Automation, "Wifi lora 32 is a part of the "heltec lora" series," *Technical Datasheet*, 2018. [Online]. Available: https://heltec.org/project/wifi-lora-32/

[58] A. M. Alberti, "novagenesis," *github*, 2008. [Online]. Available: https://github.com/antonioalberti/novagenesis

[59] L. C. P. de Leon. Yara Maria Botti Mendes de Oliveira e Raquel Cymorot, "Estudo dos níveis de radiações eletromagnéticas de alta frequência em uma importante avenida da cidade de são paulo," *Mackenzie*, Julho 2007. [Online]. Available: http://meusite.mackenzie.com.br/raquelc/SHEWC2007Paulista.pdf

[60] A. Networks, "Aruba 200 serie access point," *Technical Datasheet*, August 2017. [Online]. Available: https://www.arubanetworks.com/assets/ds/DS_AP200Series.pdf

[61] Z. C. Ge Ma, "Comparative study on ccn and cdn," *IEEE Xplore*, 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6849209/authors#authors

[62] E. Bonomo, R. H. do Santos, and A. M. Alberti, "Novagenesis over lora in an iot scenario," *SBC*, May 2022. [Online]. Available: https://sol.sbc.org.br/index.php/wpeif/issue/archive