ATUALIZAÇÃO DA TECNOLOGIA LMR PARA A LTE EM APLICAÇÕES DAS FORÇAS ARMADAS

JOSÉ RICARDO DA ASSUNÇÃO FERREIRA

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ATUALIZAÇÃO DA TECNOLOGIA LMR PARA A LTE EM APLICAÇÕES DAS FORÇAS ARMADAS

JOSÉ RICARDO DA ASSUNÇÃO FERREIRA

ORIENTADOR: UGO SILVA DIAS

DISSERTAÇÃO DE MESTRADO EM
ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGEE.DM-799/22

BRASÍLIA/DF: DEZEMBRO - 2022

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ATUALIZAÇÃO DA TECNOLOGIA LMR PARA A LTE EM APLICAÇÕES DAS FORÇAS ARMADAS

JOSÉ RICARDO DA ASSUNÇÃO FERREIRA

APROVADA POR:

_____

Prof. Dr. UGO SILVA DIAS – ENE/Universidade de Brasília
Orientador

_____

Prof. Dr. GEORGES DANIEL AMVAME NZE – ENE/Universidade de Brasília
Membro Interno

_____

Prof. Dr. TERCIO BRUM – Instituto Militgar de Engenharia
Membro Externo

BRASÍLIA, 15 DE DEZEMBRO DE 2022.

FICHA CATALOGRÁFICA

FERREIRA, JOSÉ RICARDO DA ASSUNÇÃO
Atualização da tecnologia LMR para a LTE em aplicações das Forças Armadas [Distrito Federal] 2022.
xix, 90p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Forças Armadas	2. LTE-4G
3. LMR	4. Banda Larga
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

FERREIRA, J.R.A. (2022). Atualização da tecnologia LMR para a LTE em aplicações das Forças Armadas . Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGEE.DM-799/22, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 90p.

CESSÃO DE DIREITOS

AUTOR: JOSÉ RICARDO DA ASSUNÇÃO FERREIRA
TÍTULO: Atualização da tecnologia LMR para a LTE em aplicações das Forças Armadas .
GRAU: Mestre ANO: 2022

JOSÉ RICARDO DA ASSUNÇÃO FERREIRA

Departamento de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

Dedicatória

O presente trabalho é dedicado aos meus familiares , meus pais Júlio Alves Ferreira e Maria Aparecida da Assunção Ferreira e também a minha irmã Nathália da Assunção Ferreira, pelo apoio incentivo e compreensão na conquista deste objetivo profissional.

Agradecimentos

A Deus, por me dar saúde sabedoria e paciência para conseguir lograr êxito nessa jornada.

Aos meus familiares pelo apoio e incentivo.

Aos meus pais Júlio Alves Ferreira e Maria Aparecida da Assunção Ferreira pelo incentivo e companheirismo, por estarem sempre ao meu lado prestando todos os tipos de apoio.

Ao professor Ugo Silva Dias, que nessa jornada não foi apenas o guia da jornada acadêmica, mas também um amigo que tinha as palavras certas para confortar nas horas de aflição na realização desse trabalho.

Aos companheiros e amigos que contribuíram nessa jornada.

Resumo

Este trabalho apresenta uma investigação prática dos serviços que podem ser disponibilizados com a tecnologia 4G/LTE em proveito dos órgãos da Defesa Nacional, neles englobados as Forças Armadas e os Órgão de Segurança Publicada. Nesse sentido foi realizado e apresentado um estudo a respeito das características específicas dos serviços de telefonia celular para a defesa nacional e segurança pública. Características como segurança e continuidade. Nesse contexto analisou-se também quais funcionalidades seriam possíveis serem implementadas pela tecnologia 4G. Por outro lado verificou-se a integração dessa tecnologias aos sistemas já existentes, verificando as possibilidades de coexistência do ponto de vista de interoperabilidade entre os sistemas. Além disso, realizou-se um estudo de caso para verificar a possibilidade de instalação de uma estrutura de banda larga para utilização das Forças Armadas com base da implantação realizada nos Estados Unidos. Finalizando, foram realizados testes com o sistemas de telefonia celular privada 4G com o objetivo de coletar dados para a conclusão do presente trabalho. Esses resultados mostraram um excelente desempenho do ponto de vista de atendimento as demandas das Forças Armadas nos quesitos de segurança, confiabilidade e continuidade.

Palavras-chave: Defesa Nacional, Confiabilidade, interoperabilidade e segurança, 4G/LTE

Abstract

This work presents a practical investigation of the services that can be made available with the technology 4G/LTE technology for the benefit of National Defense bodies, including the Armed Forces and Published Security. In this sense, a study was carried out and presented regarding the characteristics specifications of cell phone services for national defense and public safety. Features such as security and continuity. In this context, it was also analyzed which functionalities could be implemented. maintained by 4G technology. On the other hand, the integration of these technologies to the systems already existing ones, verifying the possibilities of coexistence from an interoperability point of view between the systems. In addition, a case study was carried out to verify the possibility of installing a broadband structure for the use of Armed Forces based on the implementation carried out in the United States. Finally, they were tests were carried out with the 4G private cell phone systems in order to collect data for the completion of this work. These results showed an excellent performance from the point of view to meet the demands of the Armed Forces in terms of security, reliability and continuity.

Keywords: National Defense, Reliability, Interoperability and Security, 4G/LTE

Sumário

Lista de Figuras

Lista de Abreviaturas e Siglas

1G Primeira Geração.

2 CTA 2º Centro de Telemática de Área.

2G Segunda Geração.

3G Terceira Geração.

3GPP *Third Generation Partnership Project.*

4G Quarta Geração.

5G Quinta Geração.

6G Sexta Geração.

ACB *Access Class Baring.*

AeHetNets *Aerial Heterogeneous Networks.*

AES *Advanced Encryption Standard.*

AMPS *Advanced Mobile Phone Service.*

ANATEL Agência Nacional de Telecomunicações.

APCO *Associated PublicSafety Communications Officers.*

APF Administração Pública Federal.

ARP *Address Resolution Protocol .*

AT&T *American, Telephone and Telegraph.*

BB *Broadband.*

BER *Bit Error Ratio.*

BEsCom Batalhão Escola de Comunicações.

C2 Comando e Controle.

C4FM *Compatible 4-Level Frequency Modulation.*

CAPEX *Capital Expenditure.*

CComGEx Centro de Comunicações e Guerra Eletrônica do Exército.

CCOp Mv Centro de Coordenação de Operações Móvel.

CDMA *Code Division Multiple Access.*

CN Centros Nodais.

COBRA Combatente Brasileiro.

COTer Comando de Operações Terrestres.

DE Divisão de Exército.

DHS *Department of Homeland Security.*

DMO *Direct Mode Operation.*

DNS *Domain Name System.*

DoD *Department of Defense.*

DoS *Denial of Service.*

DQPSK *Differential Quadrature Phase-Shift Keying.*

E-UTRAN *Evolved UMTS Terrestrial Radio Access Network.*

EB Exército Brasileiro.

EBChat Serviço de Mensageria Eletrônica do Exército.

EBCloud Nuvem Privada do EB.

EBNet Rede Corporativa de Comunicações do Exército.

EDGE *Enhanced Data rates for GSM Evolution.*

END Estratégia Nacional de Defesa.

eNodeB *Evolved Node B.*

EPC *Evolved Packet Core.*

EPS-AKA *Evolved Packet System based Authentication and Key Agreement.*

ERB Estação Rádio Base.

ETSI *European Telecommunications Standards Institute.*

EUA Estados Unidos da América.

FA Forças Armadas.

FAC2FTer Família de Aplicativos de Comando e Controle da Força Terrestre.

FDD *Frequency Division Duplex.*

FDMA *Frequency Division Multiple Access.*

FirstNet *First Responder Network Authority.*

FM *Frequency Modulation.*

GAO *Government Accountability Office.*

GCSE *Group Communication System Enabler.*

GLO Garantia da Lei e da Ordem.

GMSK *Gaussian Minimum Shift Keying.*

GPRS *General Packet Radio Service.*

GPS *Global Positioning System.*

GSM *Global System for Mobile.*

HetNet *Heteregeneous network.*

HSS *Home Subscriber Server.*

ICAM *Identity, Credential, and Access Management.*

IDR *Independent Digital Repeate.*

IEEE Instituto de Engenheiros Eletricistas e Eletrônicos.

IMS IP Multimidia Subsystem.

IP *Internet Protocol*.

IPERF *Internet Performance Working Group*.

JTACs *Japanese Total Access Communication System*.

LMR *Land Mobile Radio*.

LMRS *Land Mobile Radio System*.

LTE *Long-Term Evolution*.

MD Ministério da Defesa.

MME *Mobile Management Entity*.

NA Nós de Acesso.

NB *Narrowband*.

NIST *National Institute of Standards and Technology*.

NMT *Nordic Mobile Telecomunications*.

NOC *Network Operation Center*.

NTT *Nippon Telegraph and Telephone*.

OFDMA *Orthogonal Frequency Division Multiplexing/Multiple Access*.

OMA *Open Mobile Alliance*.

OPEX *Operational Expenditure*.

OSP Órgãos de Segurança Pública.

P-GW PDN-*gateway*.

P2P *Peer-to-peer*.

PC Posto de Comando.

PC *Personal Computer*.

PDN *Packet Data Network.*

PF Polícia Federal.

PPDR *Public Protection & Disaster Relief.*

PRF Polícia Rodoviária Federal.

ProSe *Proximity Services.*

PS-LTE *Public Safety LTE.*

PTT *Push-To-Talk.*

QoS *Quality of Service.*

RAN *Radio Access Network.*

RF Radiofrequência.

RFP *Request for Proposal.*

RITEx Rede Integrada de Telecomunicações do Exército.

RTLS *Real-time locating system.*

RTM *Radio Teléfono Móvil.*

S-GW *Serving Gateway.*

S&T *Science and Technology Directorate.*

SAM Sistema do Assinante Móvel.

SC-FDMA *Single Carrier-Frequency Division Multiple Access.*

SCCFTer Sistema de Comando e Controle da Força Terrestre.

SCM Serviço de Comunicação Multimídia.

SIM *Subscriber Identity Module.*

SisBol Sistema de Boletim.

SisCAU Sistema de Controle de Acesso de Usuários.

SISCOMIS Sistema de Comunicações Militares por Satélite.

SISTAC Sistema Tático de Comunicações.

SLP Serviço Limitado Privado.

SMP Serviço Móvel Pessoal.

SNR *Signal-to-Noise Ratio.*

SPED Sistema de Protocolo Eletrônico de Documentos.

SRDT Sistema de Radiocomunicação Digital Troncalizado.

STFC Serviço Telefônico Fixo Comutado.

TACS *Total Access Comunications System.*

TCP *Transmission Control Protocol.*

TDD *Time Division Duplex.*

TDMA *Time Division Multiple Access.*

TELEBRAS Telecomunicações Brasileiras S/A.

TETRA *Terrestrial Trunked Radio.*

TETRAPOL *Terrestrial Trunked Radio Police.*

TIA *Telecommunications Industries Association.*

TIC Tecnologia de Informação e Comunicações.

TMO *Trunking Mode Operation.*

Ton toneladas.

UE *User Equipment.*

UHF *Ultra High Frequency.*

UMTS *Universal Mobile Telecommunications System.*

USB *Universal Serial Bus.*

USIM *Universal Subscriber Identity Module.*

VHF *Very High Frequency.*

VoIP *Voice over Internet Protocol*.

VoLTE *Voice over LTE*.

Vtr Viatura militar.

W-CDMA *Wide-Band Code-Division Multiple Access*.

WB *Wideband*.

1 Introdução

1.1 Contextualização

As Forças Armadas (FA) e os Órgãos de Segurança Pública (OSP) são entidades que servem ao estado brasileiro e tem como finalidade, entre outras coisas, atividades de operações de emergência em que o fundamental é auxiliar a sociedade por meio de ações de Proteção Pública e Resposta a Desastres, Serviços de Socorro e Emergência e apoio à Infraestrutura de Governo nas atividades de fiscalização. Além disso ações como combate ao crime organizado, operações de Garantia da Lei e da Ordem (GLO) operações policiais, combate a incêndios, resposta médica de emergência, segurança de fronteiras e recuperação de desastres.

Nesse contexto, esses órgãos necessitam de coordenação das operações para garantir o pleno sucesso das operações por meio de sistemas de comunicações críticas. Comunicações essas que não podem falhar e devem operar no regime de 24/7 (vinte e quatro horas por dia, sete dias por semana) com confiabilidade, resiliência, prioridade de tráfego, durante as operações. As FA e os OSP utilizam a tecnologia de rádio conhecida como LMR a qual fornece basicamente serviços de voz, no entanto baixa taxa de dados. Essa tecnologia possui os padrões *Associated PublicSafety Communications Officers* (APCO)25, *Terrestrial Trunked Radio* (TETRA), além do padrão proprietário *Terrestrial Trunked Radio Police* (TETRAPOL).

Assim, o sistema de comunicações críticas das FA que utiliza a tecnologia de rádio móvel padrão APCO25 provê redes de voz e de dados de baixa capacidade, com sistemas espalhados por todos os estados brasileiros com presença em todas as capitais que foram sede dos eventos das Copas das Confederações, Olimpíadas e Copa do Mundo.

De outro modo, cada um dos diversos OSP possuem seu próprio sistema de comunicações críticas com tecnologias distintas, como por exemplo a Polícia Federal (PF) que utiliza a tecnologia de rádio móvel padrão TETRAPOL e a Polícia Rodoviária Federal (PRF) que utiliza a tecnologia de rádio móvel padrão TETRA. Essa diversidade de

tecnologias inviabiliza a integração dos sistemas de comunicações críticas desses órgãos, dificultando a coordenação das operações conjuntas das FA e os OSP.

Por outro lado, a tecnologia LMR, por possuir baixa taxa de dados, não suporta banda larga, provendo basicamente serviços de voz. Porém, as demandas atuais para coordenação das operações das FA e OSP necessitam de sistemas de banda larga que possam fornecer serviços de multimídia, transmissão de vídeo de alta definição (HD), *streaming* de vídeo ao vivo, acesso a banco de dados, compartilhamento de arquivos e utilização de aplicativos de coordenação operacional.

Nesse sentido, é conveniente a utilização de um sistema de banda larga unificado com o objetivo de uso de forma compartilhada entre todos os OSP e FA. Além disso, esse sistema deve suportar serviços de banda larga, mantendo a mesma escalabilidade, robustez e resiliência dos sistemas LMR.

1.2 Justificativa

No Brasil foi definido o plano de Distribuição de Banda Larga, [1] o qual visa buscar ampliações sistemáticas do LTE/Quarta Geração (4G) para todos os OSP, FA e defesa nacional. Esse sistema possibilitará uma maior integração dos meios de comunicações de alta taxa de dados, além disso, teremos a otimização da utilização do espectro da banda destinada à segurança pública, defesa nacional e infraestrutura. A utilização plena dessa tecnologia poderá prover comunicações adequadas aos ciclos de Comando e Controle (C2) além da consciência situacional das FA e OSP, atendendo prioritariamente à defesa nacional por intermédio das FA e à segurança nacional, pela garantia da interoperabilidade com OSP e de outros órgãos de interesse da segurança nacional.

Dessa forma, a tecnologia de banda larga LTE é uma tecnologia promissora para banda larga compartilhada das FA e os OSP, devido as suas particularidades de possibilitar comunicações de banda larga, e suportar serviços de multimídia com altas taxas de dados, serviços esses padronizados pelos protocolos da rede *Transmission Control Protocol* (TCP)/*Internet Protocol* (IP). Por outro lado, é necessário realizar uma investigação criteriosa sobre a possibilidade de utilização dessa tecnologia como uma atualização da tecnologia LMR, possibilitando assim, a mesma confiabilidade desse sistema, além de possibilitar, ainda, as funcionalidades de banda larga e interoperabilidade entre os usuários públicos.

Nesse contexto, a atualização das redes de voz segregadas LMR para uma rede de banda larga interoperável baseada em uma tecnologia LTE é um desejo das FA e OSP,

tendo como consequência a necessidade de realização de uma análise criteriosa dessa possibilidade, tendo em vista os diversos desafios técnicos e econômicos, além da falta de conhecimento para que tal atividade possa ser viabilizada.

Essa análise é pertinente, no sentido em que as redes de banda estreita LMR são tecnologias que já são desenvolvidas com o objetivo de atender as demandas de comunicações críticas. Por outro lado, as redes de banda larga LTE são tecnologias desenvolvidas tipicamente para atendimento às comunicações de uso comercial.

Nesse sentido, a presente dissertação tem como justificativa a realização de uma pesquisa criteriosa buscando as respostas de uma possível atualização dos sistemas LMR para o LTE 4G para os OSP e FA.

Dessa forma, esse trabalho buscará soluções para as seguintes limitações dos sistemas de comunicações críticas das FA e OSP:

- O sistemas de banda estreita não atendem à demanda dos serviços de multimídia que necessitam de alta taxa de dados;
- Falta de Interoperabilidade sistêmica entre as redes de banda estreita das FA e as redes dos demais OSP nos três níveis da administração pública;
- Sistemas de banda estreita sem integração sistêmicas com sistemas de banda larga;
- Falta de integração sistêmica dos sistemas de comunicações críticas e as redes IP Segunda Geração (2G), Terceira Geração (3G), 4G, Quinta Geração (5G), *wi-fi*;
- Alto custo de implantação, manutenção, operação e sustentabilidade de uma rede de banda larga LTE proprietária.

1.3 Objetivos do Projeto

1.3.1 Objetivo Geral

O objetivo geral dessa dissertação é verificar a viabilidade de atualização do sistema de banda estreita LMR para um sistema de banda larga LTE, no contexto de utilização em comunicações críticas das FA e os OSP. Assim como, apresentar uma alternativa que possa viabilizar a implantação desse sistema no Brasil, por meio da utilização dual, ou seja, com o compartilhamento de utilização para as redes de comunicações criticas e exploração comercial. Nesse contexto, verificar também os serviços que essa tecnologia de banda larga pode prover para a aplicação das missões típicas do EB, assim como seus projetos institucionais.

1.3.2 Objetivo Específico

O objetivo específico dessa dissertação buscou analisar as funcionalidades e futuras aplicações da tecnologia 4G para as atividades de segurança pública e FA. Nesse contexto, verificar a aplicação pratica da tecnologia 4G para atender as demandas de comando e controle da Força terrestre nos seus projetos estratégicos e nas missões específicas de Guerra e não Guerra. Analisar a possibilidade de utilização do sistema 4G como uma evolução do LMR (P25) das das FA e os OSP.

Além disso, propor uma solução para o compartilhar recursos de comunicações de voz e dados dados, das redes de comunicações críticas com a banda larga LTE/4G, entre todos os órgãos da Administração Pública Federal (APF), promovendo assim, a interoperabilidade sistêmica entre as FA e todas as agências que possam vir a ter envolvimento em ações que visem garantir a segurança nacional, em especial, durante Operações Interagências, diminuindo assim os custos de instalação, operação e de manutenção do sistema. Por meio de uma sinergia de recursos provenientes das entidades dos três níveis da administração que são o nível federal, o nível estadual e o nível municipal.

Nesse contexto, a presente dissertação tem como objetivos específicos, além do citado acima, apresentar as seguintes contribuições:

- Verificar a existência da aplicabilidade dos serviços de banda larga para as comunicações críticas em redes da Defesa Nacional e segurança pública;
- Verificar a possibilidade de integração e coexistência entre as redes LTE e LMR;
- Verificar se já foi realizada a integração e coexistência entre as redes LTE e LMR no Brasil, e em particular no EB;
- Verificar a existência de vantagem na utilização da tecnologia LTE para as FA e a segurança pública em comparação com as redes LMR;
- Verificar se há previsão de utilização dessa tecnologia nos projetos do EB;
- Verificar a possibilidade de utilização das redes LTE de forma compartilhada entre a defesa nacional, segurança pública e exploração comercial por meio de compartilhamento de excedente de banda;
- Verificar os desafios técnicos na atualização da rede LMR para a rede LTE;
- Verificar a possibilidade do LTE se tornar a rede de banda larga unificada e compartilhada entre os OSP e FA, resolvendo a falta de integração e interoperabilidade de sistemas entre as diferentes agências;

- Propor um modelo de implementação do sistema de banda larga que atenda as características de comunicações críticas;
- Apresentar um modelo de sustentabilidade de implantação de uma rede LTE com exploração comercial da banda excedente;
- Validar o LTE como sistema de comunicações de banda larga brasileiro; e
- Comprovar, por meio de realização de testes práticos, as funcionalidade da rede de banda larga LTE nos projetos do EB.

1.4 Metodologia

Para atender os objetivos, tanto gerais como específicos, a presente dissertação constituiu-se, basicamente, de três fases distintas, porém totalmente complementares:

A primeira fase abordou a pesquisa bibliográfica e documental à respeito dos assuntos técnicos necessários para servir de base para fornecer a fundamentação teórica para elaboração do trabalho. Nesse sentido, nessa primeira fase foram estudados os seguintes assuntos: comunicações críticas, serviços de comunicações críticas, frequências para utilização das FA, tecnologia de banda estreita LMR, tecnologia de banda larga LTE e projetos das FA com demanda de serviços de banda larga.

A segunda fase abordou um estudo de caso da implantação da tecnologia de banda larga com exploração dual de uso público e privado utilizado nos EUA e a proposição de uma possível implementação no Brasil com base nesse estudo de caso. Essa proposição tem como objetivo estudar as possibilidades de implementação do uso dual da tecnologia de banda larga LTE tanto para as FA, quanto para exploração comercial.

A terceira fase abordou a realização de testes em campo e, nesses testes, buscou-se explorar as possibilidades da tecnologia de banda larga LTE para o atendimento das demandas dos serviços de comunicações críticas de voz, dados e multimídia para as FA.

Por outro lado, a presente dissertação tratou-se de uma pesquisa, com relação ao objetivo de estudo, do tipo exploratória, uma vez que procurou explicar os conceitos relacionados ao problema analisado e sintetizou os conhecimentos necessários para a elaboração de propostas de soluções a serem realizadas no atendimento do objetivo. Em um outro sentido, quanto à natureza, a dissertação aqui descrita é aplicada, no sentido em que busca apresentar soluções para a atualização da tecnologia de banda estreita LMR para banda larga LTE em aplicações das FA.

1.5 Apresentação do Manuscrito

O trabalho se organiza de maneira a permitir ao leitor acompanhar o desenvolvimento deste projeto.

No Capítulo 2, é abordada a Revisão Bibliográfica, contendo a evolução dos sistemas de 4G/LTE assim como sua arquitetura, bandas de frequência e histórico de evolução, finalizando a apresentação da tecnologia utilizada nas redes de segurança pública e suas características.

No Capítulo 3, são apresentados os serviços de uma rede LTE de banda larga para os órgãos, assim como a comparação entre a tecnologia LTE e LMR do ponto de vista da aplicações em comunicações críticas, e finalizando, a aplicação dessa tecnologia nos projetos do EB.

No Capítulo 4, é abordado a forma de integração das redes LTE com as redes LMR, em particular a rede P25.

No Capítulo 5, são abordados os modos de implantação da rede de banda larga com uso dual da tecnologia LTE para os OSP e Defesa Nacional no Brasil.

A seguir, o Capítulo 6, apresenta o resultado, os dados coletados dos testes dos serviços da rede telefonia celular privada 4G aplicadas ao EB baseados em testes práticos de funcionalidade dos sistemas.

Finalizando, o Capítulo 7, apresenta as considerações finais e propõe a realização de trabalhos futuros.

2 Revisão Bibliográfica

2.1 A Evolução da Telefonia Móvel até a Terceira Geração

Os sistemas de telefonia móvel evoluíram da telefonia de Primeira Geração (1G), até a tecnologia de 4G. Essa evolução ocorreu a partir de 1980 e continua evoluindo até os dias de hoje com o advento dos sistemas de telefonia de quinta e sexta geração, respectivamente 5G e Sexta Geração (6G).

As características gerais desses sistemas são a utilização de uma Estação Rádio Base (ERB) com cobertura celular por meio de enlaces sem fio (*wireless*), em formato de célula hexagonal, uma controladora e os terminais do usuário. Nesse sentido todas as gerações são sistemas de telefonia móvel.

De outra forma esses sistemas possuem tecnologias, modulações, protocolos de acesso múltiplo ao meio, taxa de dados e serviços específicos de cada geração. A seguir serão apresentadas as características e peculiaridades da evolução da telefonia da primeira geração a terceira geração.

A 1G surgiu em 1980 e tinha como característica básica ser um sistema apenas para voz. Foi o primeiro sistema de telefonia móvel e utilizava a codificação analógica. A tecnologia utilizada era o padrão *Advanced Mobile Phone Service* (AMPS). A metodologia de acesso ao canal utilizado era o *Frequency Division Multiple Access* (FDMA) que dividia o canal de acesso em sub-faixas de frequências. O sistema utilizava a *Frequency Modulation* (FM) (modulação em frequência).

Outra característica era a diversidade de padrões de tecnologias utilizadas ao longo do mundo. Nesse sentido, cada padrão tinha suas características técnicas exclusivas e assim, não havia interoperabilidade entre os padrões. Dessa forma, pela diversidade de tecnologias, esse sistema celular não possibilitava o *roaming*. Como exemplo dessa tecnologia espalhada pelo mundo em vários continentes tem-se a AMPS, o *Nordic Mo-*

bile Telecomunications (NMT), o *Total Access Comunications System* (TACS), o RC2000 (RADIOCOM2000), o , o C450, o *Japanese Total Access Communication System* (JTACs) e,finalmente, o *Nippon Telegraph and Telephone* (NTT). Totalizando mais de cinco padrões diferentes.

A 2G surgiu em meados de 1990 e já apresentava como modificações básicas em relação à primeira geração, a utilização de codificação digital e a introdução do *Subscriber Identity Module (SIM) card*. O sistema era para voz e transmissão de dados de baixa capacidade. Como metodologia de acesso ao canal, essa geração utilizava o *Time Division Multiple Access* (TDMA) e o *Code Division Multiple Access* (CDMA). Outra modificação fundamental foi possibilidade de realização de *roaming*.

A tecnologia dessa geração tem como padrão de evolução a do *Global System for Mobile* (GSM), para o *General Packet Radio Service* (GPRS) e dessa para o *Enhanced Data rates for GSM Evolution* (EDGE). Elas se caracterizam pela crescente capacidade de transmissão de dados. O GSM era conhecido como 2G, já o GPRS, que utilizava comutação por pacotes de dados, era conhecido como 2,5G, e finalmente o EDGE era conhecido como 2,75G.

A 3G surgiu no início dos anos 2000, e tinha como característica principal a possibilidade de acesso à internet de serviços de multimídia pelo fato de possuir taxas de dados muito mais altas que os sistemas 2G. Os terminais celulares dessa geração utilizavam o *browse* para acesso à internet. As principais tecnologias dessa geração são o *Universal Mobile Telecommunications System* (UMTS) e o *Wide-Band Code-Division Multiple Access* (W-CDMA), sendo essa última a responsável pela compatibilidade com os sistemas 2G.

A figura 2.1 apresenta a evolução da tecnologia de telefonia móvel, exaltando os diversos tipos de tecnologias, assim como os diversos tipos de padrões aplicados a cada geração.

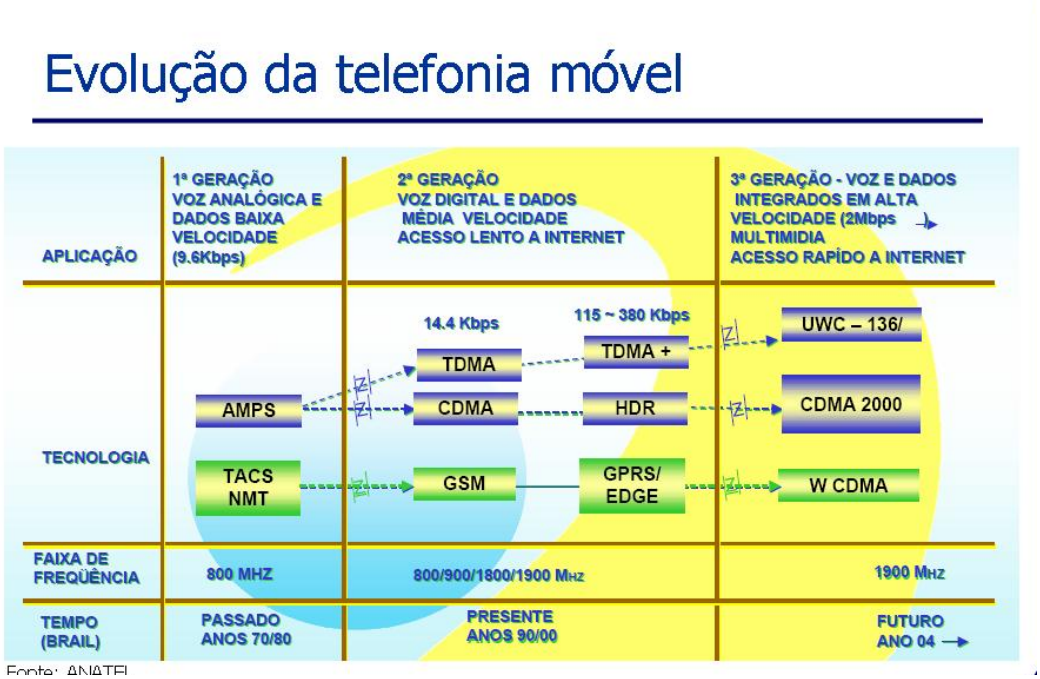

Figura 2.1: Evolução da rede de telefonia móvel até a terceira geração
Fonte: ANATEL

2.2 Evolução da tecnologia LTE (*Long-Term Evolution*)

O 4G LTE, é o sistema de telefonia de quarta geração que possibilita acesso móvel à internet. Diferente das gerações anteriores, ele é totalmente IP, ou seja, todos os dados trafegam por meio de protocolos das cinco camadas TCP/IP. Todas as especificações e características técnicas são padronizadas pela 3GPP. A qual padronizou as premissas desse sistema por meio da *TS Technical Especification* 25-915.

Como a tecnologia de acesso ao canal ele utiliza o TDMA, o FDMA e o CDMA, além do *Single Carrier-Frequency Division Multiple Access* (SC-FDMA), possibilitando assim altas taxas de dados. Além disso, essa tecnologia permite a utilização e agregação de várias bandas de frequências. Em outras palavras essa característica técnica possibilita a utilização do LTE em diversos cenários de diversidade de disponibilidade de faixas de frequências.

O sistema de telefonia LTE tem compatibilidade com os sistemas de telefonia 2G e 3G, possibilitando, dessa forma, a utilização com sistemas de telefonia legadas. Ele possui a tecnologia de separação de canais de transmissão e recepção, o *Frequency Division Duplex*

(FDD) e a utilização de um único canal para transmissão e recepção, o *Time Division Duplex* (TDD).

- Largura de banda variável, respectivamente 1,4, 3,5, 10, 15 e 20 MHz, sendo essa última a que possibilita as maiores taxas de dados;
- Interoperabilidade com redes 3GPP e redes não 3GPP;
- Latência baixa, na ordem de 10 milissegundos;
- Altas taxas de dados, chegando a 350 Mbps na jusante e 75 Mbps na montante;
- Modulação adaptativa, variando com os parâmetros da *Signal-to-Noise Ratio* (SNR) (Relação Sinal-Ruído) e *Bit Error Ratio* (BER) (Taxa de Erros de Bit);
- Alta mobilidade dos hospedeiros sem fio, podendo serem usados em deslocamentos com velocidades de mais de 150 km/h sem perder acesso à internet;

Do ponto de vista de interoperabilidade, o LTE foi projetado para realizar conexões com todas as rede de protocolo TCP/IP. Dessa forma enquadram-se tanto as rede IP tipicamente 3GPP como as redes de telefonia de segunda e de terceira geração, como redes tipicamentes não 3GPP como as redes Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE) 802.11 *Wi-Fi* entre outras.

2.3 A Arquitetura 4G LTE (*Long-Term Evolution*)

A rede de telefonia de 4G LTE herdou alguns equipamentos legados das redes de 3G justamente para se manter a possibilidade de comunicação dessa rede heterogênica com núcleos diferentes. Basicamente o LTE possui sua arquitetura baseada em três camadas com funcionalidades distintas, porém interligadas física e logicamente. São elas; a *Radio Access Network* (RAN) que fornece o acesso rádio à rede, composta pela eNodeB. Essa camada é mais conhecida como ERB. Além disso, existe o controlador da rede, responsável pelo gerenciamento, controle e acesso à rede, o *Evolved Packet Core* (EPC). E finalmente a camada de serviços, responsável por conectar o LTE à rede externa da internet.

A figura 2.2 apresenta os componentes da rede LTE segregada nas principais camadas, como: a camada do usuário onde figuram os dispositivos de acesso à rede, a camada de interface aérea a qual é composta pela RAN, controlador da rede a qual é composta pelo EPC, e a interface externa da rede com a internet, composta pelo IP Multimidia Subsystem (IMS).

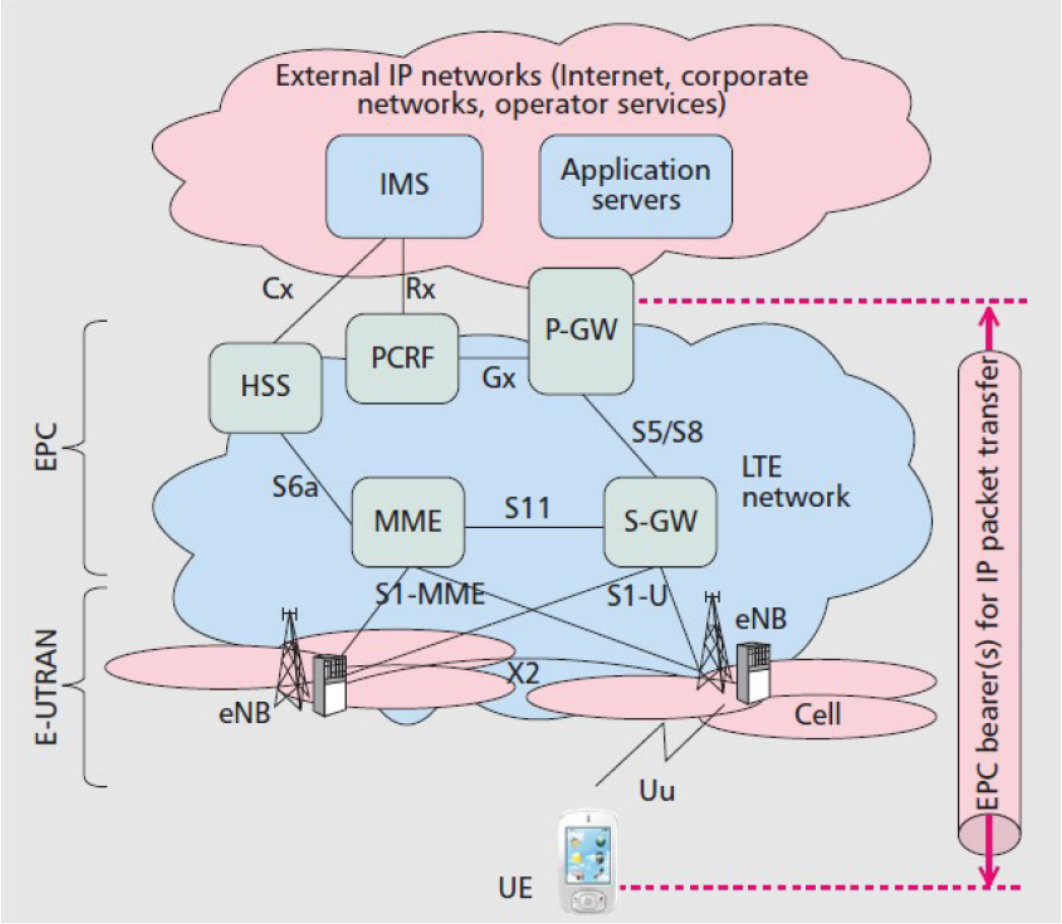

Figura 2.2: Arquitetura de alto nível do LTE
Fonte: [2]

2.3.1 *User Equipment* (UE)

O *User Equipment* (UE) (Equipamento do Usuário): É o hospedeiro móvel onde roda a aplicação dos serviços de internet. É o dispositivo final de uma rede de comunicações, conectando os diversos usuários possibilitando a comunicações de voz e dados. Esses dispositivos podem ser telefones portáteis, *smartphones*, *laptop* entre outros. Particularmente os dispositivos celulares são dotados de um mecanismo de segurança chamado de *SIM card*.

2.3.2 *Evolved UMTS Terrestrial Radio Access Network* (E-UTRAN)

A *Evolved UMTS Terrestrial Radio Access Network* (E-UTRAN): É o elemento com a função de ligação do enlace não guiado entre o equipamento móvel, UE e o núcleo do

sistema LTE. Consiste de um único componente, o eNodeB.

No plano de dados, os eNodeB são responsáveis pela entrega confiável sobre os*links* de Radiofrequência (RF), criptografia de dados de interface de rádio, compressão de cabeçalho e proteção de integridade através da pilha de protocolo de rádio. No plano de controle, os eNodeB são responsáveis pelo gerenciamento de recursos de radiocomunicação.

2.3.3 *Evolved Packet Core* (EPC)

EPC: É uma estrutura para fornecer voz e dados convergentes em uma rede 4G LTE, possibilitando o acesso externo à rede mundial de computadores. O EPC utiliza a comutação de pacotes unificando voz e dados em uma arquitetura de protocolos TCP/IP. Ela também é responsável por todas as funções de controle e gerenciamento da rede.

De um modo geral ela é formada por vários elementos, porém os principais são o *Serving Gateway* (S-GW), *Packet Data Network* (PDN), PDN-*gateway* (P-GW). De forma secundária possui também o *Mobile Management Entity* (MME), *Home Subscriber Server* (HSS) responsáveis pelo processo de autenticação e controle de acesso dos hospedeiros móveis ao núcleo da rede.

MME: Faz a gerência dos usuários da rede realizando a autenticação dos mesmos à rede.

S-GW: Permite o roteamento dos hospedeiros à rede de acesso mundial de computadores.

P-GW: Possibilita a conexão de voz e dados entre as redes LTE e as tecnologias de redes IP, tanto 3GPP quanto não 3GPP, garantindo uma boa qualidade de serviço na comunicação entre essas redes.

2.4 Bandas de Frequências para utilização das Forças Armadas no Brasil

Os países têm órgãos reguladores responsáveis por alocar espectro disponível para sistemas comerciais e governamentais, incluindo sistemas de segurança pública. Alguns países decidiram designar um espectro para uso de banda larga na segurança pública. Os EUA e o Canadá designaram 20 MHz no espectro de 700 MHz (Banda 14) para uso de banda larga de segurança pública, a fim de implantar uma Rede de Segurança Pública sendo que 10 MHz são alocados para transmissões de *uplink* e os outros 10 MHz para

comunicações de *downlink* [3]. A Coreia do Sul também alocou 20 MHz em 700 MHz (Banda 28) para sua rede segurança pública LTE. As regras nos países da América do Norte permitem que o tráfego comercial compartilhe o espectro de segurança pública, desde que o tráfego dos Órgãos de Segurança mantenha os direitos de prioridade.

Por outro lado, no Brasil temos o nosso órgão regulador, a Agência Nacional de Telecomunicações (ANATEL), que por meio da Resolução 625 aprova a atribuição, a destinação e o regulamento sobre condições de uso de Radiofrequências na Faixa de 698 MHz a 806 MHz. Ela foi publicada em 2013 e no seu Artigo primeiro, atribuiu a faixa de radiofrequências de 698 MHz a 806 MHz, adicionalmente ao serviço móvel, em caráter primário. No seu artigo 2° destinou a faixa de radiofrequências de 698 MHz a 806 MHz ao Serviço Móvel Pessoal (SMP), ao Serviço de Comunicação Multimídia (SCM) e ao Serviço Telefônico Fixo Comutado (STFC), em caráter primário e no seu artigo 3° destinou a faixa de radiofrequências de 703 MHz a 708 MHz e 758 MHz a 763 MHz adicionalmente ao Serviço Limitado Privado (SLP), em aplicações de segurança pública, defesa nacional e infraestrutura, em caráter primário, alocando assim, 10 MHz na banda 28 para a destinação de Serviço Limitado Privado, sendo a faixa de *uplink* de 703 a 708 MHz e *downlink* 758 a 763 MHz [1].

As FA e os OSP exercem missões de Defesa da Pátria e GLO, e nesse sentido, necessitam que seus sistemas de C2 possuam características de comunicações de missões críticas ou seja, os sistemas necessitam estar em pleno funcionamento em todas as áreas da operação, sem congestionamento de uso pelo usuário, além de operarem sem interrupção no regime de 24/7. Por missão de comunicações críticas entende-se a situação em que a comunicação tem que ser realizada com grande probabilidade de sucesso.

O sucesso dessas operações depende da possibilidade eficiente de comunicação sem fio e troca de dados entre as unidades que operam no campo, utilizando os terminais móveis e portáteis, por meio de um *site*, célula irradiante, e um controlador central.

Nesse sentido, as FA podem utilizar faixas de frequências de uso exclusivo, as quais podem ser utilizadas mediante solicitação a ANATEL que faz a concessão limitada no tempo, geralmente por 10 anos, renováveis por mais 10 anos, e no espaço, delimitando em quais estados será dada a autorização, para as FA.

Cabe salientar que a taxa de ocupação dos sistemas de C2 em comunicações críticas é baixa, porém faz-se necessária a manutenção do sistema com essas características, tendo em vista a necessidade de confiabilidade e de probabilidade de sucesso de realização da ligação.

Por outro lado, as faixas de 700 MHz têm boas características de alcance, além disso, possuem características de propagação superiores, quando comparadas com as outras faixas de frequências para redes 4G e 5G, possibilitando, assim, uma maior cobertura com menos estações-base, reduzindo os custos de implantação. As faixas também garantem um melhor desempenho para comunicações internas, devido às suas boas características de penetração.

A Figura 2.3 apresenta as frequências de *uplink* e *downlink*.

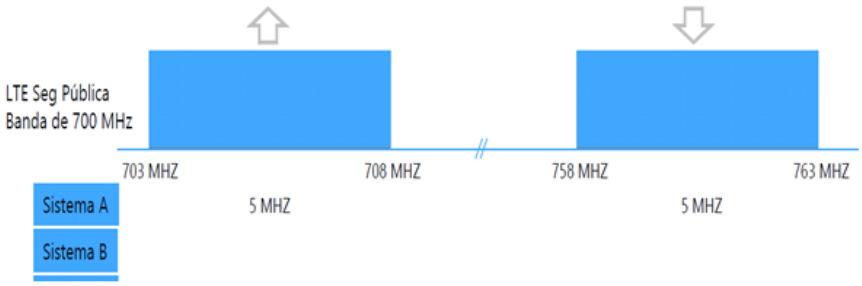

Figura 2.3: Frequências de utilização do LTE
Fonte: Adaptada da Motorola *Solution* (2018)

Assim, as bandas de frequências apresentadas na Figura 2.3, do ponto de vista de eficiência, apresentam as melhores caraterísticas para serem utilizadas por sistemas 4G e, a figura 2.4 apresenta a vantagem da faixa de frequência atribuída ao LTE de Segurança Pública em relação as outras faixas de frequências utilizadas pelo LTE em relação ao alcance.

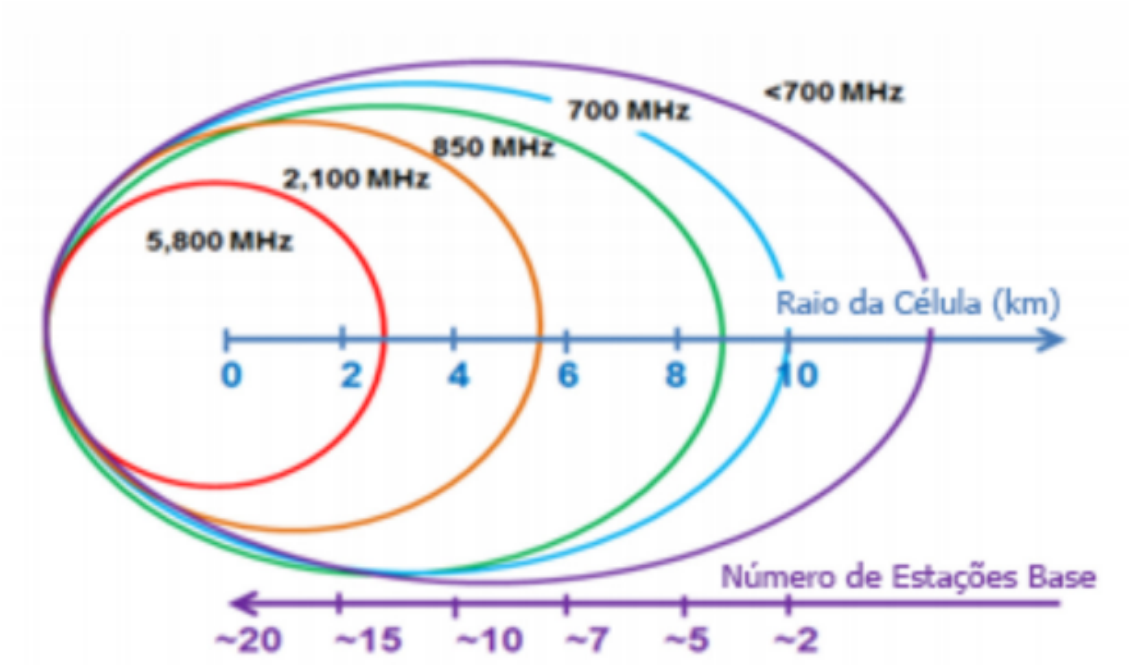

Figura 2.4: Alcance das frequências para o LTE
Fonte: [4]

Dessa forma, com a canalização de 5+5 MHz, o 4G LTE proporciona consideráveis taxa de dados; ou seja, 7,5 Mbps e 24 Mbps, respectivamente, por setor, totalizando 100 Mbps [5].

Por outro lado, a rede LTE pode cobrir uma área em média de 100 km^2, com um raio de cobertura de, em média, 4 km.

2.5 Redes de segurança Pública e Forças Armadas Atuais *Land Mobile Radio* (LMR) (P25, TETRA e TETRAPOL)

Os Órgãos Defesa Nacional e de Segurança Pública são órgãos responsáveis por criar ambientes seguros e estáveis para a execução de operações de missão crítica, como uma resposta para possíveis situações desastrosas que são causadas por natureza ou por atividades humanas. Esses serviços incluem legislação, fiscalização, operações policiais, com-

bate a incêndios, resposta médica de emergência, segurança de fronteiras, recuperação de desastres, operações de garantia da lei e da ordem, dentre outras [6].

Os *Land Mobile Radio System* (LMRS) são sistemas que consistem em equipamentos portáteis, fixos e móveis de usuário, estações repetidoras, um controlador central e um despachante [7]. As redes LMR fornecem aplicações básicas em voz, no entanto, têm baixas taxas de dados [8]. Esses sistemas fornecem comunicações para as operações dos órgãos de defesa nacional e segurança pública. Esses sistemas são subdivididos em três tipos de tecnologias básicas. A saber; o APCO-25, o TETRA e o TETRAPOL.

Todos os três padrões têm como característica geral a arquitetura de uma ERB repetidora, um *site* de controle e um *site* de gerenciamento. Além disso, todos esses sistemas são padrões de rádio digital troncalizados, ou seja possuem um canal de controle para gerenciar dinamicamente o recurso e distribuição dos canais aos usuários.

2.5.1 Padrão TETRAPOL

Esse padrão de rádio digital troncalizado LMR é um padrão de arquitetura fechada com surgimento na França e larga utilização na Europa. A organização desenvolvedora dessa técnologia é *Airbus Defence and Space*.

Como tecnologia de acesso ao canal, ele utiliza o FDMA, o que possibilita a divisão lógica do canal em canais de 12,5 KHz. Nesse sentido, esse padrão pode suportar a taxa de dados de no máximo 8 Kbps, possibilitando assim, somente os serviços de voz e baixa taxas de dados para as comunicações críticas. Ele utiliza a *Gaussian Minimum Shift Keying* (GMSK). O TETRAPOL pode ser utilizado nas frequências de *Very High Frequency* (VHF), *Ultra High Frequency* (UHF) e 800 MHz. No Brasil o padrão TETRAPOL é adotado, principalmente, pela PF.

2.5.2 Padrão APCO25

Esse padrão de rádio digital troncalizado LMR é um padrão de arquitetura aberta com surgimento e utilização nos EUA e a organização desenvolvedora dessa tecnologia é a *Telecommunications Industries Association* (TIA). Como tecnologia de acesso ao canal ele utiliza o FDMA na fase 1 e o TDMA na fase 2, o que possibilita a divisão lógica do canal em canais de 12,5 e 6,25 KHz, respectivamente. Nesse sentido, esse padrão pode suportar a taxa de dados de, no máximo, 9,6 Kbps, possibilitando assim, somente os serviços de voz e baixa taxa de dados para as comunicações críticas. Ele utiliza a modulação *Compatible 4-Level Frequency Modulation* (C4FM). O P25 pode ser utilizado nas frequências de VHF,

UHF, 700, 800 ou 900 MHz. No Brasil o padrão APCO25 é adotado, principalmente, pelas FA e pela Polícia Militar do estado de São Paulo.

2.5.3 PADRÃO TETRA

Esse padrão de rádio digital troncalizado LMR é um padrão de arquitetura aberta com surgimento e utilização na Europa. A organização desenvolvedora dessa tecnologia é *European Telecommunications Standards Institute* (ETSI). Como tecnologia de acesso ao canal ele utiliza o TDMA, o que possibilita a divisão lógica do canal em canais de 25 KHz. Nesse sentido, esse padrão pode suportar a taxa de dados de, no máximo, 28,8 Kbps, possibilitando assim, somente os serviços de voz e baixa taxas de dados para as comunicações críticas, porém com maior capacidade de dados que o TETRAPOL e o P25. Ele utiliza a modulação *Differential Quadrature Phase-Shift Keying* (DQPSK). O TETRA pode ser utilizado nas frequências de VHF, UHF ou 800 MHz. No Brasil o padrão TETRA é adotado, principalmente, pela PRF.

Em resumo essas tecnologias de comunicação podem ser classificadas, com base em suas taxas de dados suportadas, em três categorias: *Narrowband* (NB) (Banda estreita), *Wideband* (WB) (Banda Larga e *Broadband* (BB) (Banda Larga). As tecnologias NB têm taxas de dados em torno de algumas dezenas de Kbps, e são adequadas para aplicações centradas em voz. TETRA e P25 são classificadas nesta categoria. As tecnologias WB suportam aplicativos com taxas de dados em torno de várias centenas de Kbps na qual enquadramos o LTE. Nesse sentido, as tecnologias NB e WB fornecem apenas os serviços de voz, dados, e envio de posicionamento por meio de *Global Positioning System* (GPS) [9].

Os serviços de voz incluem chamadas *full-duplex* de alta qualidade, *Push-To-Talk* (PTT) *half-duplex*, chamadas em grupo, chamadas um-para-um, chamadas um-para-muitos, chamadas de emergência e escuta ambiente. Os serviços de dados incluem mensagens, redes de sensores sem fio, leitura de mapas, *Real-time locating system* (RTLS) (sistemas de localização em tempo real), serviços de rastreamento, navegação na *Web*, acesso a servidores e leituras biométricas.

Entre os serviços de voz destacamos:

- Chamadas *Full Duplex* ;
- Chamadas *Half-Duplex*;
- Chamadas em Grupo; e

- Chamadas de Emergência;

Atualmente, existe a demanda crescente por serviços de sistemas em banda larga, como compartilhamento de multimídia, chamadas de vídeo e *streaming* de vídeo ao vivo. Esses serviços desempenham um papel importante para que mais operações sejam concluídas com sucesso. Ao analisarmos a resiliência dos sistemas LMR verificamos que possuem três níveis de redundância na utilização da rede, com capacidades decrescentes do ponto de vista de limitação do número de usuários:

- Modo troncalizado: Nesse modo os sistemas operam com toda a sua capacidade utilizando o canal de controle para gerenciar os recursos de acesso a rede;
- Modo repetidora: Nesse modo o sistema opera como repetidoras convencionais sem o gerenciamento dos recursos alocados;
- Modo direto: Nesse modo a comunicação é de equipamento rádio para equipamento rádio.

Os padrões TETRA, TETRAPOL e P25 atendem perfeitamente a demanda de voz requerida para as missões críticas, porém não atendem a demanda de alta taxa de dados de banda larga [10].

Por outro lado, o LTE devido ao grande avanço atual e padronização para atendimento aos requisitos de comunicações críticas é considerado como um candidato promissor para atender as demandas de banda larga para os FA em operações de missões críticas.

2.6 Conclusão

Neste capítulo foram apresentadas as revisões bibliográficas da tecnologia que foi investigada, começando por sua evolução até os dias de hoje. Apresentamos também as suas características e arquitetura na qual verificamos todos os componentes do sistema e suas aplicações. Analisamos também a banda de frequências utilizadas pelas FA, assim como sua aplicação no contexto de utilização para missões críticas e disponibilidade.

De forma complementar, foram apresentados os sistemas de comunicações críticas das FA e dos OSP (LMR), suas características, e além disso, foi apresentada a falta de padronização no que diz respeito às diversas tecnologias LMR (TETRA, TETRAPOL e P25)

Por fim, os conceitos tratados neste capítulo servem de fundamento teórico para o perfeito entendimento do desenvolvimento desse trabalho que seguirá no próximo capítulo.

3 Os sistemas de comunicações críticos dos Órgãos de Defesa aplicados à Rede 4G LTE

3.1 Serviços de uma rede de banda larga LTE

A rede de banda larga 4G LTE pode fornecer serviços de multimídia que utilizam os protocolos das comunicações da pilha TCP/IP. Nesse sentido, pode fornecer diversos serviços tanto com necessidade de baixíssima taxa de dados, quanto com serviços de necessidade de altas taxas de dados.

Nesse sentido, essa rede pode prover serviços de banda larga para voz [11], assim como serviços de protocolos IP [12]. Dessa forma, a rede de banda larga está apta para fornecer quaisquer tipos de serviços que possam ser utilizados nos sistemas de comunicações críticas. Dentre os principais serviços destacamos os serviços de voz, os serviços de dados e os serviços de multimídia.

- Serviços de voz:
  - chamadas *full-Duplex* de alta qualidade;
  - PTT;
  - *Half-Duplex*;
  - Chamadas em grupo;
  - Chamadas um-para-um; e
  - Chamadas de emergência e escuta.
- Serviços de dados:
  - Mensagens;
  - Redes de sensores sem fio;

  - Sistemas de localização em tempo real;
  - Rastreamento e monitoramento;
  - Acesso a servidores para informações; e
  - Leituras biométricas.

- Serviços de multimídia:
  - Compartilhamento de imagens;
  - Compartilhamento de vídeos;
  - Reconhecimento facial;
  - Serviços de aplicativos;
  - Videoconferências em tempo real; e
  - Envio e recebimento de arquivos robustos.

O LTE fornece uma arquitetura de sistema plana totalmente IP com baixa latência de interface aérea que melhorará o desempenho do sistema. Além disso, os sistemas LTE funcionam em diferentes frequências de portadoras, o que reflete sua flexibilidade regional e sua potencial interoperabilidade. A interoperabilidade é importante para facilitar o suporte de vários fornecedores de equipamentos LTE e melhorar a capacidade de acessar redes estrangeiras como entidade visitante. Os sistemas LTE são altamente escaláveis e capazes de suportar um grande número de usuários [11], e além disso, eles são flexíveis em termos de implantação de rede e tamanho de célula, o que permite a cobertura de áreas geográficas pequenas ou grandes.

O LTE pode oferecer ainda serviços de priorização dinâmica de usuários, uma funcionalidade muito útil para aplicação de multiusuários, conforme apresentado na Figura 3.1 que ilustra a forma de priorização de usuários, realizada na camada de aplicação, em um ambiente de operação de multi-agências. Essa priorização pode garantir níveis de acesso baseados na prioridade de importância das autoridades. Existem diversos níveis de prioridade a serem utilizados, conforme a especificidade da operação. Na figura em questão, são apresentados os exemplos de níveis de prioridade geográfico, organizacional, jurisdicional, funcional, individual, incidental e os relativos aos tipos de serviços.

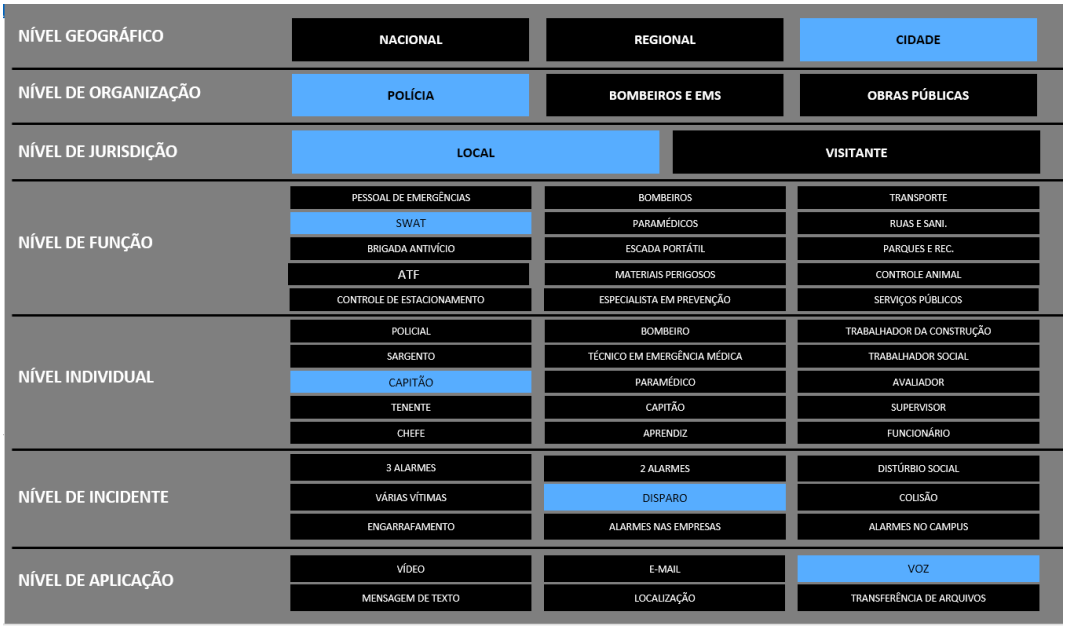

Figura 3.1: Priorização dinâmica do usuário no nível da aplicação
Fonte: Adaptada da Motorola *Solution* (2018)

3.2 Comparações entre LTE e LMR

No contexto de análise da possibilidade de utilização da rede de banda larga para a segurança pública é importante salientar as diferenças dessas duas tecnologias em termos de aplicação funcional [12].

Nesse sentido, foi realizada uma análise dessas tecnologias, dentre as quais destacam-se:

3.2.1 Tipos de serviços:

O uso da tecnologia LTE em redes das FA e segurança pública oferece muitas vantagens sobre as tecnologias LMR. Para começar, a tecnologia LTE é capaz de executar serviços de emergência de banda larga que demandam compartilhamento de fotos, arquivos e vídeos [13]. A adoção do LTE para Rede de banda larga para as FA e segurança pública abrirá as portas para novos aplicativos, como *streaming* de vídeo ao vivo, videoconferência, detecção de campo, rastreamento e muitos outros serviços que não são atingíveis pelos atuais LMR.

3.2.2 Implantação de Infraestrutura:

A tecnologia LTE oferece vantagem econômica em termos de custos de infraestrutura (*Capital Expenditure* (CAPEX)) e custos operacionais (*Operational Expenditure* (OPEX)) [14]. O mercado de LTE, em comparação com outros mercados de sistemas LMR com poucos fornecedores, e o suporte de vários fornecedores e operadoras da tecnologia LTE torna possível reduzir o custo de implantação efetiva [11]. Além disso, existem mais de trezentas redes LTE que estão atualmente implantadas em todo o mundo. Portanto, é fácil construir uma rede de banda larga para as FA e a segurança pública interoperáveis em muitos países usando sistemas LTE [15]. Nos sistemas LMR, a interoperabilidade é um problema, pois os equipamentos TETRA não funcionam em redes P25 e vice-versa.

3.2.3 Segurança Cibernética:

O domínio de segurança das redes LTE é muito ativo. Em termos de segurança, os sistemas LTE estão expostos a muitas ameaças, como roubo de identidade, exposição à privacidade, ameaça de rastreamento de IP, o que leva à exposição da localização, transmissão/*multicast* de ameaças de informações falsas, ataques de *Denial of Service* (DoS), ataques físicos na base estações e ataques de protocolo na rede de acesso de rádio [16]. No entanto, muitos especialistas estão trabalhando no fortalecimento de todos os aspectos de segurança, fechando as *backdoors* e interrompendo possíveis violações.

3.2.4 Atualização de aplicativos:

Os protocolos de segurança LTE são atualizados regularmente para manter sua imunidade contra ataques novos e existentes.

3.2.5 Interoperabilidade com outras redes IP comerciais:

A infraestrutura e o compartilhamento de espectro entre redes comerciais LTE, redes das FA e OSP fornecerão sistemas de gerenciamento de emergência eficazes e confiáveis. Isso afetará o número de profissionais de segurança pública que pode ser implantado rapidamente em um período curto, além de ser uma solução economicamente ótima para o provisionamento de serviços BB em rede de banda larga para a segurança pública através da utilização de sistemas de segurança pública híbridos onde os serviços são prestados por meio de redes dedicadas e comerciais.

3.2.6 Integração com redes comerciais 2G, 3G e as futuras 5G:

A rede de banda larga LTE permite integração com todas as redes comerciais, integração de voz e dados, independente da geração da tecnologia. Por outro lado, a interoperabilidade com as redes LMR só pode ser realizada por voz e com a utilização de um integrador. No caso das FA é possível integrar as redes 4G por meio do servidor *wave* e seus aplicativos.

3.2.7 Rede heterogênica com variedade e diversidade no tamanho de células:

Os sistemas LTE são altamente escaláveis, pois um grande número de usuários distribuídos pode se comunicar de forma eficiente. São, também, flexíveis em termos de tamanho de célula, podendo ser macrocélulas, microcélulas, picocélulas e femto-células.

3.2.8 Redes Heterogêneas:

Uma rede LTE é chamada de *Heteregeneous network* (HetNet) por compreender diferentes tipos de estações base (pontos de acesso). Por exemplo, estações base de macrocélulas, microcélulas, picocélulas e femto-células. Esta nova tecnologia é baseada em ter células pequenas, implantando estações base de baixo consumo de energia, curto alcance e baixo custo sob a área de cobertura das macrocélulas [17]. O HetNet tem como objetivo aproximar os pontos de acesso LTE dos usuários finais para melhorar o desempenho em termos de capacidade, cobertura e atrasos.

Isso pode ser utilizado em uma situação onde o aumento da capacidade da rede for um requisito. Neste caso, as áreas de cobertura fornecidas por células pequenas podem se sobrepor a uma cobertura de macrocélulas ou à cobertura de outras células pequenas. Assim, a tecnologia de HetNet pode ser considerada como uma solução para fazer *backup* ou compensar qualquer possível escassez no domínio da infraestrutura. As células pequenas podem ser implantadas em locais de desastres sem planejamento prévio para fornecer cobertura ou aumentar a capacidade do sistema.

3.2.9 Gerenciamento dinâmico de prioridades:

O conceito de *Quality of Service* (QoS) (Qualidade de Serviço) e o gerenciamento de prioridades inerentes aos sistemas LTE são benéficos no domínio das redes de banda larga para a segurança pública. Como conclusão, os mecanismos de QoS aplicados nos sistemas LTE são adequados para a transferência de dados de missão crítica em rede de

banda larga para as FA e a segurança pública, especialmente durante operações críticas e tempos de congestionamento. Há uma variedade de serviços *Public Protection & Disaster Relief* (PPDR) que podem ser facilitados por meio de sistemas LTE, incluindo aqueles que exigem conectividade IP entre clientes e servidores, que podem ser tratados com eficiência por esta conectividade básica fornecida pelas redes LTE.

3.2.10 Dispositivos do usuário:

O LTE utiliza UE, como *smartphones, tablet* e*notebook* utilizados de forma comercial sem a necessidade de resistência específicas, possibilitando o acesso à rede por meio de aparelhos celulares comerciais de baixo custo. Por outro lado, os terminais das redes LMR são proprietários de cada tecnologia e fabricante ao custo de, por exemplo, um terminal APX do APCO25 da Motorola.

3.2.11 Resiliência na utilização:

Os sistemas LMR operam em três níveis de resiliência. O primeiro é o nível *Trunking Mode Operation* (TMO). Neste modo, o sistema funciona como um sistema digital troncalizado em que um dos canais é usado como canal de controle. O segundo é o nível *Independent Digital Repeate* (IDR). Neste nível, a rede funciona com repetidoras convencionais sem a utilização de um canal de controle, e no terceiro nível, o *Direct Mode Operation* (DMO), onde o sistema funciona com a comunicação direta sem passar por repetidoras de terminal para terminal. Por outro lado, a rede LTE só consegue operar com todos os ativos funcionando, ou seja, com a E-UTRAN conectada ao EPC [18]. Esse nível de resiliência é semelhante à operação TMO do LMR. Nesse contexto, a rede LTE possui resiliência muito menor do que as redes LMR. De outra forma, estudos apontam a possibilidade de utilização futura de comunicações dispositivo a dispositivo, das redes LTE o que aumentaria seu nível de resiliência. Essa funcionalidade de voz de modo direto é conhecida como serviços de proximidade LTE *Proximity Services* (ProSe). Esse serviço ProSe, é uma tecnologia promissora para tornar a tecnologia LTE extremamente útil para as redes de comunicações críticas.

3.2.12 Número de fornecedores da tecnologia:

Pelo fato do protocolo ser aberto, existem muitos fabricantes que podem fornecer os ativos da rede de banda larga, não ficando na dependência de empresas específicas como, por exemplo, os ativos do sistema LMR P25 da Motorola , que não são interoperáveis com os de outros fabricantes.

3.2.13 Células especiais pessoais e aéreas:

Uma possibilidade de utilização de Células Pessoais Móveis, Estações Base Aéreas como mecanismo promissor para redes rápidas de emergência é o uso de eNodeB aéreos [19]. Os eNodeB aéreos implantados podem ser de diferentes tipos, capazes de voar em diferentes altitudes. Portanto, formam células com raio de cobertura variável [20]. Semelhante ao conceito de HetNet, esta arquitetura é referida como *Aerial Heterogeneous Networks* (AeHetNets) [21].

3.2.14 Faixas de frequência com serviços de uso comercial:

A faixa de frequência na qual opera o LTE apresenta uma série de serviços que podem ter exploração comercial. Essa característica faz com que os serviços praticados com a rede de banda larga possam ser disponibilizados também para uso comercial.

3.2.15 Função *PTT*:

Nas redes LMR essa função é realizada por meio do botão PTT. Isso faz com que a comunicação de voz seja bem mais dinâmica e rápida pois a comunicação acontece de forma instantânea. Por outro lado, nas redes de banda larga LTE, essa função é implementada com *Voice over Internet Protocol* (VoIP) [22] e por meio de aplicativos como os da *Open Mobile Alliance* (OMA) sobre celular e no Brasil o aplicativo *wave*.

3.2.16 Possibilidade de utilização como banda estreita LMR:

O LTE pode ser usado como LMR desde que estejam implementadas as funcionalidades de ProSe para comunicação dispositivo a dispositivo sem passar pelo núcleo da rede, serviços de voz PTT com baixa latência e comunicações em grupo *Group Communication System Enabler* (GCSE).

3.2.17 Possibilidade de utilização como banda larga LTE:

O LMR não pode fornecer serviços de banda larga que as redes LTE podem fornecer.

3.2.18 Capacidade de Integração:

A rede LTE, por ser uma rede IP, possibilita integração com redes 3GPP e não 3GPP [23]. Essa tecnologia permite a integração e interoperabilidade entre os OSP e as FA, com o compartilhamento da estrutura física porém com a separação lógica, o que permite a segregação dessas redes.

3.3 Aplicação operacional prática dos projetos do Exército Brasileiro com a tecnologia LTE (CCOp Mv, COBRA e SCCFTer)

O EB para cumprir as missões constitucionais de Defesa Nacional e GLO necessita de sistemas de comunicações que possam prover as ligações e fornecer infraestruturas necessárias para as atividades de C2 em todos os escalões de atuação nas mais diversas atividades.

Nesse sentido, a Estratégia Nacional de Defesa (END) tem a previsão de diversos projetos com a finalidade de atender as necessidades operacionais de C2, principalmente no que diz respeito às demandas de sistemas de comunicações para prover serviços de voz, dados e multimídia.

Nesse contexto, a tecnologia de banda larga LTE é muito promissora, pois pode atender as demandas dos serviços de voz, dados e multimídia. Assim, o presente capítulo analisará a aplicação dessa tecnologia em diversos projetos do EB.

3.3.1 Centro de Coordenação de Operações Móvel (CCOp Mv)

O CCOp Mv é um sistema que possibilita aos decisores, em diversos escalões, a possibilidade de consciência situacional para exercer de forma efetiva o C2. Para essa finalidade ele se utiliza de diversos tipos de equipamentos que provêm os meios necessários para a tomada de decisão. Meios esses denominados de Tecnologia de Informação e Comunicações (TIC) [24].

CCOp Mv é um Centro de C2 configurado para apoiar, com recursos de C2, um Grande Comando Operacional em situações de guerra e não guerra, possibilitando apoio em sistemas, equipamentos, *softwares* e acesso a sistemas táticos e estratégicos [25]. O CCOp Mv será composto por um Conjunto de Coordenação das Operações (cinco Viatura militar (Vtr) de 5 toneladas (Ton) e por Nós de Acesso (8 Vtr $2^1/^2$ Ton).

O CCOp Mv empregará tecnologia de rede de acesso de longa distância de 4G LTE; equipamentos transceptores de curta, média e longa distâncias com diversas capacidades de dados; equipamentos típicos de uma rede de protocolos TCP/IP, enlaces guiados e não guiados. Os não guiados englobam comunicações por satélite e enlaces de micro-ondas.

O CCOp Mv tem como composição:

1. Conjunto de Coordenação das Operações.

2. Nós de Acesso.

- Conjunto de Coordenação das Operações.
  (a) Módulo de Gerenciamento das Comunicações.
  (b) Posto de Comando (PC).
  (c) Módulos de Trabalho:
    – de Estado-Maior;
    – de células segregadas; e
    – de Ambiente de Cooperação e/ou Coordenação com Agências.

A sua arquitetura é apresentada na Figura 3.2, que apresenta a composição do CCOp Mv. Do ponto de vista da análise da arquitetura da pilha de protocolos TCP/IP. O nó de acesso é a cabine que possui os enlaces de comunicações integrados por meio de um integrador de voz e dados, possuindo também a funcionalidade de prover cobertura *wi-fi* e LTE para os agentes civis e militares. O módulo de gerenciamento de comunicações que faz a gerência, configuração e manutenção da rede, é o *Network Operation Center* (NOC) do CCOp Mv. O PC, que possui toda a infraestrutura de TIC para prover os serviços necessários ao C2. É no PC que estão todos os servidores de aplicação, e os módulos de trabalho que são responsáveis por proporcionar aos agentes civis e militares as condições necessárias de acomodação e serviços necessários para a realização das tarefas específicas de coordenação das atividades.

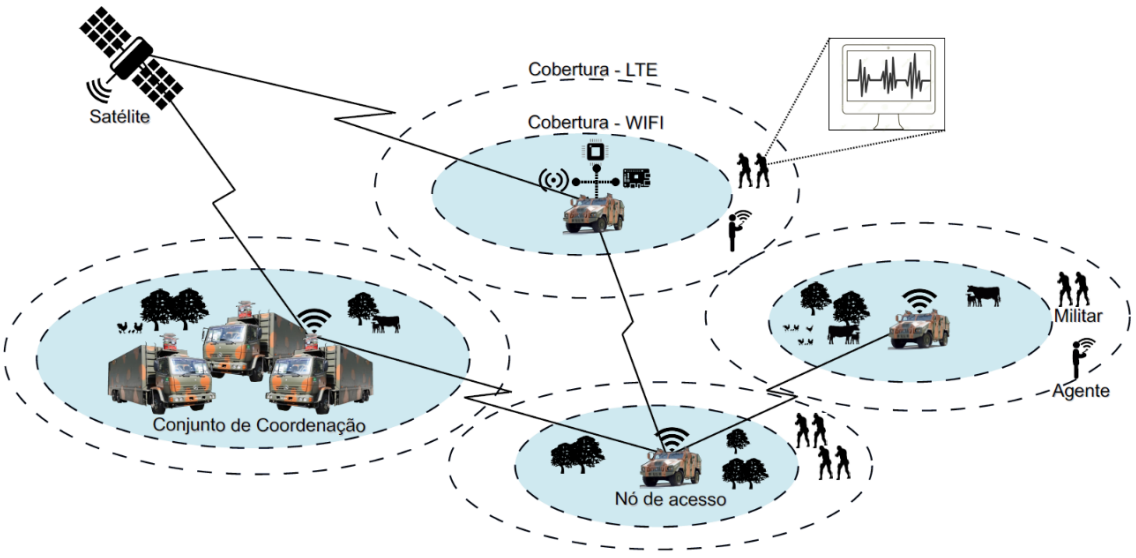

Figura 3.2: Arquitetura CCOp Mv
Fonte: [26]

O uso da tecnologia de banda larga LTE irá prover os serviços mencionados anteriormente de voz, dados e multimídia. Mesmo que operando de forma isolada, sem possibilidade de acesso a rede de computadores mundiais, o LTE pode prover, localmente, todos os serviços previstos em instalações fixas que possuam toda a infraestrutura de acesso à internet.

A Figura 3.3 apresenta a estrutura de TIC instalada nos módulos de trabalho para acompanhamento em tempo real das operações.

Como um dos serviços principais destacamos o fornecimento de uma intranet, que é uma rede interna. Neste tipo de rede, o acesso aos serviços é condicionado aos servidores de aplicações locais conectados física e logicamente ao EPC, fornecendo localmente serviços como Sistema de Protocolo Eletrônico de Documentos (SPED), pacificador *mobile*, entre outras aplicações hospedadas nos servidores locais. Nesse contexto, a conexão entre os *host* com o EPC acontece por meio não guiado, proporcionando assim alta mobilidade entre esses dispositivos. Em princípio, nos servidores disponibilizados hospedamos os seguintes serviços: Rede Corporativa de Comunicações do Exército (EBNet), Família de Aplicativos de Comando e Controle da Força Terrestre (FAC2FTer), VoIP, SPED, entre outros serviços de protocolo TCP/IP.

Figura 3.3: Gerenciamento de operações

3.3.2 Combatente Brasileiro (COBRA)

O Projeto COBRA 2020, é um projeto que visa modernizar os equipamentos de utilização do combatente individual para que ele possa atuar com eficiência nos diversos cenários de atuação. Nesse contexto, ele necessita ser dotado de diversos tipos de funcionalidades essenciais para estar apto a cumprir diversas missões de combate em diversos ambientes operacionais. As funcionalidades essenciais são citadas abaixo:

a) letalidade

b) sobrevivência

c) consciência situacional

Especificamente, o 4G LTE, para atender a demanda de consciência situacional, é utilizado de duas formas, para prover comunicações típicas de telefonia celular entre os integrantes da fração espalhada no terreno e para prover rede de acesso aos integrantes da fração espalhada no terreno, possibilitando acesso à EBNet.

a) Fornecimento de serviços entre os combatentes no terreno: Serviços de aplicações de voz individual ou em grupo, videoconferências, vídeos em tempo real,individual ou em grupo, troca de dados individuais e utilização de aplicativos de C2, dentre outras demandas nas quais temos tecnologia *IP*. Esses serviços de comunicações entre os combatentes no terreno acontece por meio de cobertura de células veiculares ou portáteis, quando utilizadas em áreas sem nenhuma infraestrutura de rede 4G pública ou quando se deseja manter uma estrutura 4G privada do EB.

b) Rede de acesso a longa distância: Serviços que possibilitam o acesso dos terminais LTE à EBNet possibilitando que as informações possam chegar nos locais onde as autoridades necessitem avaliar as informações para tomada de decisões. A Figura 3.4 apresenta a utilização do hospedeiro móvel (*smartphone*) no qual roda aplicação de consciência situacional com o objetivo de prover C2 para os militares integrantes da patrulha.

Figura 3.4: Utilização do sistema LTE pelo COBRA

3.3.3 Sistema de Comando e Controle da Força Terrestre (SC-CFTer)

Esse sistema define toda a infraestrutura composta por equipamentos de enlace, redes e aplicação necessários para a realização de C2 nos diversos escalões de atuação que necessitem de consciência situacional.

Nesse sentido ele define os sistemas de C2 de cada escalão operacional do EB, visando atender a demanda de C2 e consciência situacional de cada nível.

SCCFTer no Corpo de Exército

Utilização do LTE como Sistema do Assinante Móvel (SAM) de dados podendo fornecer os mesmos serviços do CCOp Mv. Provendo para a áreas do PC do Corpo de Exército os serviços de acesso à EBNet, FAC2FTer, fornecendo todos os tipos de serviços aplicáveis com tecnologia da pilha de protocolos TCP/IP. Podendo esses serviços serem prestados por meio da INTRANET, desde que se tenham os servidores locais hospedando as aplicações e conectados física e logicamente ao EPC.

A Figura 3.5 apresenta o LTE com a funcionalidade de SAM de banda larga, fornecendo as funcionalidades dos serviços da pilha de protocolo TCP/IP para as autoridades ocupantes da área do PC do EB.

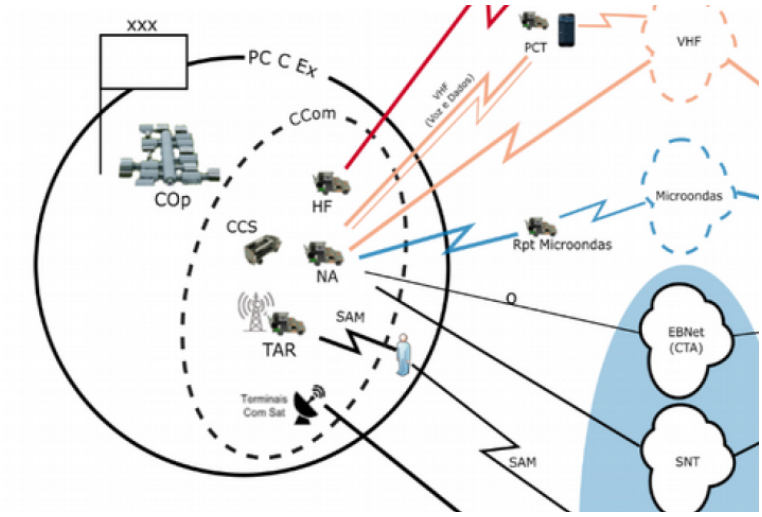

Figura 3.5: LTE no Corpo de Exército

SCCFTer na Divisão de Exército

Utilização do LTE como SAM de dados podendo fornecer os mesmos serviços do CCOp Mv, provendo para a áreas do PC da DE os serviços de acesso à EBNet, FAC2FTer, fornecendo todos os tipos de serviços aplicáveis com tecnologia da pilha de protocolos TCP/IP. Podendo esses serviços serem prestados por meio de INTRANET, desde que se tenha os servidores locais hospedando as aplicações conectados física e logicamente ao EPC.

A Figura 3.6 apresenta o LTE com a funcionalidade de SAM de banda larga, fornecendo as funcionalidades dos serviços da pilha de protocolo TCP/IP para as autoridades ocupantes da área da DE.

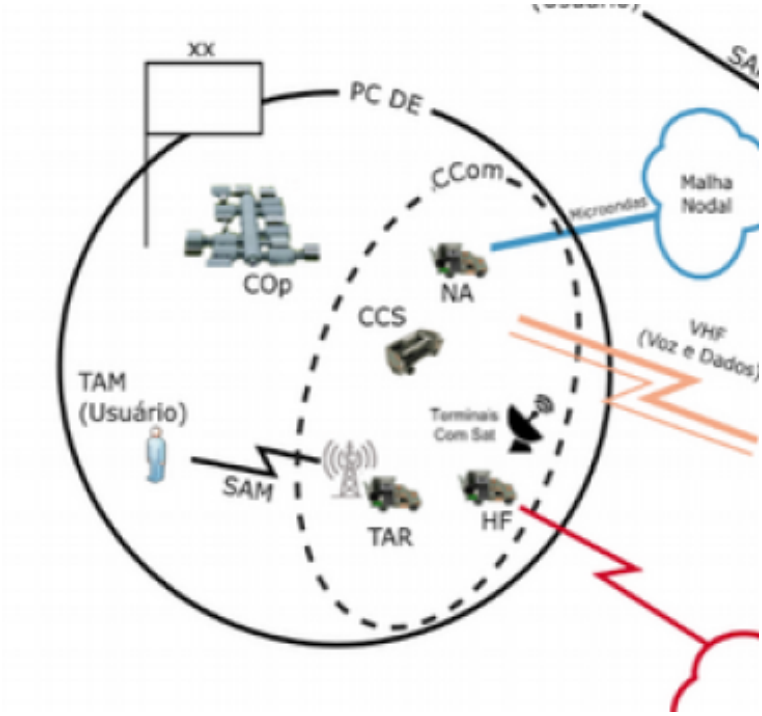

Figura 3.6: LTE na DE

SCCFTer na Brigada

Utilização do LTE como SAM de dados podendo fornecer os mesmos serviços do CCOp Mv, provendo para as áreas do PC na Brigada, os serviços de acesso à EBNet, FAC2FTer, fornecendo todos os tipos de serviços aplicáveis com tecnologia da pilha de protocolos TCP/IP. Podendo esses serviços serem prestados por meio de INTRANET, desde que se tenha os servidores locais hospedando as aplicações conectados física e logicamente ao EPC.

A Figura 3.7 apresenta o LTE com a funcionalidade de SAM de banda larga, fornecendo as funcionalidades dos serviços da pilha de protocolo TCP/IP para as autoridades ocupantes da área da Brigada.

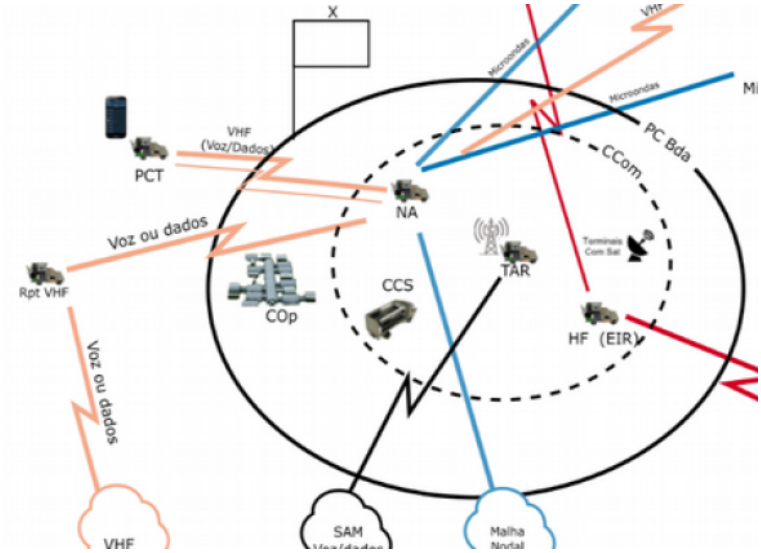

Figura 3.7: LTE na Brigada

SCCFTer nas Unidades e Subunidades Independentes

Utilização do LTE como SAM de dados podendo fornecer os mesmos serviços do CCOp Mv, provendo para as áreas do PC das Unidades e Subunidades Independentes os serviços de acesso à EBNet, FAC2FTer, fornecendo todos os tipos de serviços aplicáveis com tecnologia da pilha de protocolos TCP/IP. Podendo esses serviços serem prestados por meio de INTRANET, desde que se tenha os servidores locais hospedando as aplicações conectados física e logicamente ao EPC.

A Figura 3.8 apresenta o LTE com a funcionalidade de SAM de banda larga, fornecendo as funcionalidades dos serviços da pilha de protocolo TCP/IP para as autoridades ocupantes da área da Unidade.

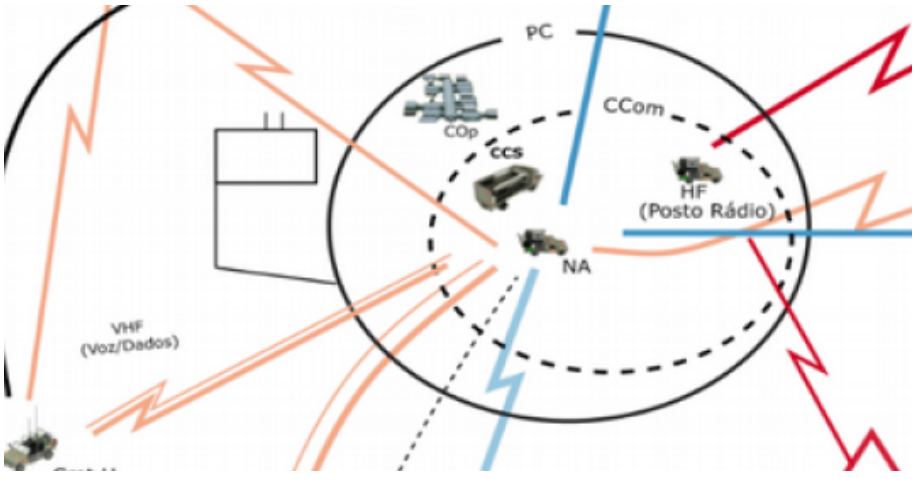

Figura 3.8: LTE na Unidade

3.3.4 O Sistema Tático de Comunicações (SISTAC)

O Sistema Tático de Comunicações (SISTAC) é um sistema que tem como objetivo prover diversos tipos de enlaces de comunicações, tanto por voz quanto por dados de baixa e de alta capacidade. Além dos enlaces, esse sistema provê todas as funcionalidade previstas no protocolo de camadas da pilha TCP/IP por meio de roteadores *switches*, hospedeiros e aplicação de consciência operacional [27]. Para atender a demanda de C2 de uma DE, o SISTAC possui constituição celular, abrangendo a área de atuação de uma DE.

O sistema permite a interligação entre os elementos vizinhos, elemento apoiado e elemento apoiador. Além disso, o sistema deve integrar-se a diversos tipos de enlaces, tanto do tipo guiados como fibra ópticas cabo ethernet entre outros, quanto do tipo não guiados, como*links* de canais de rádio por satélites,*links* de canais de rádio terrestre micro-ondas e*links* de telefonia 4G LTE.

Podemos dividir a estrutura da rede do SISTAC de acordo com os elementos do núcleo da rede, os elementos da periferia da rede e os elementos de gerenciamento da rede.

- Núcleo da rede: Nesse elemento encontramos o Centros Nodais (CN), que é uma cabine responsável pela realização do*link*de rede que é o*link*que implementa a malha de dados da alta capacidade no interior da rede. O CN é dotado de diversos tipos de equipamentos como rádios táticos para comunicações de voz e de baixa, média e alta capacidade de dados. Além disso o CN deve permitir o acesso por sistema de assinante móvel de alta capacidade por meio do 4G LTE, o qual fornece serviços de banda larga móvel e rede de acesso de longa distância à rede mundial de computadores. Especificamente, por ocupar o núcleo da rede, ele necessita de quatro enlaces de rede, que serão realizados por meio de quatro enlaces de rádios micro-ondas.
- Periferia da rede: Nesse elemento encontramos os Nós de Acesso (NA), que são cabines responsáveis pela realização do*link*de junção que é o*link* que implementa a malha de dados da alta capacidade da borda da rede. Os NA são dotados de diversos tipos de equipamentos como rádios táticos para comunicações de voz e de baixa, média e alta capacidade de dados. Além disso os NA devem permitir o acesso por sistema de assinante móvel de alta capacidade por meio do 4G LTE, o qual fornece serviços de banda larga móvel e rede de acesso de longa distância à rede mundial de computadores. Especificamente, por ocupar a periferia da rede, ele necessita de dois enlaces de rede que serão realizados por meio de rádios micro-ondas.
- Gerenciamento da rede: Nesse elemento encontramos toda a parte de gerenciamento, configuração, planejamento e controle da rede. A cabine de gerenciamento é ligada

à rede, normalmente por meio guiado e gerencia os ativos da rede por meio de aplicativos específicos.

Especificamente, o 4G LTE é utilizado nesse sistema com SAM fornecendo os serviços de banda larga móvel. Os serviços são bem semelhantes ao projeto CCOp Mv, não sendo previsto, porém a integração entre agências.

3.4 Conclusão

Neste capítulo foi apresentada a aplicabilidade da tecnologia LTE para FA, essa aplicação foi realizada com base na necessidade de banda larga para as aplicações de multimídia, e serviços de que necessitam de altas taxas de dados e mobilidade. Além disso, foi apresentado os principais serviços requeridos para a aplicação 4G LTE, entre eles citamos como principais as aplicações de C2, gerenciamento dinâmico de operações, integração com o legado LMR, rede de acesso de longa distância em locais isolados sem cobertura celular pública.

Além disso, foi realizada uma comparação entre a tecnologia LTE e LMR para rede de banda larga para a segurança pública com ênfase nos diferentes tipos de serviços, integração com as rede IP, custo de implantação, capilaridade da rede, faixas de frequências de uso comerciais, entre outros.

Foi apresentado, também, as possibilidades de aplicação operacional da tecnologia LTE nos projetos vigentes das FA como por exemplo o CCOp Mv, COBRA, Sistema de Comando e Controle da Força Terrestre (SCCFTer), SISTAC.

Do exposto no capítulo, podemos verificar que existe um grande número de serviços de banda larga de grande interesse dos FA os quais não podem ser fornecidos pela tecnologia LMR. Assim como, na diferença entre as tecnologias LMR e LTE verificou-se que o LTE possui um grande número de funcionalidades, as quais são capazes de atender, parcialmente, as demandas requeridas aos sistemas LMR, e completamente, as demandas de banda larga. Finalizando, verificou-se uma grande aplicabilidade da tecnologia nos projetos do EB, fato esse que justifica investimentos nessa tecnologia para sua utilização.

4 Integração da tecnologia LTE com o LMR

No processo de atualização do sistemas de comunicações críticas para um sistema de banda larga LTE é fundamental a adoção de requisitos de interoperabilidade com o legado LMR objetivando uma convivência harmônica entre esses dois sistemas [28]. Nesse sentido, foram realizados estudos por uma equipe multidisciplinar com o objetivo de verificar os requisitos técnicos que deveriam ser adaptados da tecnologia LTE para atender os requisitos de comunicações críticas, além de verificar as interfaces físicas e lógicas definidas pela 3GPP para essa finalidade.

Nesse contexto, buscou-se a integração e interoperabilidade de três tipos básicos de redes:

- As redes LMR legadas que atendem a todos os requisitos de comunicações críticas, porém com baixa taxa de dados;
- As redes LTE proprietárias das FA e dos OSP [29], que detém a responsabilidade do controle, da gerência, da configuração, da instalação e da manutenção do sistema. Em outras palavras, eles são provedores e usuários do sistema;
- As redes LTE comerciais [30], nas quais esses órgãos são apenas usuários do sistema e não detém a responsabilidade do controle, da gerência, da configuração, da instalação e da manutenção do sistema.

Podemos verificar que a Figura 4.1 apresenta as interfaces físicas e lógicas padronizadas pela 3GPP entre os ativos das redes heterogênicas de banda larga e banda estreita. As interfaces garantem a utilização harmônica entre as redes de segurança pública (LTE e LMR) e as redes de exploração comercial LTE. A infraestrutura de *core* central é responsável pela integração macro da rede, integrando as redes legadas de banda estreita LMR, às redes de banda larga LTE comercial e o LTE privado da segurança pública. Assim, verificamos a apresentação dessa arquitetura de interoperabilidade entre as redes heterogênicas LMR e LTE, tanto pública como privada.

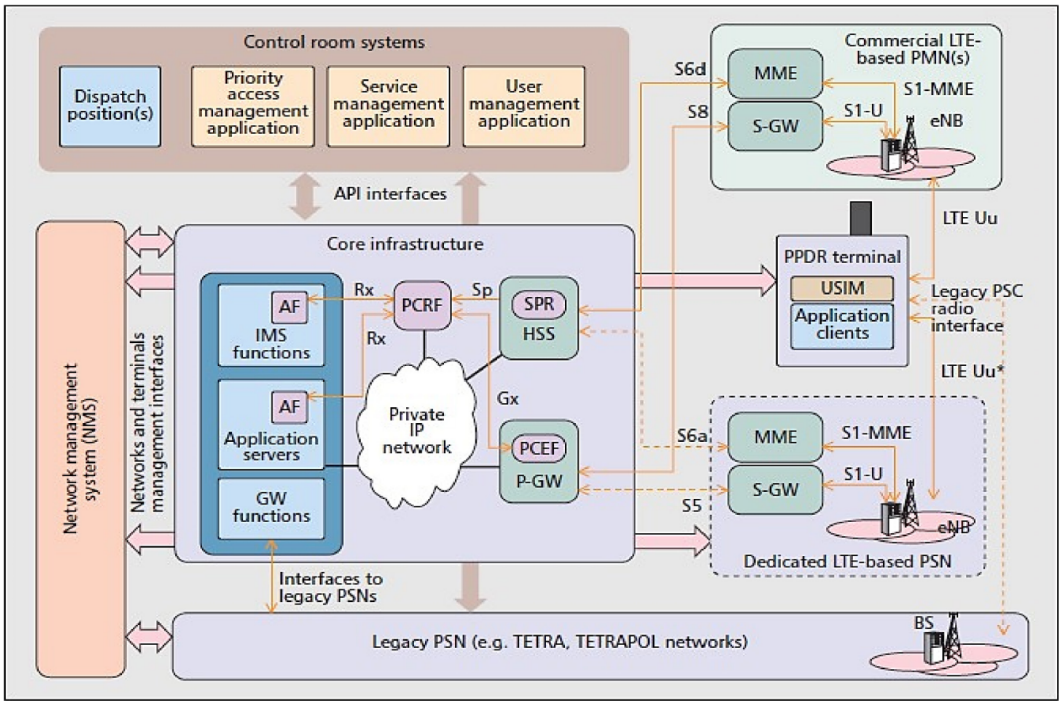

Figura 4.1: Interoperabilidade das redes 3GPP
Fonte: [31]

4.1 Arquitetura do servidor *wave*: funcionamento e características

O servidor *wave* é uma plataforma de interoperabilidade que integra redes de rádio LMR e redes LTE para entregar serviços unificados pareando voz de missão crítica com banda larga e aplicações multimídia.

A solução *wave* permite que as organizações construam redes de comunicação PTT interoperáveis, altamente extensíveis e flexíveis que conectam e estendam os sistemas de rádios bidirecionais existentes a redes e dispositivos de banda larga, em qualquer lugar. O *wave* 5000 oferece comunicações PTT entre rádios, *smartphones*, *tablets* e PC de qualquer local. O sistema pode suportar até 3000 usuários [32].

O *wave* 5000 é um aplicativo de fácil instalação e a funcionalidade é fornecida através de um servidor. O servidor pode ser comprado para o sistema ou integrado em uma rede existente. O *wave* 5000 Server gerencia todas as comunicações entre os sistemas MOTOTRBO e as redes e dispositivos de banda larga e mantém as credenciais dos usuários e as informações de configuração dos clientes de *smartphones*.

A Figura 4.2 apresenta a arquitetura de alto nível de integração.

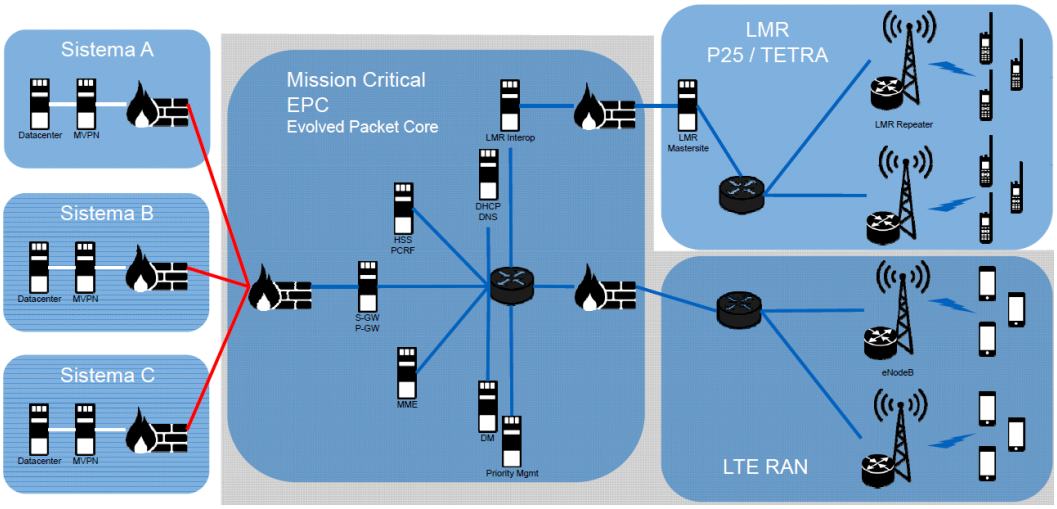

Figura 4.2: Arquitetura de integração LTE e LMR
Fonte: Adaptada da Motorola *Solution* (2018)

O sistema utiliza uma interface fixa para integrar-se com os sistemas de rádio MOTOTRBO *Connect Plus, Capacity Plus e Linked Connect Plus*. O aplicativo pode ser integrado a um sistema MOTOTRBO™, mas também pode ser usado como uma solução PTT de banda larga independente quando os rádios não são necessários [33]. O servidor *wave* gerencia todas as comunicações e salva todas as credenciais de configuração para os clientes do *smartphone* no sistema.

A figura 4.2 apresenta a arquitetura de alto nível em blocos da integração das redes banda LMR estreita e banda larga LTE, assim como a infraestrutura do servidor *wave* de forma detalhada, com as ligações físicas entre os ativos da rede heterogênica. Além disso, apresenta também o *gateway* de rádio para integração do sistema com rádios táticos militares. Por outro lado, a figura 4.3 apresenta a arquitetura mais detalhada à nível da integração das redes banda LMR estreita e banda larga LTE. O LTE RAN é interligado ao EPC, por outo lado o LMR é interligado ao EPC por meio do servidor de integração *wave* 5000. Além disso o EPC é integrado aos sistemas comerciais 3GPP e não 3GPP.

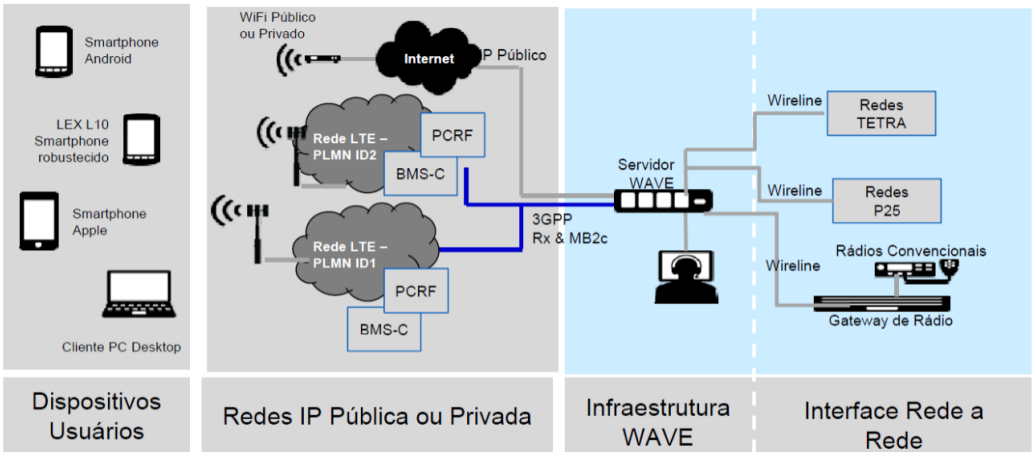

Figura 4.3: Arquitetura *wave* de integração
Fonte: Adaptada da Motorola *Solution* (2018)

O servidor *wave* apresenta ainda os seguintes benefícios:

- Estender o alcance aos usuários fora da cobertura dos usuários do sistema de rádio LMR existente para incluir computadores pessoais e dispositivos modernos;
- O sistema pode conectar vários sistemas de rádios bidirecionais e remover barreiras à interoperabilidade de comunicação e colaboração da força de trabalho;
- Oferece níveis mais altos de discrição para se comunicar com as equipes e maior flexibilidade para usuários que precisam se conectar a um sistema de rádio LMR ou a qualquer momento, em qualquer lugar;
- Mapeamento, presença e monitoramento de atividades de canal;
- Chamadas privadas, em grupo ou em vários grupos;
- Comunicações seguras com cada usuário, tendo um *login* e senha exclusivos, criptografia *Advanced Encryption Standard* (AES)-256 entre servidor e dispositivo do usuário, áudio, controle e credenciais todos criptografados;
- Opera sobre qualquer rede IP;
- Acesso às comunicações PTT do *Personal Computer* (PC);
- Monitoração, transmissão e recebimento de áudio de vários sistemas de comunicação, incluindo redes de rádio bidirecionais e telefones; e
- Uso de navegador da *Web* para acessar seus canais de comunicação *wave*;

4.2 Interoperabilidade entre redes LTE e LMR (P25)

No Brasil, em particular no EB, já foi realizada essa integração entre as redes LTE e a P25 por meio do servidor *wave*. Cabe salientar que essa integração é principalmente integração de voz entre os rádios e os dispositivos banda larga celulares [34].

Na arquitetura adotada pelo EB, existe uma integração lógica entre o controlador do P25 (*Mastersite* M3) e o servidor *wave*. Além disso, o aplicativo *wave* tem que ser instalado nos hospedeiros que são os dispositivos inteligentes *IOS*, transformando-os em um aparelho PTT.

A Figura 4.4 apresenta a arquitetura de integração das redes banda LMR estreita e banda larga LTE utilizado pelas FA. Essa arquitetura é formada por um servidor *wave* 5000, conectado física e logicamente ao EPC do LTE privado das FA e o controlador dos *sites* P25 *Mastersite*, um computador com a aplicação de gerenciamento e configuração do *wave*, e uma integrador para ligação com rádios táticos.

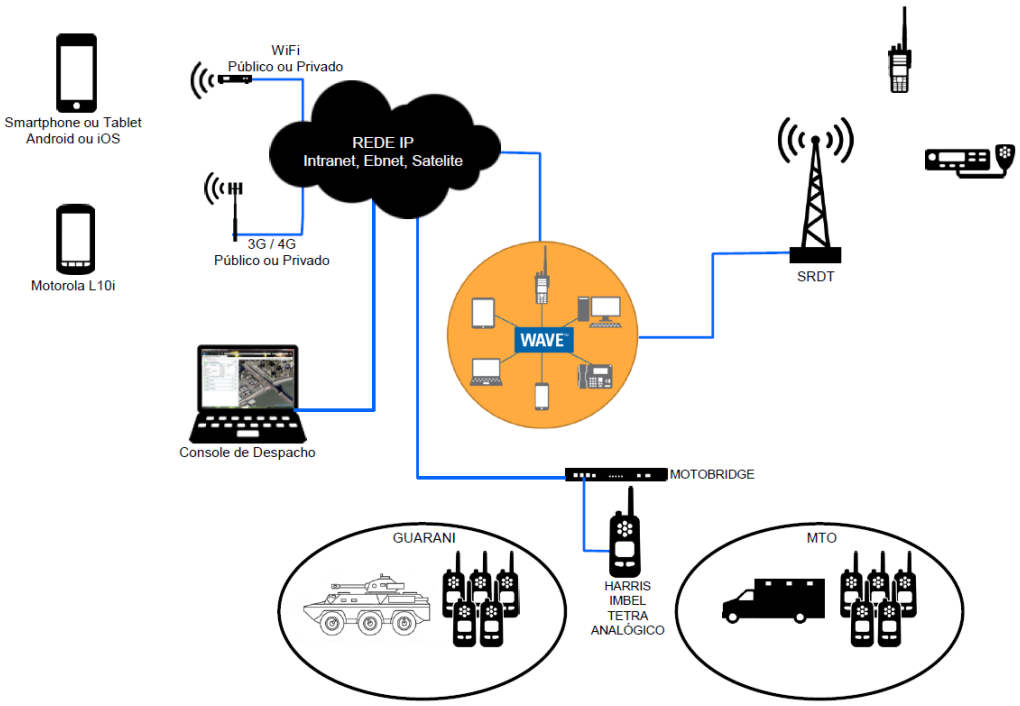

Figura 4.4: Arquitetura de integração LTE x P25
Fonte: Adaptada da Motorola *Solution* (2018)

Nesse sentido, o sistema apresenta solução de comunicação em grupo PTT sobre rede IP (celular, *Internet/Intranet* ou rede LTE privada) utilizando *smartphones* ou *tablets*

clientes com sistema operacional *Android*, IOS, podendo ser usado com a finalidade de flexibilidade para comunicação PTT, permitindo a comunicação entre:

- Rádio banda estreita com terminais Banda Larga;
- Terminais Banda Larga com Terminais Banda Larga;
- Integração de celular por meio de redes IP (celular, *Internet/Intranet* ou rede LTE privada) ;
- Acesso instantâneo e seguro à rede de rádio usando *Wi-Fi*, 3G ou 4G;

4.3 Conclusão

Neste capítulo foram apresentadas as possibilidades de integração dos sistemas de tecnologia banda larga LTE e os sistemas atuais LMR. Dessa forma, essa integração poderá garantir a utilização dos sistemas de forma harmônica, possibilitando uma atualização gradual para os sistemas de banda larga.

Além disso, foi apresentado a arquitetura do servidor *wave* que é utilizada para essa integração dos sistemas do EB [35]. Nesse sentido, verificamos as diversas funcionalidades dessa integração como comunicação PTT, por meio de aplicativos, entre LTE e P25.

Resumindo, podemos verificar que a integração entre as redes já é uma realidade. O EB já possui a integração de voz e redes de banda larga, proporcionando uma expansão dos serviços de voz da rede P25.

5 Implementação da Tecnologia LTE no Brasil para as Forças Armadas

5.1 Análise do modelo de implantação nos EUA

Atualmente, existe a demanda crescente por serviços de sistemas em banda larga para as missões críticas das FA e dos OSP, como compartilhamento de multimídia, chamadas de vídeo e *streaming* de vídeo ao vivo [28]. Esses serviços desempenham um papel importante para que mais operações sejam concluídas com sucesso. Nesse contexto, os sistemas LMR não atendem essas demandas de altas taxas de dados.

Outro problema é a falta de interoperabilidade entre os órgãos de governo. Esse problema se dá pelo fato de existir uma diversidade de tecnologias LMR que não se comunicam de forma nativa. Por exemplo, o sistema LMR das FA que é o APCO25 não tem integração sistêmica [29] com o sistema LMR da PF que é o TETRAPOL e muito menos com o sistema LMR da PRF que é o TETRA.

Além disso, a rede LTE é baseada em padrões abertos, com arquitetura consistente. Por outro lado, seria necessário altos investimentos para garantir a implantação de uma rede privada LTE que atendesse exclusivamente aos órgãos de governo. Além dos altos custos de implantação teríamos os custos de operação e manutenção e isso tornaria essa rede privada LTE totalmente inviável do ponto de vista econômico, pois dependeria apenas dos recursos públicos tanto federal, estadual e municipal, uma vez que nesse modelo os órgãos de governo seriam ao mesmo tempo provedores e usuários do sistema.

No entanto, a tendência mundial é de utilização dual da rede de banda larga com utilização compartilhada entre as FA, os OSP e o restante da sociedade. Atualmente três países estão trabalhando para implantar essa rede de banda larga de telefonia compartilhada para a segurança pública, são eles: EUA, Reino Unido e México. Nesse contexto, será apresentado, basicamente, as características de implantação nos EUA, tendo em vista servir de modelo, com algumas adaptações, do que pode ser feito aqui no Brasil.

5.1.1 *Projeto First Responder Network Authority* (FirstNet)

Nos EUA, o desenvolvimento desta rede nacional compartilhada é traduzido no projeto da *First Responder Network Authority* (FirstNet). A FirstNet, é uma agência federal criada pelo Congresso americano em 2012 para supervisionar a construção, implantação e operação de uma nova rede de banda larga de segurança pública nacional [30].

A FirstNet deve fornecer os benefícios das redes comerciais de banda larga (por exemplo, acesso prioritário a dados de alta velocidade, serviços baseados em localização, ferramentas de gerenciamento de incidentes), com maior confiabilidade, segurança e redundâncias necessárias para as atividades de comunicações críticas que a segurança pública requer [3].

Para atender a esse objetivo, o Congresso alocou 20 MHz para a segurança pública, sendo que a FirstNet detém a licença para os 20 MHz de espectro. A lei autorizadora da locação permite a FirstNet firmar uma parceria público-privada e um contrato de terceirização para construir, gerenciar e operar a rede de banda larga com exploração dual.

A lei também permitiu acesso à capacidade da rede em caráter secundário por outros usuários, ou seja, acesso ao espectro quando não estiver em uso pela segurança pública [3]. Em outras palavras ela pode explorar economicamente a banda não utilizada pelas FA e pelos OSP.

Nesse contexto, a empresa terceirizada, *American, Telephone and Telegraph* (AT&T), tem permissão para explorar todos os 20 MHz do espectro em caráter primário para Defesa Nacional e os OSP e, em caráter secundário, para exploração comercial. Dessa forma, ela pode gerar receitas de usuários de segurança pública que devem ser usadas para apoiar e melhorar a rede, podendo também, gerar receita de outros usuários (por exemplo, usuários secundários, clientes comerciais) quando o espectro não estiver em uso pela segurança pública [36].

A Figura 5.1 apresenta o modelo de negócio no qual a rede é mantida com recursos dos usuários de segurança pública e exploração comercial, explicitando o modelo dual de utilização da rede de banda larga tanto para a segurança pública quanto para emprego comercial. Nesse sentido a rede de banda larga para segurança pública pode apresentar a RAN tanto fixa como móvel. A RAN possui um*link* para o *core* da rede e também para os usuários da rede privada.

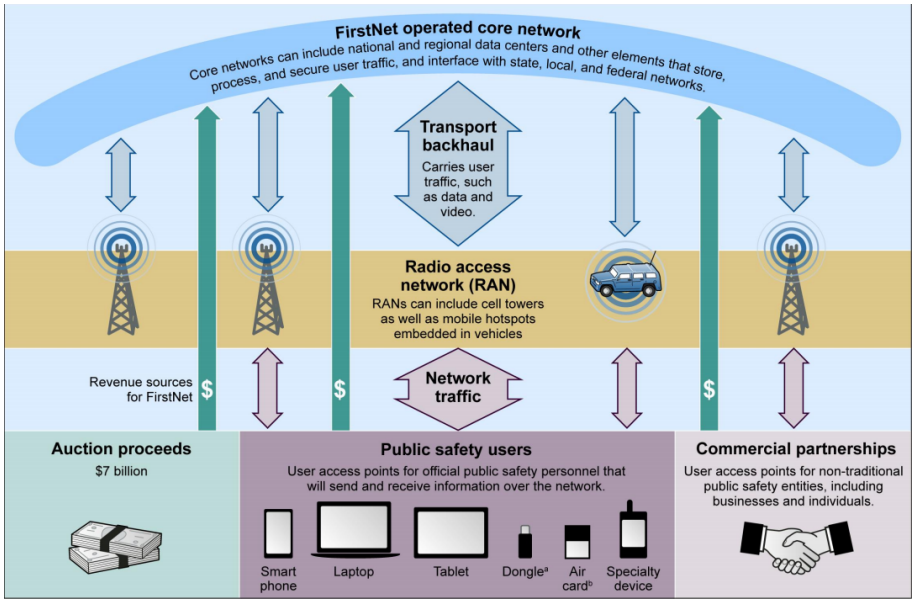

Figura 5.1: Modelo de Negócio EUA
Fonte: [37]

Por outro lado, após análise da capacidade da rede implementada pela vencedora do processo em termos de áreas de cobertura, verificou-se a necessidade de expansão da rede. Nesse sentido, analisou-se a possibilidade de integração de outras redes comerciais à rede FirstNet implantada pela AT&T, salientando a importância da manutenção da segurança, interoperabilidade e sustentabilidade da rede original em atendimento aos requisitos de comunicações críticas.

5.1.2 Expansão da Rede utilizando a integração núcleo a núcleo

Durante o processo de implantação da rede de banda larga, defensores da segurança pública e especialistas do setor debateram se deveria haver um único fornecedor nacional para o FirstNet ou se poderia haver vários fornecedores e vários núcleos interconectados para compor a rede original da FirstNet [38], em outras palavras, a rede seria fornecida por uma única entidade ou diversas entidades.

Nesse contexto, a FirstNet decidiu por uma solução centralizadora, ou seja, solução nacional de um único fornecedor [30]. Essa solução foi incluída no contrato de terceirização *Request for Proposal* (RFP) que é um documento que lista todas as necessidades da empresa contratante para aquisição de produtos ou contratação de serviços de terceiros. Parecida com uma licitação privada, a RFP mostra o interesse de uma empresa aos fornecedores, que concorrerão entre eles para fechar o negócio.

Após a adjudicação da RFP pela empresa AT&T, vários fornecedores comerciais defenderam a interligação de outros núcleos ao núcleo FirstNet/AT&T. Isso permitiria que os provedores comerciais pudessem fornecer os serviços para a segurança pública explorando o excedente de banda e aumentar a área de cobertura da rede FirstNet/AT&T quando necessário.

Porém, a AT&T argumentou que a RFP exigia, nos seus termos, que terceirização dos serviços fossem executadas apenas por uma única entidade comercial com um núcleo de rede apenas, não permitindo, assim, vários núcleos de redes de diversas entidades comerciais. Além disso, afirmou que a integração de vários núcleos na rede nacional aumentaria os riscos cibernéticos. Essas considerações fizeram com que a FirstNet concordasse com a AT&T pois a adoção de um único núcleo de uma única operadora reduziria o risco de complicações inerentes a uma arquitetura multinúcleo que seria operada por entidades distintas dificultando o controle, a fiscalização e a responsabilização por serviços prestados abaixo do acordado em RFP, pois a responsabilidade pela rede seria compartilhada entre as prestadoras de serviço ocasionando complexidade operacional, complexidade e vulnerabilidade na segurança. Assim, segundo FirstNet/ AT&T uma proposta de interoperabilidade núcleo a núcleo não seria a melhor solução para implementar a rede de segurança pública, pois aumentaria os riscos da segurança cibernética entre outros.

Nesse contexto, objetivando a perfeita implantação da rede de banda larga para a segurança pública compartilhada com o uso comercial, foram analisados as condições necessárias para atender a demanda do Congresso Americano que na assinatura do ato de concessão exigia que a rede fosse segura, interoperável e autossustentável [37]. Em complementação o *Government Accountability Office* (GAO) observou em seu relatório de julho de 2017, que os clientes da segurança pública, que entrevistou, levantaram preocupações sobre vários aspectos da rede, incluindo resiliência, confiabilidade, redundância, segurança cibernética, estruturas para identidade do usuário, credenciamento de usuários e gerenciamento de acesso, e priorização de usuários na rede. Os estados levantaram preocupações semelhantes durante a revisão dos planos estaduais. Essas preocupações levaram às seguintes constatações e providências por parte da FirstNet e AT&T:

- Segurança: declararam que a integração de outras redes centrais que podem não adotar e aplicar os mesmos requisitos técnicos de segurança, protocolos, treinamento e melhores práticas pode comprometer a qualidade do serviço de banda larga;
- Interoperabilidade: O ato de concessão da faixa de 20 MHZ à FirstNet possibilitava a interoperabilidade por meio de interconexão núcleo a núcleo e acordos de *roaming* automático mútuo com outras operadoras além da AT&T [39]. Porém a AT&T

observou que a interoperabilidade entre núcleos pode ser tecnicamente viável, mas ainda não foi testada entre operadoras comerciais o que traz um grande risco do ponto de vista técnico, além de trazer altos riscos de segurança. Nesse sentido a FirstNet concordou com a AT&T, observando que há incerteza sobre como as conexões núcleo a núcleo afetariam a interoperabilidade e a segurança;

- Sustentabilidade: Em seu Relatório de 2017, o GAO observou que, no momento em que as operadoras comerciais também puderem oferecer os serviços de banda larga para os OSP competindo com a rede da FirstNet que isso pode prejudicar a adesão desses órgãos à sua rede, o que pode afetar a sustentabilidade e a melhoria de longo prazo da rede implementada pela FirstNet [40]. Por um lado a interoperabilidade dos núcleos posde estimular a concorrência e reduzir os custos, por outro lado, pode afetar negativamente a quantidade de adesões à rede da FirstNet prejudicando a viabilidade de expansão, operação e manutenção da rede a longo prazo;
- Segurança Cibernética: A lei exige que a rede seja segura e confiável, e tenha proteções contra ataques cibernéticos. A FirstNet/AT&T aproveitou as melhores práticas do setor e as melhores práticas federais para garantir uma rede segura para a segurança pública. A AT&T planeja integrar a segurança cibernética em dispositivos e aplicativos. Todos os dispositivos devem ser rastreados antes que os usuários possam acessar a rede. A AT&T planeja rastrear dispositivos com base nos padrões da AT&Te, em seguida, a FirstNet/AT&T planejam fazer a triagem desses dispositivos, com base nos padrões federais incluídos no *National Institute of Standards and Technology* (NIST) *Cyber Security Framework*. A FirstNet/AT&T planejam fornecer um sistema de gerenciamento de identificação e gerenciamento de credenciais e acesso *Identity, Credential, and Access Management* (ICAM) altamente seguro, que permite um sinal único para usuários do FirstNet. A FirstNet está trabalhando com os Departamentos de Segurança Interna, Justiça e Comércio e o Escritório de Administração e Orçamento para alavancar melhores práticas e para garantir que a rede seja segura. Nesse contexto, a FirstNet seria construída com camadas de segurança, projetadas em RAN, a rede central e as plataformas de serviço, bem como os dispositivos. Além disso, os *firewalls* aplicarão políticas de segurança rigorosas desenvolvidas em cooperação com o *Department of Homeland Security* (DHS) e o *Department of Defense* (DoD) para atender aos requisitos do NIST. O projeto FirstNet deve ser guiado pelos padrões 3GPP para criptografia e outras medidas de segurança baseadas em padrões e práticas recomendadas. As comunicações devem ser executadas em um núcleo separado, sem fio e criptografado, para garantir que as comunicações de segurança pública sejam seguras. Além disso, a AT&T deve for-

necer um centro de operações para monitorar o tráfego na rede FirstNet e garantir que seja seguro. Apesar dessas atividades, existem riscos de segurança cibernética. Os aplicativos desenvolvidos para a rede por desenvolvedores externos precisarão ser rastreados e seguros. Um projeto piloto de 2017 conduzido pela *Science and Technology Directorate* (S&T) do DHS descobriu que 33 (trinta e três) aplicativos populares usados pela segurança pública tinham preocupações com segurança e privacidade O DHS enfatizou a necessidade de rastrear e testar aplicativos de segurança pública quanto a vulnerabilidades.

5.1.3 Cobertura da rede

No que diz respeito à cobertura, a FirstNet incluiu duas disposições principais sobre cobertura. Um requisito de curto prazo para fornecer à segurança pública acesso à cobertura nacional dentro de seis meses após a concessão, para acelerar a adoção da banda larga, conforme incentivado pela lei, e um requisito para fornecer um plano de implantação de cinco anos de longo prazo, com marcos de cobertura rural para cada fase de implantação, conforme exigido pela lei. Embora as disposições da RFP reflitam os requisitos da lei, a natureza proprietária do contrato e os planos de implantação do estado tornam difícil determinar se os requisitos da lei estão sendo atendidos, como os recursos fornecidos, por exemplo US$ 6,5 bilhões e 20 MHz, estão sendo usados e se a rede está sendo implantada conforme pretendido pelo Congresso.

Para o plano de implantação de curto prazo, a FirstNet exigiu que a contratada fornecesse cobertura nacional, usando o espectro de Banda Classe 14 (espectro FirstNet) ou outro espectro (não-Banda Classe 14), no prazo de seis meses após a adjudicação. Esta disposição permite que o contratante forneça cobertura nacional através da construção da nova rede nacional no espectro de Banda Classe 14 (espectro FirstNet) ou fornecer cobertura nacional usando seu próprio espectro e redes. Essa disposição visava agilizar a entrega da rede de banda larga aos OSP, conforme incentivado pela lei, e oferecer uma solução nacional enquanto a rede FirstNet estava sendo construída, o que deve levar cinco anos para a implantação inicial.

Após a adjudicação do contrato, a AT&T anunciou que abriria todas as suas bandas de espectro habilitadas para LTE (ou seja, todo o seu espectro de banda larga) para uso de segurança pública e forneceria serviços de prioridade e preempção para usuários de segurança pública que assinassem a rede FirstNet. Isso forneceria aos usuários de segurança pública acesso imediato a serviços de banda larga, acesso a uma rede nacional e garantias de que as comunicações de segurança pública seriam priorizadas na rede comercial da AT&T durante emergências.

5.1.4 Grau da Segurança Resiliente

Em seu relatório de julho de 2017 [3], o GAO observou, também, que os clientes da segurança pública, que entrevistou, levantaram preocupações sobre vários aspectos da rede, incluindo resiliência, confiabilidade, redundância, cibersegurança, estruturas para identidade do usuário, credenciamento de usuários e gerenciamento de acesso e priorização de usuários na rede. Os estados levantaram preocupações semelhantes durante a revisão dos planos estaduais.

A rede de banda larga deve ter requisitos técnicos para garantir que a rede seja confiável, segura, e principalmente resiliente e possa resistir a danos e desastres. Nesse sentido, a FirstNet declarou que a sua rede terá os requisitos de resiliência de uma rede típica de banda larga de segurança pública, projetando a sua rede com os padrões pelos quais os sistemas de segurança pública são construídos, ou seja, com requisitos e recursos adicionais, para garantir que a rede continue funcionando nas condições adversas. Dessa forma, os equipamentos da rede de banda larga podem ter redundância no fornecimento de energia. Por outro lado, a rede de transporte que fornece o *backhaul* poderá ter duplicidade para o tráfego de dados garantindo assim uma maior confiabilidade da rede de banda larga.

A segurança, confiabilidade e resiliência da rede FirstNet são importantes não apenas para garantir que a rede continue operando durante e após grandes desastres, mas também para conquistar a adesão dos usuários de segurança pública.

5.1.5 Acessibilidade e Sustentação Modelo EUA

De acordo com a lei, a rede deve ser permanentemente autofinanciada. O GAO declarou que a FirstNet/AT&T estabeleceram uma estrutura para financiar a rede para atender a esse requisito. Eles podem cobrar dos usuários (por exemplo, usuários de segurança pública e usuários secundários) pelo uso da rede, podendo também monetizar (ou seja, obter receita com) o excesso de capacidade do espectro de banda larga de 20 MHz da rede de governo, quando não estiver em uso pela segurança pública. A partir dessa receita, a AT&T deve pagar as taxas operacionais e administrativas da FirstNet, realizar investimentos de US$ 40 bilhões ao longo da vigência do contrato para apoiar a construção, operação e manutenção da rede de governo.

A Figura 5.2 apresenta o modelo de sustentabilidade da rede, na qual os clientes da rede são divididos em usuários de segurança pública e usuários comerciais. Ambos os usuários pagam pelos serviços da rede, porém a prioridade sempre é dos usuários de segurança pública. Nesse sentido, parte dos recursos são destinados para ampliação da

rede, parte para a sua manutenção e parte para a operação dessa rede. A FirstNet e a AT&T fazem o gerenciamento desses recurso para atender a demanda da lei.

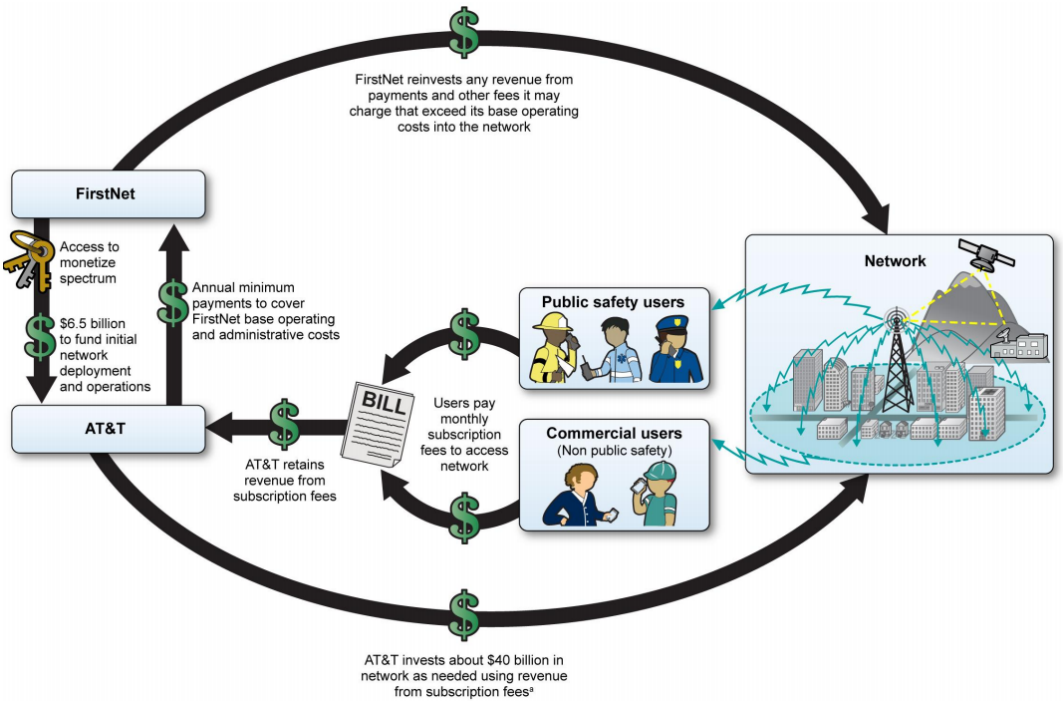

Figura 5.2: Modelo de sustentabilidade EUA
Fonte: [37]

Nesse modelo temos os seguintes passos:

- A FirstNet dá acesso à AT&T para exploração econômica do espectro de 20 MHZ;
- A FirstNet faz um investimento inicial de US$ 6,5 bilhões à AT&T para iniciar a implantação e operação inicial da rede;
- Os usuários de segurança pública utilizam a rede e pagam a AT&T pelos serviços explorados. Cabe salientar que esses possuem prioridade na utilização dos serviços;
- Os usuários comerciais, utilizam a rede e pagam a AT&T pelos serviços explorados, quando a rede não estiver sendo utilizada pela segurança pública;
- A AT&T recebe os lucros da exploração dos serviços dos assinantes da rede;
- A AT&T realiza pagamentos mínimos anuais à FirstNet para cobrir os custos operacionais e administrativos básicos;
- A FirstNet reinveste na rede qualquer receita de pagamento e outras taxas que possa cobrar que excedam seus custos operacionais básicos;

- A AT&T investe cerca de US$ 40 bilhões na rede conforme necessário usando receita dos usuários do sistema.

5.2 Aplicação adaptada do modelo dos EUA para o Brasil

Uma diferença fundamental na implantação no Brasil é que a faixa de frequência de utilização para um sistema de banda larga (4G/LTE) foi atribuída às FA e aos OSP, pela ANATEL.

Nesse contexto, poderia ser criada uma rede única para segurança pública em banda larga, com o Governo Federal utilizando a Telecomunicações Brasileiras S/A (TELEBRAS) como órgão gestor, assim como a FirstNet nos EUA.

A TELEBRAS na qualidade de administradora dos serviços da rede de comunicações críticas de banda larga de uso dual (privado e público), com arquitetura de redes 4G ou 5G, coordena o acesso às redes de segunda à quinta geração de telefonia. Nesse contexto, priorizando o acesso à rede ao Ministério da Defesa (MD).

A TELEBRAS seria proprietária dos ativos, e homologada para uso das frequências, sendo subsidiada por recursos oriundos da exploração da banda quando essa não tivesse sendo utilizada pela segurança pública. Ela também seria responsável pela instalação, operação e manutenção da rede, podendo esses serviços serem terceirizados, mas a responsabilidade técnica ficaria com a TELEBRAS.

Nesse contexto, a TELEBRAS poderia ceder a exploração para empresas privadas e essas garantiriam a instalação, operação e manutenção da rede e em contrapartida, a utilizariam a faixa de frequência sem ter pagado por ela em leilão.

5.2.1 Aderência aos Requisitos de Comunicações Críticas

O Grau de segurança, principalmente a cibernética, é fundamental para a confiabilidade do sistema, pois o sigilo dos dados que irão trafegar na rede é fundamental para o sucesso das operações. Além disso, a garantia de prioridade no tráfego, escalabilidade e sustentabilidade das redes são os parâmetros que poderão tornar a rede viável para a utilização em comunicações críticas. Nesse contexto, TELEBRAS seria responsável pelos seguintes parâmetros:

- Segurança cibernética da rede de acordo com os parâmetros estabelecido pelas FA;

- Prioridade de acesso à rede, de acordo com os parâmetros estabelecido pelas FA;
- Integração da HetNet, CCOp Mv, LTE tático (*core*, ou eNodeB) com a rede da própria TELEBRAS ou rede parceira;
- Expansão, manutenção e operação da rede mediante partes dos lucros obtidos com a exploração do excedente da banda;
- Resiliência da rede: As redes devem ser projetadas com elementos de redundância e estabelecimento de procedimentos de restauração rápida com recursos de *backup*. Deste modo, caso algum elemento se torne indisponível, a funcionalidade poderia ser transferida automaticamente para outro elemento ou o elemento indisponível poderia ser restabelecido no menor tempo possível. Por este motivo, torna-se essencial que o sistema tenha visibilidade de todos os recursos em tempo real, sendo que em determinadas configurações existem limitações dos recursos compartilhados.

5.2.2 Acessibilidade e Sustentação para o Brasil

O modelo seria semelhante ao utilizado nos EUA, porém com a diferença de que as FA utilizariam a rede sem pagar pelos serviços pois a contrapartida seria a utilização da banda ociosa explorada economicamente.

A Figura 5.3 ilustra um possível modelo de acessibilidade econômico brasileiro, no qual os clientes da rede são divididos em usuários das FA e usuários comerciais. Apenas os usuários comerciais pagariam pelos serviços da rede, porém a prioridade sempre seria dos usuários do MD. Esses usuários seriam isentos da remuneração pelos serviços, tendo em vista que a faixa de frequência utilizada seria aquela autorizada para utilização desse órgão. O gerenciamento desses recursos seria da TELEBRAS e das terceirizadas.

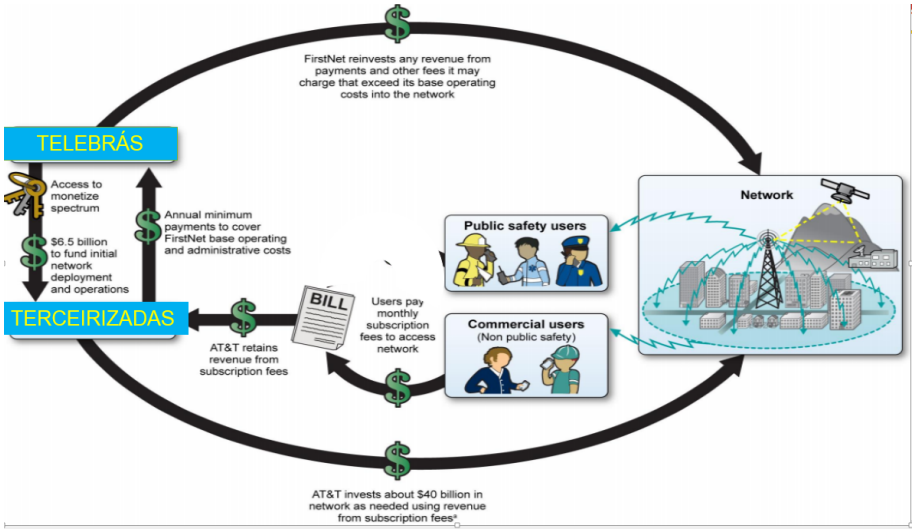

Figura 5.3: Modelo de sustentabilidade Brasil
Fonte: Adaptado de [37]

A utilização e não pagamento do serviço se justificaria pela baixíssima taxa de ocupação do espectro. Cerca de 1% (um por cento) de ocupação efetiva. Essa sobra poderia ser explorada pelas operadoras parceiras.

Para garantia de isonomia econômica do bem público (espectro) deveria-se, obrigatoriamente, exigir contrapartida ao uso da frequência em caráter secundário, por intermédio de fornecimento de infraestrutura/equipamentos/serviços/sistemas/licenças para ampliação da Rede Privativa de Comunicação da APF.

A Parceira seria responsável pelo fornecimento de toda a infraestrutura que a TELEBRAS porventura não atendesse, disponibilizando toda a sua infraestrutura de acesso.

A Parceira iria remunerar a TELEBRAS com um percentual da receita recebida dos usuários privados.

A TELEBRAS iria remunerar a Parceira por cada ativação de novo usuário.

5.2.3 Cobertura da rede no Brasil

A cobertura inicial seria da TELEBRAS e das operadoras terceirizadas, porém a expansão da rede seria realizada com partes dos lucros da exploração econômica do espectro, seguindo a orientação de um conselho da segurança pública que iria decidir sobre a expansão dessa rede. Nesse sentido poderiam ser realizados *roaming* para expandir a capilaridade da rede.

A ativação de novos *sites* seria realizada mediante pedido do MD à TELEBRAS, por meio de solicitação administrativa com os parâmetros necessários para a realização do projeto de expansão para atender os serviços solicitados, ficando assim, responsável por todo o serviço de instalação e, englobando as seguintes atividades:

- Realização do planejamento do novo *site*, assim como a capacidade necessária para cada setor a ser criado;
- Busca, aquisição do *site*;
- Implantação do *site* ;
- Expansão da rede nas áreas de cobertura por meio de acordos de *roaming*.

5.2.4 Priorização de Tráfego

A rede em questão teria uma priorização de tráfego para usuários da Rede Privativa de Comunicação da Administração Pública Federal (provisionados no núcleo de rede com perfil específico).

A TELEBRAS deveria manter, mediante acordo com os parceiros, o respeito a priorização de tráfego onde a TELEBRAS não opera a rede de forma direta.

A metodologia de acesso ao meio utilizando o *Orthogonal Frequency Division Multiplexing/Multiple Access* (OFDMA) no enlace de descida (*Downlink*) e o *SC-FDMA* (Múltiplo Acesso por Divisão de Frequência com portadora única) no enlace de subida (*Uplink*), poderiam garantir uma alocação dinâmica para usuários com tipos, qualidades de serviços, e prioridades diferentes.

Uma forma eficiente de priorização de tráfego seria a de controle de admissão e as classes de acesso. Priorização na classe de acesso (*Access Class Baring* (ACB). Essa priorização acontece no *Universal Subscriber Identity Module* (USIM) do *SIM card*, determinando quais dispositivos têm prioridade de acesso à rede.

O controle de admissão e *preemption*, determina qual usuário é servido e qual tipo de serviço será oferecido. Utiliza o protocolo *Address Resolution Protocol* (ARP). Em uma situação de alto tráfego em que seja necessário utilizar a rede pelos usuários das FA, a rede automaticamente retira os usuários privados.

5.2.5 Segurança Cibernética

Esse problema técnico é o mais difícil a ser resolvido pois a rede LTE compartilhada, diferente da LMR, não será de domínio completo das FA. Nesse contexto, existem di-

ferentes ataques na rede de acesso e no EPC da rede. O LTE tem um papel central em nossa sociedade da informação combinando metas de desempenho com mecanismos de segurança modernos e atende tanto no uso casual, bem como infraestrutura crítica e comunicações de segurança pública. Ambos os cenários exigem uma especificação e implementação resiliente e segura de LTE, pois interrupções e vetores de ataque abertos podem levar a riscos graves.

A Figura 5.4 apresenta os tipos de ataques cibernéticos que a rede LTE pode sofrer [41], mostrando os principais ataques em uma rede de telefonia de 4G LTE. A rede está estruturada de forma a diferenciar os diversos tipos de ataque: ataques na rede de transporte que interligam todos os ativos dessa rede; ataque nos servidores tanto os de autenticação quanto nos servidores de aplicação; ataque no hospedeiro, podendo ser aparelhos móveis ou fixos, e ataque na interface de acesso à rede, que é o enlace de *uplink e downlink*.

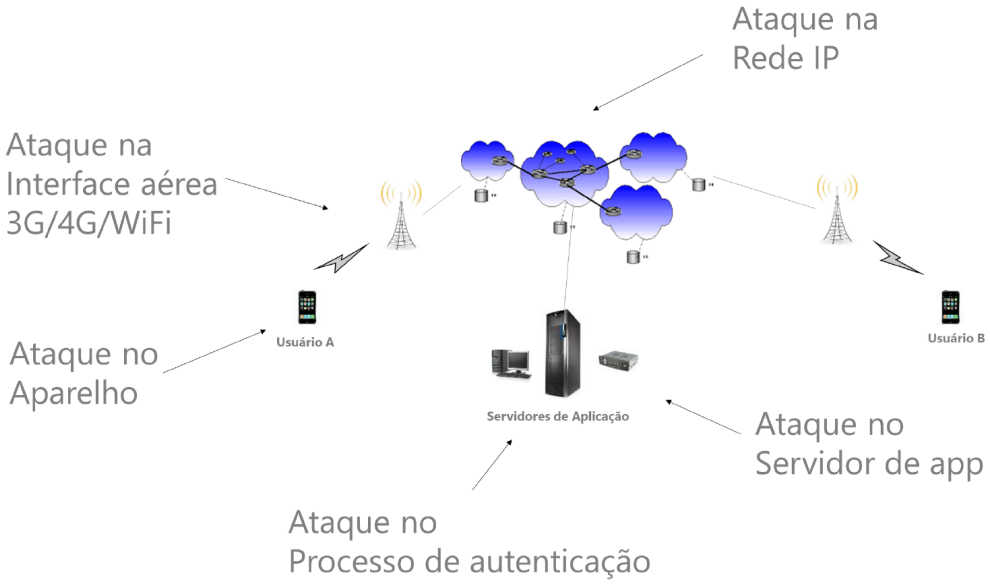

Figura 5.4: Principais ataques na rede de banda larga
Fonte: Adaptada da Motorola *Solution* (2020)

Nas subseções abaixo, apresentamos os principais ataques da redes LTE.

Ataque de interface aérea

Nesse ataque podem ser roubados os dados do USIM do aparelho do usuário e tentar se autenticar na rede, esse ataque normalmente pode ser minimizado por conta dos protocolos de autenticação e controle de acesso ao núcleo da rede. Essa vulnerabilidade está na interface entre o UE e a E-UTRAN.

Ataque na rede *IP*

Esse ataque é caracterizado pela interceptação ou invasão da rede de transporte (*link da internet*), que conecta os diversos dispositivos da rede como servidores, EPC, E-UTRAN entre outros.

Ataque no aparelho

Esse ataque é caracterizado pelo extravio do aparelho ou utilização por meio de quebra de senha de utilização. O invasor, de alguma forma, consegue acessar o UE e entrar na rede.

Ataque no processo de autenticação

Essa vulnerabilidade está na interface entre o UE o HSS do EPC. Ele acontece no processo de autenticação do UE e a rede.

Ataque no servidor de aplicação

Esse ataque é caracterizado pela invasão dos aplicativos que são utilizados para prover os serviços de comunicações críticas e estão hospedados nos provedores de serviços.

5.2.6 Atividades de segurança cibernética na rede LTE

Para minimizar os problemas do ataque cibernético a rede LTE podemos citar nas subseções abaixo quais mecanismos podemos utilizar.

Segurança de acesso à rede

Mecanismo que fornece acesso seguro aos serviços para usuários e protege o*link* de acesso por rádio contra eventuais ataques. O LTE fornece mecanismos de segurança altamente sofisticados para autenticação, autorização, integridade e confidencialidade que tornam a interface aérea do LTE e a sinalização de controle de recursos de rádio altamente seguros e imunes a intrusões ilegais. A segurança pela interface de rádio, que fica entre a Estação Rádio e o UE, consiste na proteção da integridade da sinalização de controle e na criptografia da sinalização de controle e dos dados do usuário.

Para redes de Missão Crítica, recomenda-se a adoção de algoritmos de segurança especificados pelo 3GPP para garantir a integridade e criptografia das informações. Os algoritmos 128-EIA1, 128-EIA2 e 128-EIA3 destacam-se para garantir a integridade. Já para criptografia, as opções dos algoritmos são 128-EEA1,128-EEA2, 128-EEA3 que podem ser utilizados para proteger a sinalização de controle e os dados dos usuários.

Segurança de domínio do usuário

Mecanismo que fornece acesso seguro para estações móveis, incluindo autenticação mútua entre o Módulo de Identidade do Assinante Universal e o UE. A autenticação e o gerenciamento das chaves são essenciais para a segurança da rede celular porque fornecem autenticação mútua entre os usuários e a rede e derivam chaves criptográficas para proteger a sinalização e os dados do plano do usuário. Informações sensíveis são armazenadas no *SIM card* do dispositivo LTE/UE, bem como no servidor HSS que dá para garantir a autenticação mútua do UE e da rede LTE. Toda a sinalização de controle de recursos de rádio é protegida de acesso não autorizado e a inspeção fim-a-fim usando algoritmos para garantir a confidencialidade e a integridade entre o UE e o MME. Cada geração de redes celulares sempre define, pelo menos, um método de autenticação, sendo usado para redes *Evolved Packet System based Authentication and Key Agreement* (EPS-AKA) LTE (para redes 4G).

Segurança no domínio da aplicação

Mecanismo que garante a segurança na troca de mensagens de aplicativos, tanto no domínio do usuário, quanto no domínio do provedor. A segurança no domínio da aplicação deve ser realizada de ponta a ponta entre a aplicação no terminal e o recurso que fornece o serviço, cabendo ao provedor garantir a disponibilidade do serviço do canal de comunicação. Entretanto, a confidencialidade e integridade devem ser tratadas na camada da aplicação. A criptografia de ponta a ponta deverá estar disponível na solução de rede móvel do fabricante (rádio, *Voice over LTE* (VoLTE), etc).

Nesse contexto, a prevenção tomada pelas FA fica restrita a segurança ponto a ponto, criptografia, para voz/dados na camada de aplicação, na qual os mecanismos de segurança serão instalados nos hospedeiros finais, além da segurança de acesso aos dispositivos.

Por outro lado, a TELEBRAS deverá aplicar os demais mecanismos de segurança para garantir a confiabilidade da rede. Nesse sentido, os servidores, tanto de aplicação, quanto de autenticação, deverão receber uma atenção especial.

5.2.7 Qualidade de Serviço (*QoS*)

A QoS vai determinar a confiabilidade do sistema em operações típicas militares e não militares. Para o LTE são definidas classes de QoS. Algumas dessas classes já são especificadas para missão crítica na 3GPP, porém, além desses parâmetros, mediante estudos técnicos e da necessidade de atendimento à demanda operacional, poderão ser adicionados mais requisitos de QoS.

5.2.8 Interoperabilidade com os Sistemas Proprietários das Forças Armadas

Para uma completa integração e utilização dessa rede será necessária a integração com a rede proprietária de cada órgão, pois como já dito anteriormente, nos projetos das FA será necessária a utilização de redes estanques proprietárias, que serão utilizadas exclusivamente por militares. Nesse sentido, teremos redes heterogênicas, tanto do ponto de vista de diferentes tipos de provedores de serviço, quanto com relação ao tamanho das células. Analisaremos por ora, apenas a rede heterogênica do ponto de vista de provedores de serviço.

- Provedor TELEBRAS: A rede que atualmente é operada e gerenciada pela TELEBRAS. Nessa rede, o provedor tem controle sobre todos os ativos da rede;
- Provedor parceiros: São aqueles aos quais poderão ser realizados de acordos de *roaming* ou de utilização da rede, porém a TELEBRAS não detém todo controle sobre os ativos da rede;
- Provedor FA: Utilização do núcleo 4G operacional Por exemplo, o CCOp Mv, LTE tático entre outros. O objetivo é ter uma rede heterogênica, com células de tamanho variado e integradas onde a periferia da rede será realizada por essas redes de acesso privado, porém, esse terá apenas o serviço de rede de acesso local, não realizando controle de configuração da rede da TELEBRAS.

Nesse sentido, a rede móvel privada da segurança pública composta por redes com o CCOp Mv, LTE tático, iriam se integrar a rede gerenciada pela TELEBRAS. No primeiro caso, por meio de ligação entre núcleos de rede e, no segundo caso, de eNodeB para *core*. Além disso, os recursos dessa rede não serão compartilhados para utilização civil, pois são para a atividade típica do MD.

Possibilidades de integração entre as redes publica e privada

1) Ligação entre núcleos de rede: Nesse cenário o núcleo de rede do EB deverá ser interconectado ao núcleo TELEBRAS, através de *backhaul*. Nesse contexto, a gerência e configuração da rede ficariam com o MD. A arquitetura é apresentada na Figura 5.5, que explicita a rede heterogênica composta pelo LTE privado do MD e parte do LTE público da TELEBRAS. A conexão de EPC à EPC possibilita a segregação física e lógica das redes. Nesse contexto, as FA poderão gerenciar, operar e configurar a própria rede. Por outro lado, ela poderá utilizar a rede privada da TELEBRAS para aumentar a sua área de cobertura, porém nesse caso ela será apenas usuária dos serviços.

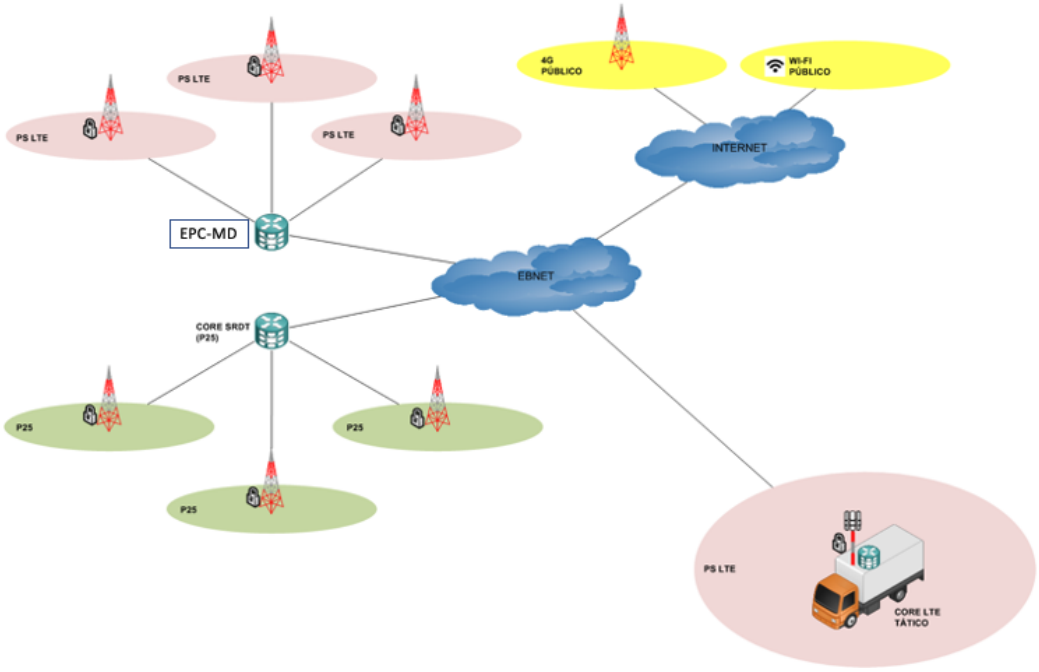

Figura 5.5: Ligação entre núcleos de rede
Fonte: Adaptada da Motorola *Solution* (2018)

2) Ligação eNodeB ao núcleo da rede: A eNodeB LTE deverá ser conectada através de *backhaul* diretamente ao núcleo da rede TELEBRAS, dessa forma, o MD não teria controle sobre gerência e configuração da rede. A arquitetura é apresentada na Figura 5.6, que explicita rede heterogênica composta por eNodeB do MD conectado e sendo controlado pelo EPC da TELEBRAS. Dessa forma, o MD só iria gerenciar os recursos próprios, como local de instalação dos *sites* e terminais para os usuários. Por outro lado, a TELEBRAS teria a gerência e a configuração de toda a rede, inclusive os *sites* do MD.

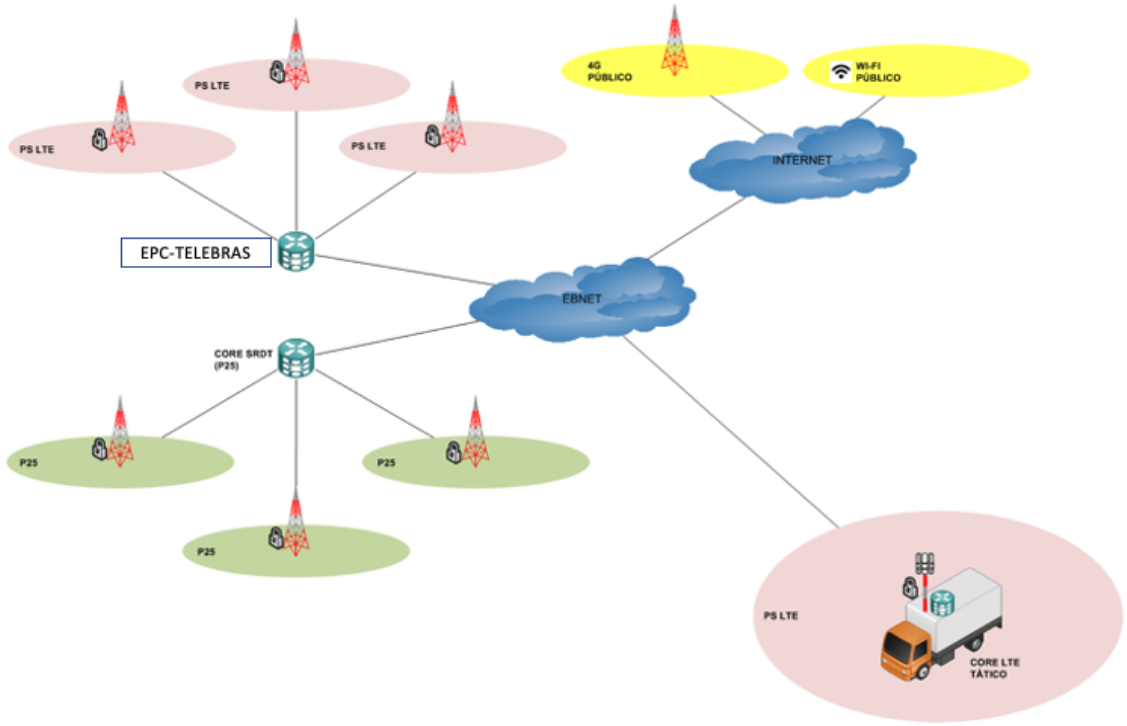

Figura 5.6: Ligação eNodeB ao núcleo da rede
Fonte: Adaptada da Motorola *Solution* (2018)

Em ambos os casos, O MD ficará responsável por fornecer o *backhaul* da ligação de *core* a *core* ou de eNodeB para *core* da TELEBRAS. Os recursos dessa rede não serão compartilhados para utilização civil pois são para a atividade típica do MD.

3) Operações totalmente segregadas e independentes: Nas operações em lugares sem nenhuma cobertura LTE, como Brumadinho - MG, ou operações como no sete de setembro, não haverá necessidade de conexão ao núcleo de rede da TELEBRAS.

Nesse cenário pode ser necessário uma coordenação de compartilhamento de frequências. Esse compartilhamento se dará apenas em localidades com cobertura de telefonia celular, porém a demanda operacional determinará nessa cidade, uma rede totalmente segregada e independente.

A Figura 5.7 apresenta a segregação total entre a operação das redes, explicitando a rede segregada do MD. Essa rede é utilizada em locais onde não há nenhum tipo de cobertura comercial, como por exemplo, em operações tipicamente militares ou em situações de alto grau de congestionamento da rede. Essas redes são instaladas em plataformas comerciais e possibilitam uma rede local estanque e segregada. Nessa rede a gerência, configuração e operação são de responsabilidade do MD.

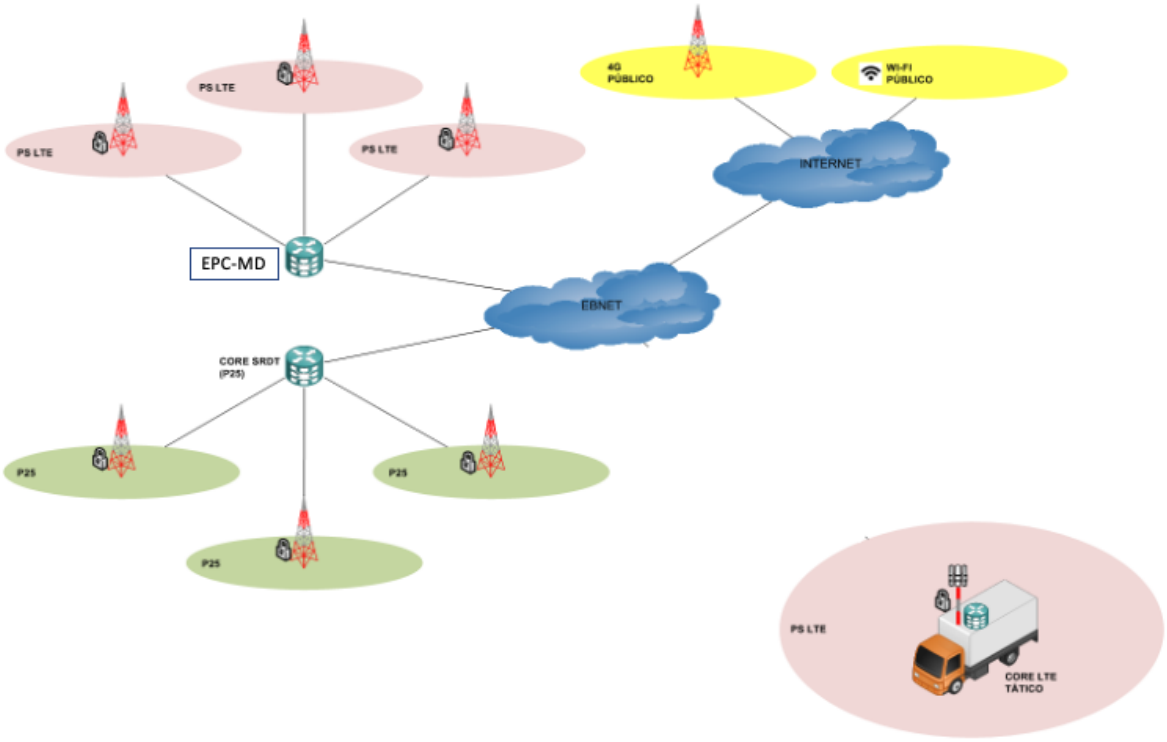

Figura 5.7: Rede segregada e independente
Fonte: Adaptada da Motorola *Solution* (2018)

5.3 Conclusão

Os EUA vêm realizando esforços no sentido de implantar uma rede de comunicações críticas de banda larga por meio da agência FirstNet. Nesse sentido, foram tomadas uma série de medidas, entre elas, o franquiamento da possibilidade de exploração da banda de frequência para essa aplicação, além de um valor para os investimentos iniciais. Nesse contexto, foram levantados vários desafios a serem ultrapassados, tanto na definição do modelo de adesão pelos órgãos, assim como nas possibilidades de expansão da rede. Foram apresentados desafios técnicos dessa implantação. Por apresentar semelhanças com a política adotada no Brasil, foi utilizado o modelo dos EUA para analisar e verificar as possíveis adaptações para implementação dessa rede de banda larga no Brasil.

A partir dessa análise verificou-se a viabilidade de implementação desde que se atente para algumas premissas como o modelo econômico para a implantação, a operação e manutenção dessa rede, a possibilidade de exploração comercial do excedente de banda, a priorização de utilização do sistema por parte dos órgãos, a segurança cibernética da rede e o atendimento aos requisitos de comunicações críticas da 3GPP. Além disso, a

possibilidade de integração com redes proprietárias dos órgãos, nas quais o gerenciamento, configuração e manutenção ficariam por conta desses órgãos.

Essa rede poderá gradativamente substituir a tecnologia LMR pois, como já dito anteriormente, ela pode vir a atender totalmente os serviços que ora só a tecnologia LMR atende.

Finalizando, há grandes vantagens na implantação dessa rede de banda larga, pois por um lado, teremos uma rede com uso dual pela Defesa Nacional e pela sociedade, sendo que do ponto de vista da aplicação operacional para o usuário da Defesa Nacional, seria uma rede proprietária, assim como são as redes LMR com todas as garantias de prioridade de uso, segurança cibernética, confiabilidade e capilaridade.

Por outro lado a operação, manutenção, implantação e expansão da rede seriam de responsabilidade da TELEBRAS a qual realizaria essas tarefas com parte dos lucros da exploração econômica da faixa de frequência desse sistema. Assim, a Defesa Nacional e os órgãos seriam usuários da rede com os privilégios de prioridade da rede. Além disso, a rede teria um alcance mundial pois permitiria acesso a tecnologias 2G, 3G, 4G e 5G. Finalizando, será viável a atualização da tecnologia LMR para a LTE na qual a Defesa Nacional e os órgãos serão usuários da rede, sendo que, essa rede irá atender a todas as necessidades de comunicações críticas, principalmente às de banda larga.

6 Análise dos Testes do Sistema LTE

Foram realizados testes em campo na cidade do Rio de Janeiro e Brasília, para que se pudesse obter resultados da aplicação do sistema de banda larga LTE do EB nas atividades táticas militares.

Esses testes foram realizados de forma institucional, coordenado pela gerência técnica do sistema de C2 do EB e executado pela unidade operacional do sistema de C2. Os testes tiveram como finalidade a verificação das funcionalidades do sistema de banda larga LTE em aplicações militares.

Foram testadas algumas aplicações de banda larga em operações táticas, tais como: *streaming* de vídeo com dispositivos portáteis, tipo *Smartphone*, dispositivos optrônicos/luneta, videoconferência e *drone*. Além disso, testou-se o uso de aplicações institucionais, como o Pacificador, videoconferência e Rede Integrada de Telecomunicações do Exército (RITEx), além disso foi testada a integração entre as redes de comunicações envolvidas (LTE Tático, LTE Fixo, EBNet, Sistema de Radiocomunicação Digital Troncalizado (SRDT), Internet).

6.1 Arquitetura da Rede

O sistema para testes é composto por redes heterogênicas compostas por ERB do sistema P25 e seu controlador *Master Site*, além da eNodeB fixo e tático com seus respectivos EPC. Além disso, utilizou-se o servidor *wave* para realizar a integração das redes P25 e LTE.

Nesse teste foi utilizado o *site* tático LTE que tem a capacidade de ser utilizado em operações onde se necessite de flexibilidade nas questões de áreas de cobertura em locais isolados.

Para viabilizar os testes, foi instalado o sistema *Public Safety LTE* (PS-LTE) em Viatura de C2 do EB com o objetivo de avaliar a operação tática do sistema LTE privado, sua integração às redes de rádio comunicação existentes e a estrutura fixa já instalada.

Os núcleos das redes P25 e LTE utilizam o *bakhal* da EBNet para realização da conexão. Finalizando, no *core* tático estão instalados os servidores de vídeo, entre outros ligados ao EPC tático.

A Figura 6.1 apresenta a arquitetura de redes do teste do LTE à qual é uma rede heterogênica tanto do ponto de vista de tecnologias de banda larga e banda estreita quanto de diversidade de tamanho da *site* LTE.

A elipse vermelha apresenta a área de cobertura de três *sites* fixos LTE, gerenciados por um *core* LTE FIXO (EPC) e um *site* tático LTE gerenciado por um *core* LTE TÁTICO (EPC) que se encontra instalado em uma viatura de C2, ambos privativos de utilização do EB.

A elipse verde representa a área de cobertura do sistema de três *sites* de banda estreita LMR, APCO25 do EB, gerenciados pelo *core* SRDT P25 (*Master Site*).

A elipse amarela representa a área de cobertura do LTE e uma rede *wi-fi* públicos, ou seja uma rede de tecnologia 3GPP e uma rede de tecnologia não 3GPP.

A nuvem da EBNet, que é a Intranet do EB.

A nuvem da INTERNET que conecta à rede interna do EB com a rede mundial de computadores.

Todos os quatros sistemas (LTE privado fixo e móvel, P25, e 4G e *wi-fi* públicos) estão conectados física e logicamente uns aos outros.

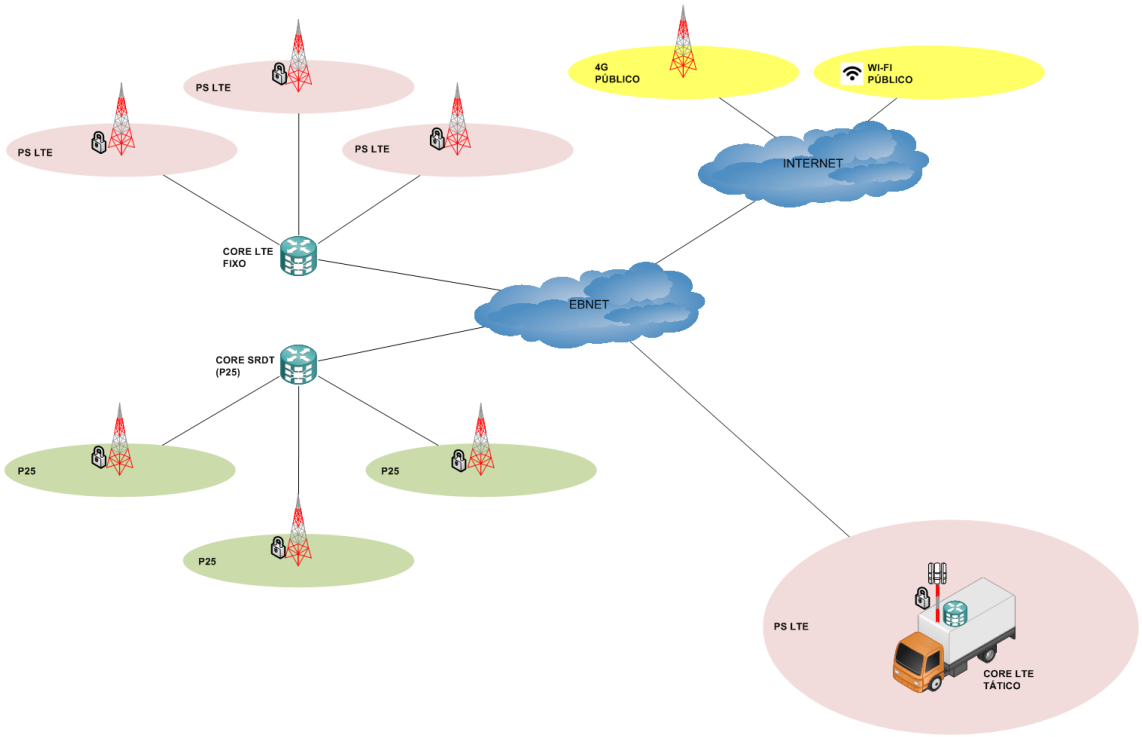

Figura 6.1: Arquitetura do teste LTE

6.2 Aplicações

6.2.1 Distribuição de Vídeo sobre Rede LTE

Transmissão de vídeo em tempo real por intermédio do dispositivo móvel LEX L10. As transmissões serão iniciadas por um ou mais usuários e poderão ser acompanhadas por todos os integrantes da rede, inclusive pelos meios existentes na viatura de C2. Também é possível a transmissão simultânea de vídeo, ou seja, mais de um usuário poderá transmitir o vídeo de uma operação em tempo real para outros usuários e, inclusive, para a central de operações.

Transmissão de vídeo em tempo real por intermédio de *drone* da Companhia de Precursores Paraquedista ou do Sistema do Olho de Águia da Aviação do EB. As imagens geradas poderão ser distribuídas aos militares em incursão na área de combate e/ou para envio ao Centro de Operações em tempo real. Esta ferramenta permitirá operação independente, sem necessidade de infraestrutura física e promoverá mobilidade operacional, com recepção e distribuição das imagens coletadas por optrônicos de alta performance e/ou lunetas dos *snipers*.

Esta possibilidade técnica facultará o envio de imagens nas duas direções, ou seja, imagens coletadas pelos sensores, humanos ou artificiais, para os demais combatentes e Centro de Operações, ou do Centro de Operações para os militares infiltrados em tempo real.

Equipamentos utilizados:

- DIGIFORT: Servidor de vídeo integrado ao EPC;
- *Drone*: sistema de captação de imagens e geração de vídeos em tempo real acoplada a um *drone* que sobrevoa a área a qual se quer fazer as imagens;
- Olho de Águia: sistema de captação de imagens e vídeos em tempo real acoplado a uma aeronave que sobrevoa a área a qual se quer fazer as imagens;
- Dispositivos Optrônicos e/ou Lunetas: dispositivos de uso individual do militar com a capacidade de gerar imagens e vídeos em tempo real.

LEX Distribuição de Vídeo

Esse teste se caracteriza pela captação e distribuição de vídeo por um ou vários dispositivos LTE LEX L10 na área de cobertura do LTE Tático o qual fornece a rede de acesso à Internet e a (EBNet), as quais estão ligadas a uma rede 4G Pública e a rede 4G privada fixa do EB.

A distribuição das imagens nessas redes é viabilizada por meio do servidor de vídeos instalados no LTE tático, o DIGIFORT. Isso possibilita que as autoridades possam acompanhar em tempo real da cabine do LTE Tático ou em qualquer ponto de acesso da EBNet ou internet às operações.

A Figura 6.2 apresenta a rede heterogênica deste teste a qual é composta pelas redes LTE fixa e tática privada do EB e a rede LTE pública.

Na viatura de C2 encontra-se instalado o servidor DIGIFORD, responsável pelo recebimento, armazenamento e distribuição dos vídeos. Foi instalado, também, o mosaico com as imagens das câmeras dos dispositivos LEX captadas em tempo real.

Em termos de conexões tem-se:

- O enlace, não guiado, do LEX na área de cobertura da rede LTE tática ao *core* LTE TÁTICO;
- As rotas entre o *core* LTE TÁTICO e os dispositivos LEX na área de cobertura do LTE privado, assim como os dispositivos LEX na área de cobertura do LTE público.

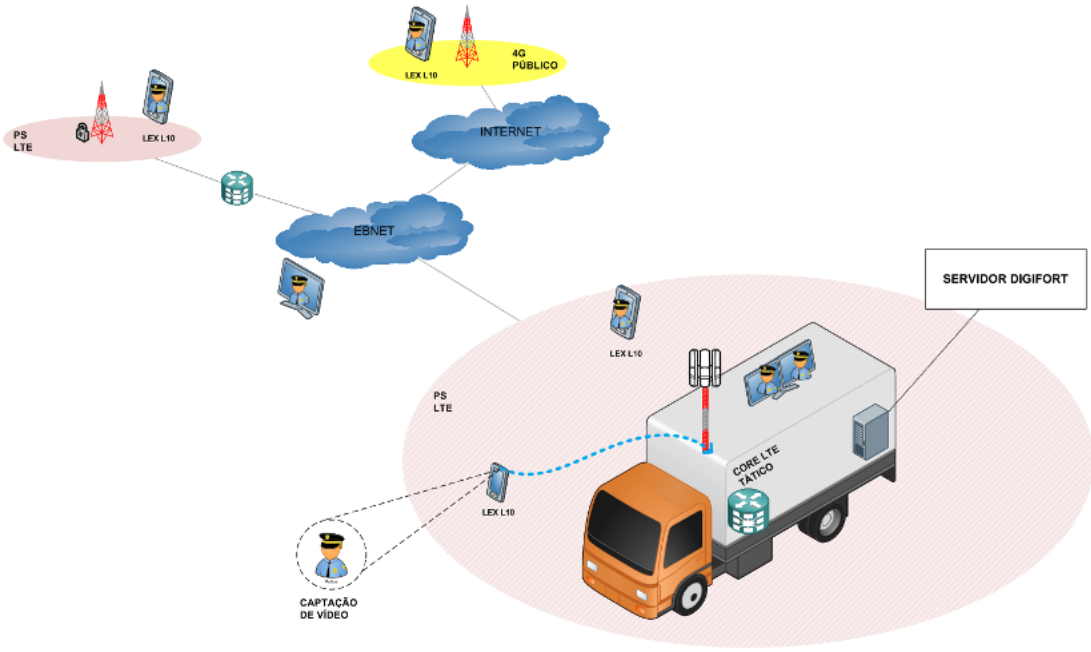

Figura 6.2: Distribuição de Vídeo Lex

- Configuração: Dispositivos LTE LEX L10 com a ferramenta DIGIFORD Cliente; Servidor DIGIFORD embarcado na Viatura de C2 integrado ao *core* LTE Tático.
- Atividades: Rodar DIGIFORD Cliente no LEX L10 conectado a rede PS-LTE Tática; Deslocar com terminal LEX dentro da área de cobertura LTE Tático realizando *streaming* de vídeo de *smartphone* para *smartphone* e de *smartphone* para central de operações.
- Resultado: Usuários podem fazer transmissão de vídeo em tempo real e monitorar o vídeo transmitido por outros usuários através de *smartphone*.

Drone Distribuição de Vídeo

Esse teste se caracteriza pela captação e distribuição de vídeo por dispositivos do tipo *drone*. O *drone* capta a imagem e envia para a estação terrena, e essa por sua vez é conectada a um *modem* LTE ou um dispositivo LTE operando na área de cobertura do LTE Tático o qual fornece a EBNet, as quais estão ligadas a uma rede 4G Pública e a rede 4G privada fixa do Exército. A distribuição das imagens nessas redes é viabilizado por meio do servidor de vídeos instalados no LTE tático o DIGIFORD. Isso possibilita que as autoridades possam acompanhar em tempo real da cabine do LTE Tático ou em qualquer ponto de acesso da EBNet ou internet às operações.

A captação de imagens pelo *drone* tem diversas aplicações além de C2, como por exemplo realização de segurança orgânica em instalações militares e poderia ser utilizado como complemento de serviços de guarda ao quartel.

A Figura 6.3 apresenta a arquitetura semelhante à da Figura 6.2, com a diferença de captação de imagens realizada pelo *drone* e as conexões da rede, onde se tem:

- A rota entre a câmera do *drone* e o *core* LTE TÁTICO;
- As rotas entre o *core* LTE TÁTICO e os dispositivos LEX na área de cobertura do LTE privado, assim como os dispositivos LEX na área de cobertura do LTE público.

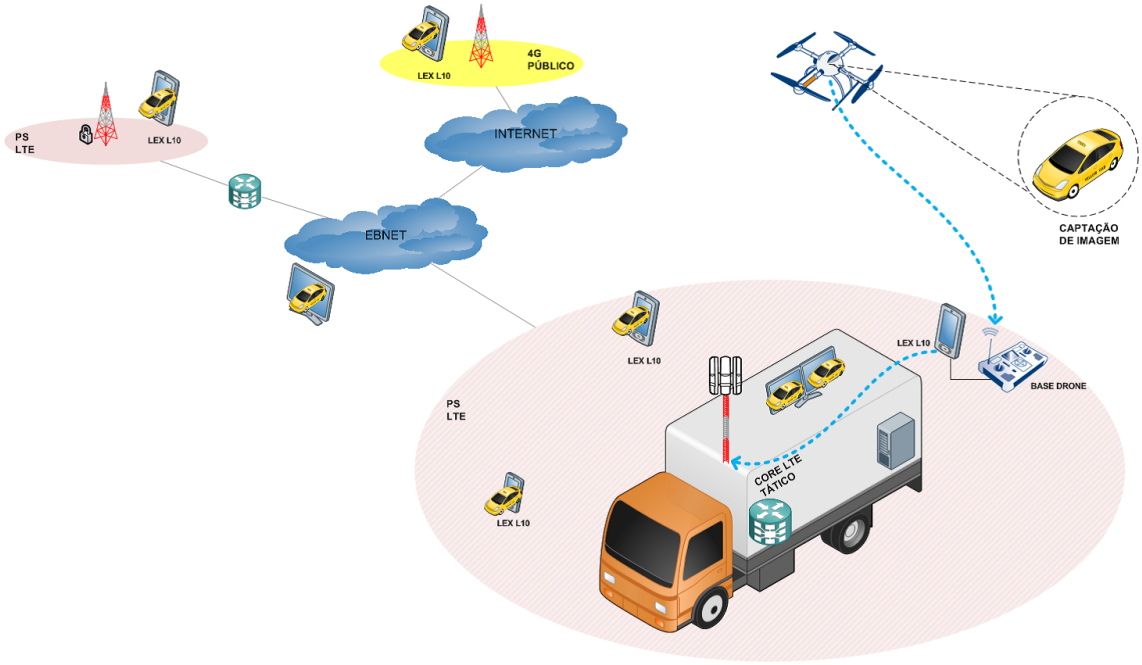

Figura 6.3: Distribuição de Vídeo *Drone*

- Configuração: Dispositivos LTE LEX L10 com a ferramenta cliente de reprodução de vídeo; *Drone* com câmera e capacidade de *streaming* de vídeo; Base de controle de *Drone* com interface *Universal Serial Bus* (USB) e controle por sistema *Android*.
- Atividades: Subir *Drone* e gerar vídeo *streaming* para a base de controle; Redistribuir o vídeo dentro da área de cobertura LTE Tático através do dispositivo LEX L10 acoplado na base do *drone*.
- Resultado: Usuários de *Drone* podem fazer transmissão de vídeo em tempo real para outros usuários através do LEX L10 na rede LTE Tática; Usuários da rede LTE Tática, LTE Fixa, EBNet e Internet são capazes de visualizar o vídeo gerado pelo *Drone*.

Olhos de Águia Distribuição de Vídeo

Esse teste se caracteriza pela captação e distribuição de vídeo um ou vários dispositivos aéreos. O helicóptero capta a imagem e envia para a estação terrena, e essa por sua vez é conectada a um *modem* LTE ou um dispositivo LTE operando na área de cobertura do LTE Tático o qual fornece a EBNet, as quais estão ligadas a uma rede 4G Pública e a rede 4G privada fixa do EB.

A distribuição das imagens nessas redes é viabilizada por meio do servidor de vídeos instalados no LTE tático, o DIGIFORD. Isso possibilita que as autoridades possam acompanhar em tempo real da cabine do LTE Tático ou em qualquer ponto de acesso da EBNet ou internet às operações.

A captação de imagens pelo helicóptero tem diversas aplicações além de C2, como por exemplo a realização de segurança orgânica em instalações militares. A diferença entre o olhos de águia e o *drone* é o alcance maior das imagens que podem ser geradas e enviadas à rede de acesso LTE.

A Figura 6.4 apresenta a arquitetura que é a mesma da figura 6.2 com a diferença de captação de imagens realizada pelo Olhos de águia e as conexões da rede, onde se tem:

- A rota entre o Olhos de águia e o *core* LTE TÁTICO;
- As rotas entre o *core* LTE TÁTICO e os dispositivos LEX na área de cobertura do LTE privado, assim como os dispositivos LEX na área de cobertura do LTE público.

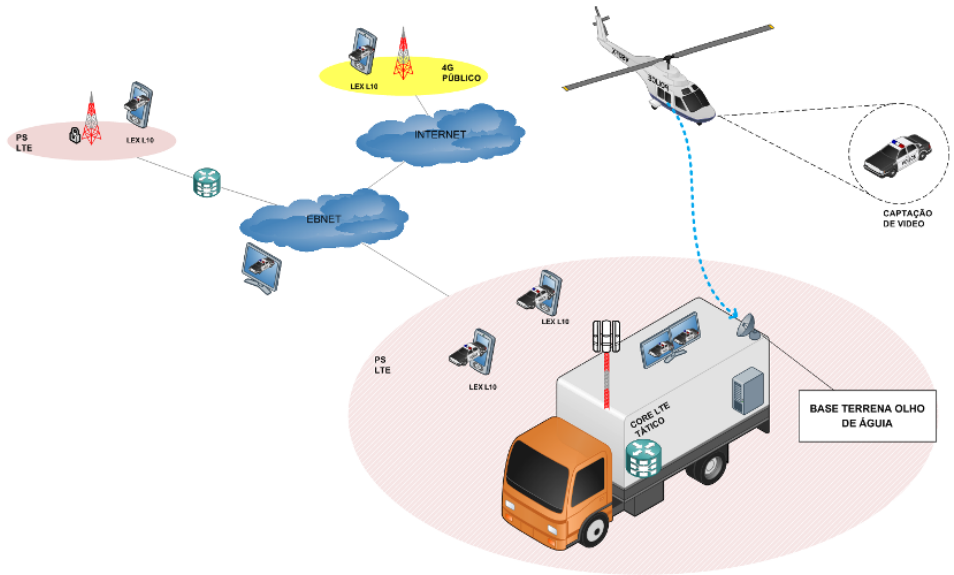

Figura 6.4: Distribuição de Vídeo Olhos de Águia

- Configuração:Dispositivos LTE LEX L10 com a ferramenta cliente de reprodução de vídeo; Aeronave equipada com sistema Olhos de Águia; Base Terrena do sistema Olhos de Águia embarcado na Viatura de C2 integrado ao *core* LTE Tático.
- Atividades: Subir *Drone* e gerar vídeo *streaming* para a base de controle; redistribuir o vídeo dentro da área de cobertura LTE Tático através do dispositivo LEX L10 acoplado na base do *drone*.
- Resultado: Aeronave gera vídeo *streaming* e transmitir para a Base Terrena do Sistema Olhos de Águia; redistribuir o vídeo dentro da área de cobertura LTE Tático através *core* LTE Tático.

Dispositivos Optrônicos/Luneta - Distribuição de Vídeo

Esse teste se caracteriza pela captação e distribuição de vídeo um ou vários dispositivos optrônicos/luneta. Eles captam as imagens e as enviam para um *modem* LTE ou um dispositivo LTE operando na área de cobertura do LTE Tático o qual fornece a rede de acesso à EBNet, as quais estão ligadas a uma rede 4G Pública e a rede 4G privada fixa do Exército.

A distribuição das imagens nessas redes é viabilizada por meio do servidor de vídeos instalados no LTE tático, o DIGIFORD. Isso possibilita que as autoridades possam acompanhar em tempo real da cabine do LTE Tático ou em qualquer ponto de acesso da EBNet ou internet as operações.

A Figura 6.5 apresenta a arquitetura que é a mesma da figura 6.2 com a diferença de captação de imagens realizada pelo optrônico e as conexões da rede, onde se tem:

- A rota entre o optrônico e o *core* LTE TÁTICO;
- As rotas entre o *core* LTE TÁTICO e os dispositivos LEX na área de cobertura do LTE privado, assim como os dispositivos LEX na área de cobertura do LTE público.

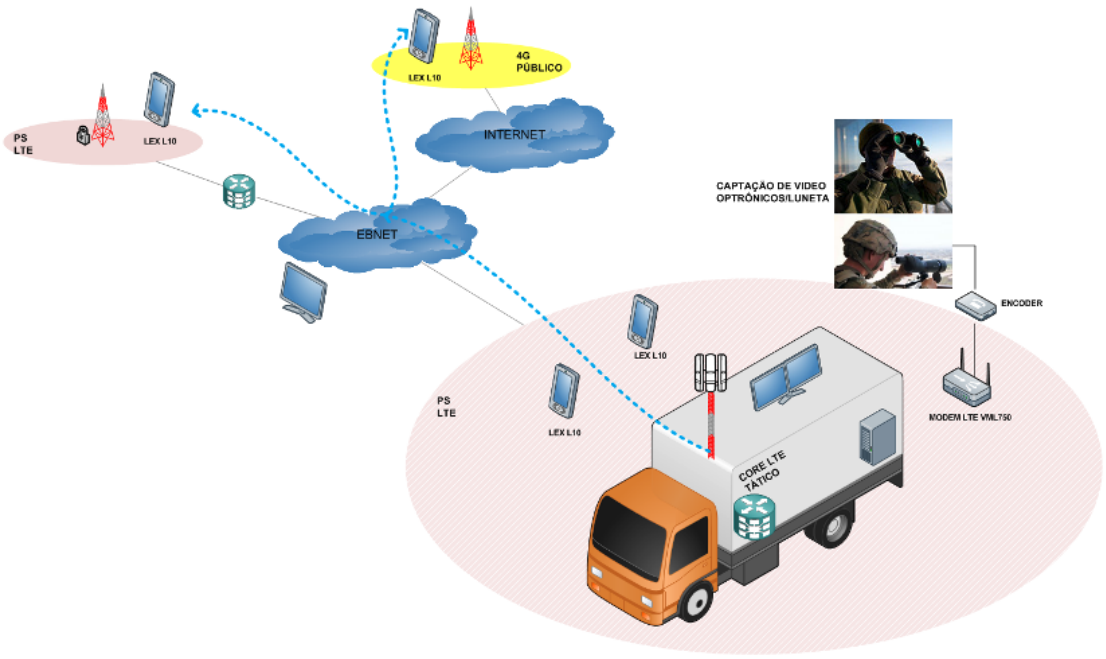

Figura 6.5: Distribuição de Vídeo Optrônicos

- Configuração: Dispositivos LTE LEX L10 com a ferramenta cliente para reprodução de vídeo; Dispositivos optrônicos/ luneta com interface para saída de vídeo; *Encoder* de vídeo com interface de rede IP; *Modem* veicular LTE VML750 para integração com *Encoder* e distribuição de vídeo.
- Atividades: Operador do dispositivo optrônico gera vídeo e acopla no *Encoder*; *Encoder* capta vídeo gerado pelos optrônicos e distribui na rede LTE Tático através do *modem* VML750; O vídeo é redistribuído dentro da área de cobertura LTE Tático através *core* LTE Tático.
- Resultado: Usuários do dispositivo LEX L10 dentro da cobertura LTE Tática podem visualizar a transmissão de vídeo em tempo real gerada pelo dispositivo optrônico; Usuários da rede LTE Fixa, EBNet e Internet, também são capazes de visualizar a transmissão de vídeo através da integração do *core* LTE Tático com a EBNet .

6.2.2 Integração das Redes de Rádio – P25 (SRDT)/LTE *WAVE*, TETRA (LMR) e VHF *Harris*

Interoperabilidade entre a rede LTE , a rede rádio SRDT, rede TETRA, rede *Harris* e a rede celular 4G (LTE Público). Os operadores que estiverem utilizando o dispositivo móvel LEX L10 filiados à rede LTE poderão acompanhar a comunicação dos grupos de conversação criptografados do SRDT, ou de outro órgão durante uma operação inter

agências. Isto acontecerá por intermédio da aplicação de PTT e botão PTT dedicado do LEX L10ig. Estes usuários poderão também se comunicar com os grupos de conversação, trocar mensagens escritas e visualizar a localização dos usuários da rede LTE.

A Figura 6.6 apresenta a arquitetura dessa rede que é composta pelos sistemas LTE privado fixo e móvel, P25, e 4G público. Na viatura tática de C2 estão instalados os equipamentos de interface da rede. São dois os equipamentos de interface:

- O servidor *wave* que faz a interface da rede de banda larga para banda estreita, possibilitando a comunicação via PTT entre as redes. Essas comunicações são tanto para chamadas individuais como para chamadas em grupo. O *wave* possui a arquitetura cliente-servidor, onde o servidor está instalado na viatura tática e o cliente é o dispositivo LEX que hospeda a aplicação do *wave*. Na tela do dispositivo LEX verifica-se o aplicativo *wave* hospedado no cliente LEX;
- A *motobrigdge* que faz a interface entre a rede de banda estreita P25 com a rede de rádios táticos *Harris*.

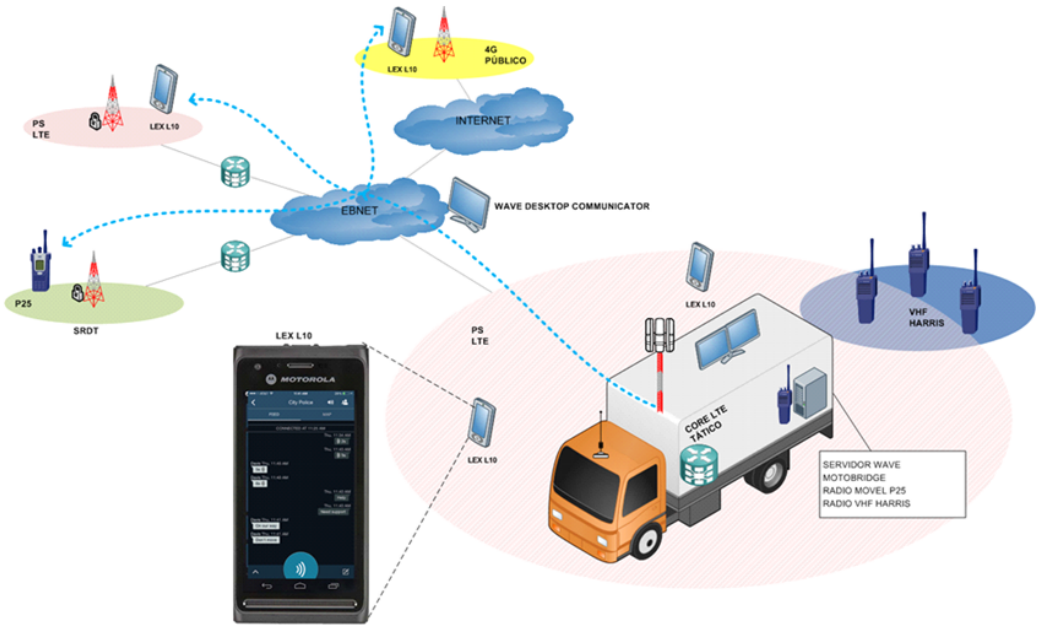

Figura 6.6: Integração de redes rádio

- Configuração: Dispositivos LTE LEX L10 com cliente *WAVE Mobile Communicator*; Dispositivos *Smartphone Android* com cliente *WAVE Mobile Communicator*; Servidor *wave* embarcado na Viatura de C2 integrado ao *core* LTE Tático; *Gateway* de Integração Motobridge com Rádios Donor das redes P25, TETRA e VHF; Rádio

P25 afiliado na cobertura SRDT, Rádios TETRA afiliados na rede Polícia Civil RJ e Rádio VHF *Harris* para comunicação ponto-a-ponto.

- Atividades: Usuário do dispositivo LEX L10 na rede LTE Tática gera chamadas de grupo para as redes P25, TETRA e VHF; Usuário do dispositivo LEX L10 na rede LTE Fixa gera chamadas de grupo para as redes P25, TETRA e VHF; Usuário do dispositivo *smartphone Android* na Internet gera chamadas de grupo para as redes P25, TETRA e VHF; Usuários de rádio das redes P25, TETRA e VHF gera chamada de grupo.
- Resultado: Usuários LEX L10 nas redes LTE Tática, LTE Fixa e Internet são capazes de gerar e receber chamadas de grupo para as redes de rádio P25, TETRA e VHF; Usuários de rádio das redes P25, TETRA e VHF são capazes de gerar e receber chamadas de grupo integrada nas redes LTE e Internet.

6.2.3 Aplicativos Institucionais do EB Pacificador, RITEx, Videoconferência – Aplicativos Institucionais

Utilização em campo dos aplicativos institucionais do EB: Pacificador, RITEx, C2 em Combate e Videoconferência. Cabe ressaltar que, neste último caso, a transmissão por videoconferência permitirá o envio da consciência situacional local em tempo real, por meio do Sistema de Comunicações Militares por Satélite (SISCOMIS) ou EBNet.

Esse teste se caracteriza pela disponibilização dos aplicativos institucionais do EB – Pacificador, RITEx (telefonia IP) e Videoconferência – para os usuário do Viatura de C2 e para o usuários na cobertura LTE Tática através de dispositivos LEX L10.

A Figura 6.7 apresenta os servidores de aplicação que estão na nuvem da EBNet, (RITEx, Pacificador, e Videoconferência), conectadas física e logicamente aos hospedeiros móvel LEX 10. Por ser uma arquitetura cliente-servidor, a aplicação é instalada no LEX 10.

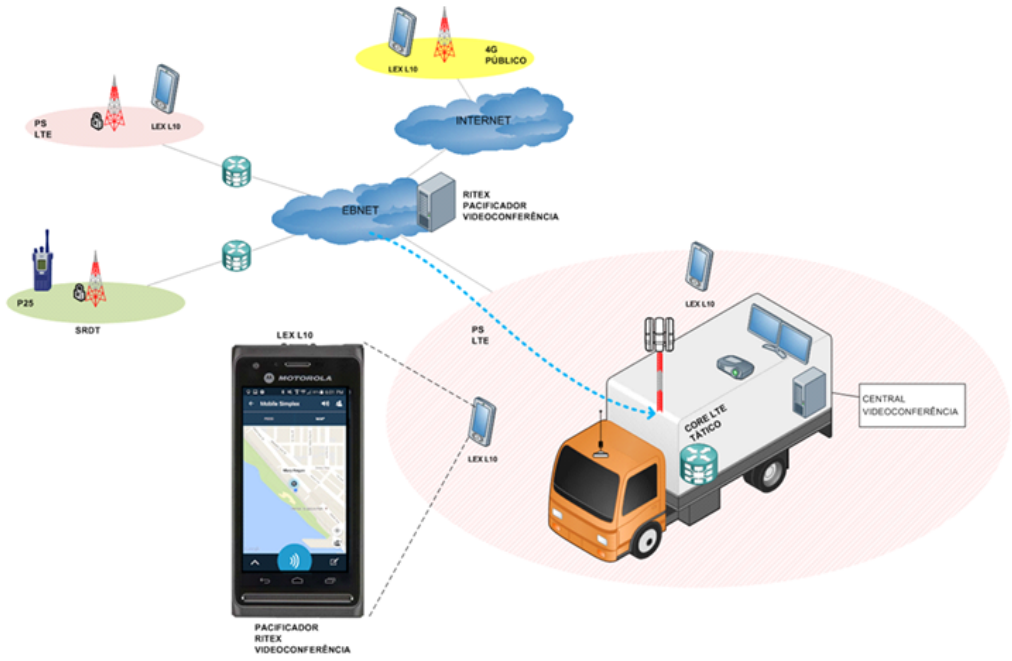

Figura 6.7: Aplicativos EB

- Configuração: Dispositivos LTE LEX L10 com a ferramenta cliente do Pacificador, RITEx e Videoconferência para *Android*; Viatura de C2 integrada a EBNet.
- Atividades: Operador do C2 inicia sessão de videoconferência e acessa Pacificador.
- Usuário do LEX L10 afiliado na rede LTE Tática inicia participação na videoconferência através do aplicativo cliente de videoconferência; Usuário do LEX L10 afiliado na rede LTE Tática aciona aplicativo cliente Pacificador; Usuário do LEX L10 afiliado na rede LTE Tática gera chamada/recebe chamada telefônica através do aplicativo cliente RITEx.
- Resultado: Usuários de *Drone* podem fazer transmissão de vídeo em tempo real para outros usuários através do LEX L10 na rede LTE Tática; Usuários da rede LTE Tática, LTE Fixa, EBNet e Internet são capazes de visualizar o vídeo gerado pelo *Drone*.

Rede Integrada de Telecomunicações do Exército - RITEX

Serviço de acesso à RITEx, no âmbito interno do EB, bem como acesso à rede local de telefonia (Operadora). Essa rede possui um prefixo para a rede interna, começando com o dígito 8 (oito), já a externa não tem um padrão de número definido.

Esse serviço possibilita a realização de chamadas corporativas, internas as organizações militares do EB, sem custo, por todo o território nacional. Possui, também, a possibilidade de realizar e receber ligações externas, se for autorizado pelo administrador das centrais telefônicas. Na região do Rio de Janeiro, o 2º Centro de Telemática de Área (2 CTA) cumpre a missão com duas centrais telefônicas, sendo uma instalada fisicamente no Palácio Duque de Caxias, sem licenças disponíveis, e uma na Estação Transceptora, na Vila Militar, com aproximadamente 50 (cinquenta) licenças. Essas centrais telefônicas encontram-se logicamente instaladas na nuvem da EBNet e podem ser acessadas por qualquer ponto de acesso dessa rede.

Por ocasião do teste do RITEx, o 2 CTA disponibilizou o *software* INTELBRAS IS Mobile e cinco ramais (licenças, válidas por um dia) RITEx, os quais tiveram um excelente desempenho, pois as ligações RITEx RJ – BSB e vice versa ocorreram sem alterações. O prefixo RITEx utilizado nos testes foi o 810 e o prefixo externo utilizado foi o (21) 2519.

A Figura 6.8 apresenta o *software* utilizado para essa comunicação.

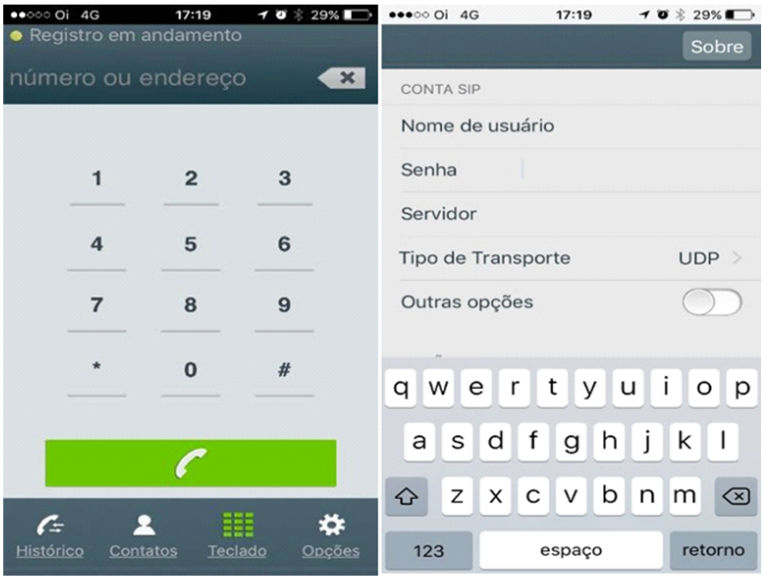

Figura 6.8: *Software* Intelbras IS Mobile

Videoconferência

Serviço que permite a comunicação audiovisual de videoconferência para todos os elementos participante da rede. Nos aparelhos celulares, a videoconferência pode ser realizada através do *software Avaya Scopia Mobile*, disponível para sistemas *android e IOS*. A configuração é simples, pois o usuário só deverá apontar para o IP do *gatekeeper*

(centralizador de *streamings* de vídeo). Por ocasião dos testes, foi possível realizar videoconferências com militares na região de Brasília, utilizando o *gatekeeper* do Comando de Operações Terrestres (COTer), já no Rio de Janeiro, o 2 CTA também disponibilizou seu *gatekeeper*, porém o serviço não pôde ser testado, tendo em vista algumas pendências na liberação do *firewall* daquele Centro.

A Figura 6.9 apresenta o aplicativo *Scopia Mobile* que é a aplicação instalada no hospedeiro móvel para realizar as videoconferências institucionais.

Figura 6.9: Aplicativo Scopia Mobile

Rede Corporativa de Comunicações do Exército (EBNet)

Serviço que permite o acesso à EBNet. Os terminais LEX foram configurados com endereços válidos na rede metropolitana do 2 CTA, possibilitando o acesso à rede de dados e aos serviços corporativos, como se os terminais fossem computadores conectados à uma organização militar. Exemplo de serviços corporativos acessados via rede LTE: Correio eletrônico Zimbra, SPED, Sistema de Boletim (SisBol) etc.

Rede de Dados Corporativa do Exército (INTERNET)

Serviço que possibilita, aos usuários conectados à EBNet, navegar na rede mundial de computadores através do*link* do 2 CTA, oferecendo acesso seguro e confiável.

O acesso seguro à internet é possível através do *software* Sistema de Controle de Acesso de Usuários (SisCAU), desenvolvido pelo 2 CTA, o qual delega para o administrador da rede da organização militar a inclusão de usuários e a atribuição de perfis de acesso. A rede dos terminais LEX (IP pool Lex) foi configurada no *firewall* do 2 CTA e está atrelada ao Batalhão Escola de Comunicações (BEsCom) e, portanto, o administrador do SisCAU do BEsCom está apto a criar usuários para que terminais LEX LTE possam acessar a internet. Por ocasião do reconhecimento, foi feito um acesso ao sítio www.uol.com.br, com o usuário de um integrante da Seção de Tecnologia da Informação do BEsCom.

PTT (*wave*)

Serviço que proporciona a comunicação de voz entre dispositivos LTE, simulando um equipamento rádio, bem como a integração com rádios do SRDT Astro 25, da Motorola Solutions. Ao instalar o aplicativo *wave*, disponível para os sistemas operacionais *android e IOS*, o usuário deverá configurar o servidor e se autenticar no sistema. Após a autenticação, o usuário estará apto a escolher os diversos grupos disponíveis, por exemplo, o grupo EB-RJ *standard*, grupo utilizado na comunicação interna (nos celulares LEX10 LTE), durante os testes no Rio de Janeiro. A infraestrutura de acesso ao servidor *wave* está descrita no diagrama do sistema LTE.

A Figura 6.10 apresenta o aplicativo *wave* que é a aplicação instalada no hospedeiro móvel para realizar as ligações de voz via PTT entre as redes de banda larga para banda larga ou banda estreita para banda larga.

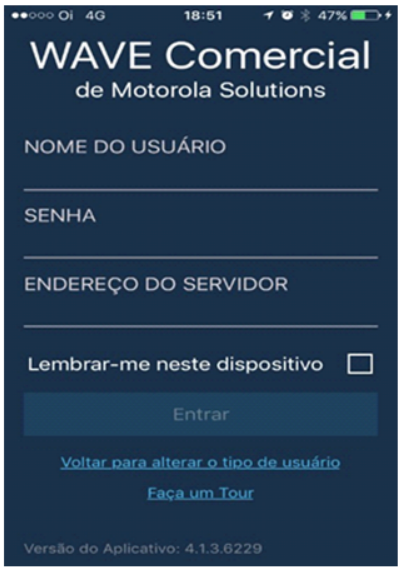

Figura 6.10: Aplicativo *wave*

Pacificador

O Pacificador é um *software* de C2 com a finalidade de apoiar operações de GLO e de defesa/segurança de Grandes Eventos, possibilitando a formação da consciência situacional, a sincronização das ações entre os elementos envolvidos, bem como o tratamento de incidentes ocorridos, sendo que ele possibilita a troca de informação de geoposicionamento entre os militares espalhados no terreno, no caso da utilização do sistema 4G LTE, ou dos militares espalhados no terreno para uma central de operação que pode monitorar a localização dos militares espalhados no terreno em tempo real.

O Sistema Pacificador tem por finalidade apoiar Operações de GLO e de Segurança de Grandes Eventos, possibilitando o incremento da consciência situacional, a sincronização das ações entre os elementos envolvidos, bem como o tratamento de incidentes. Tal sistema baseia-se no conceito de um Centro de Operações, constituído por estrutura física e por pessoal, por sua vez composto de operadores fisicamente localizados nas próprias instalações do Centro de Operações e agentes móveis. O Sistema Pacificador pode ser encontrado sob a forma de "Pacificador Móvel" ou "Pacificador COp". O primeiro possui a arquitetura de redes *Peer-to-peer* (P2P) e a segunda, o cliente-servidor. Na arquitetura cliente-servidor, o servidor hospeda a aplicação do sistema e faz o tratamento das informações de georreferenciamento.

Por ocasião do reconhecimento, a equipe conseguiu acessar o pacificador Cop, através do endereço https onde está instalado o servidor da aplicação. (O celular LEX10 recebeu o servidor *Domain Name System* (DNS) do 2 CTA, através do IP pool do sistema e, portanto, conseguiu resolver nomes). Entretanto, a versão pacificador móvel não funcionou.

EBchat

O Serviço de Mensageria Eletrônica do Exército (EBChat) é um serviço de troca de mensagens exclusivo para militares do EB que possuem conta na Nuvem Privada do EB (EBCloud) (ebcloud.eb.mil.br). Todos os dados são criptografados e as chaves criptográficas são armazenadas em servidor hospedado na infraestrutura do EB. Atualmente, o EBChat é disponibilizado para sistemas operacionais *Android*, pois existem limitações para gerar o aplicativo para o sistema IOS. O referido serviço não foi testado durante os testes no Rio de Janeiro.

6.3 Teste de Cobertura LTE

6.3.1 Área de Cobertura BEsCom *Site* Fixo

O objetivo desse teste é verificar o alcance da rede LTE na qual a eNodeB está instalada no BEsCom, no Rio de Janeiro. Dessa forma, o alcance do *site* foi de aproximadamente 2,35 km sem visada direta para transmissão de *streaming* de vídeos. Nesse sentido, teremos as distâncias do diâmetro de comunicações de 4.7 km.

A Figura 6.11 apresenta área do mapa da Vila Militar no Rio de Janeiro na qual foram realizados os testes. A área sombreada em verde apresenta o cone de cobertura do *site* LTE fixo. Nesse mapa é apresentado também, o perfil do terreno, demonstrando que não havia visada direta entre o ponto de instalação do *site* e o ponto máximo de alcance do teste.

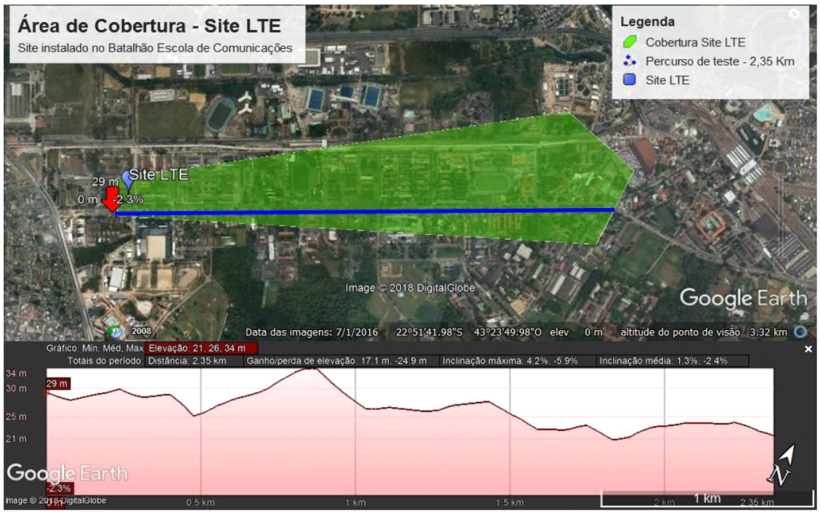

Figura 6.11: Área de Cobertura *site* Fixo

6.3.2 Área de Cobertura BEsCom *Site* Móvel

O objetivo desse teste é verificar o alcance da rede LTE na qual a eNodeB está instalada na viatura de C2. Dessa forma, o alcance do *site* móvel foi de aproximadamente 2,57 km sem visada direta para transmissão de *streaming* de vídeos.

A Figura 6.12 apresenta área do mapa da Vila Militar no Rio de Janeiro na qual foram realizados os testes. A área sombreada em verde apresenta o cone de cobertura do *site* LTE tático. Nesse mapa é apresentado, também o perfil do terreno, demonstrando que não havia visada direta entre o ponto de instalação do *site* e o ponto máximo de alcance do teste.

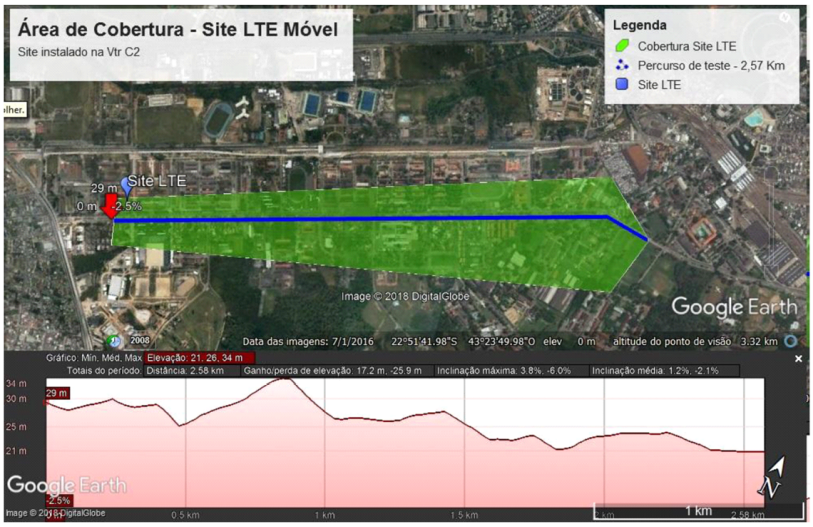

Figura 6.12: Área de Cobertura *site* Móvel

6.4 Teste de desempenho da rede

Esses testes foram realizados na rede LTE instalada em Brasília, composta por cinco eNodeB instalados em Brasília e um EPC instalado no Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx).

A Figura 6.13 apresenta a arquitetura da rede LTE fixa privada do EB. A rede é composta por cinco *sites* LTE gerenciados por um EPC. Essa rede está ligada física e logicamente aos servidores de aplicação (Pacificador, Digiford, DNS, *wave*), hospedados na EBNet.

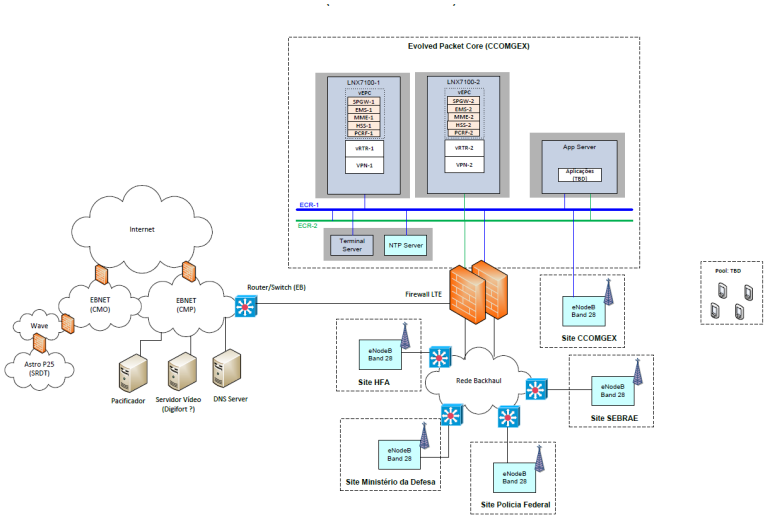

Figura 6.13: Arquitetura da rede LTE Brasília

6.4.1 LTE *downlink* - Teste de *throughput* de *downlink*

Esse teste verificou o *throughput* de *downlink*, nas distâncias em que a SNR atingia o limiar de sensibilidade do terminal. A figura a seguir mostra o local onde foram realizados os testes. Para a SNR maior do que 20.

- Configuração: Servidor IPERF instalado junto ao *core* LXN7100 LEX com *App Magic* IPERF e *G-Net-Track Lite*. Sinal do LTE com SNR $>$ 20.
- Atividades: Deslocar com terminal LEX até local onde há condição de sinal necessários para os testes (SNR $>$ 20).
- Verificar nível de sinal e setor pelo *App G-Net-Track Lite*; Iniciar a aplicação Magic IPERF no LEX como Servidor pelo servidor IPERF conectado ao core LXN7100, iniciar a transmissão de dados usando o IPERF como cliente.

A Figura 6.14 apresenta a configuração no aplicativo IPERF onde o LEX é configurado como servidor, assim, a direção dos dados é do *site* (cliente) para o LEX (servidor).

iperf3 –c 10.134.3x.x -i 1

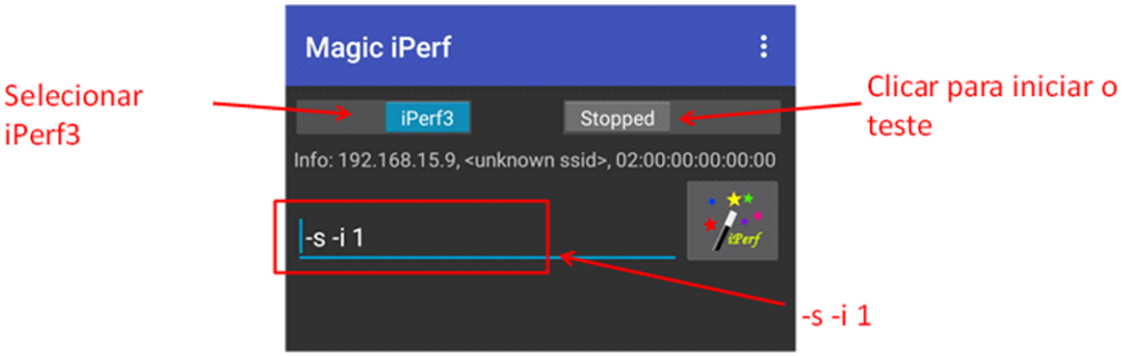

Figura 6.14: Transmissão de dados usando o IPERF como cliente

- Resultado:Velocidade de 10Mbps ou mais.

6.4.2 LTE *uplink* - Teste de *throughput* de *uplink*

Esse teste verificou o *throughput* de *uplink*, nas distâncias em que a SNR atingia o limiar de sensibilidade do terminal.

A figura 6.15 mostra o local onde foram realizados os testes. Para a SNR maior do que 20.

- Configuração: Servidor IPERF instalado junto ao *core* LXN7100 LEX com *App Magic* IPERF e *G-Net-Track Lite*. Sinal do LTE com SNR $>$ 20.
- Atividades: Deslocar com terminal LEX até local onde há condição de sinal necessários para os testes (SNR $>$ 20); Verificar nível de sinal e setor pelo *App G-Net-Track Lite* pelo servidor IPERF conectado ao core LXN7100; iniciar a aplicação o IPERF como servidor iperf3 –s -i 1; Iniciar a transmissão de dados pelo *App Magic* IPERF no LEX. A Figura 6.15 apresenta a configuração no aplicativo IPERF onde o *site* é configurado como servidor, assim, a direção dos dados é do LEX (cliente) para o *site* (servidor).

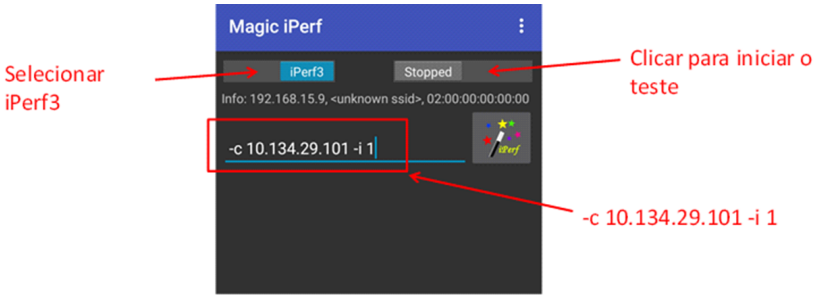

Figura 6.15: Teste de *throughput* de *uplink*

- Resultado:Velocidade de 3 Mbps ou mais.

6.4.3 LTE *downlink* - Teste de capacidade de *downlink* do setor

- Configuração: Servidor IPERF instalado junto ao core LXN7100; três aparelhos LEX com *App Magic* IPERF e G-Net-Track Lite; três aparelhos LEX no mesmo setor da eNodeB Sinal do LTE com SNR > 20.
- Atividades: Deslocar com três terminais LEX até local onde há condição de sinal necessários para os testes (SNR > 20); Checar SNR e setor da eNodeB utilizado pelo LEX através do *App G-Net-Track Lite*; Desligar setores das demais eNodeB caso necessário; Iniciar a aplicação Magic IPERF como Servidor nos três aparelhos LEX; Abrir três sessões no servidor IPERF; Em cada sessão do servidor IPERF iniciar a transmissão de dados usando o IPERF como cliente. A Figura 6.16 apresenta a configuração no aplicativo IPERF onde três aparelhos LEX são configurados como servidores. Nesse caso é atribuída uma porta para cada LEX, ou seja a porta 5201 é atribuída ao LEX 1, a porta 5202 ao LEX 2 e a 5203 ao LEX 3. Assim, a direção dos dados é do *site* (cliente) para os três LEX (servidores).

  iperf3 -c 10.134.x.x -i 1 –p 5201 Sessão 1
  iperf3 -c 10.134.x.x -i 1 –p 5202 Sessão 2
  iperf3 -c 10.134.x.x -i 1 –p 5203 Sessão 3

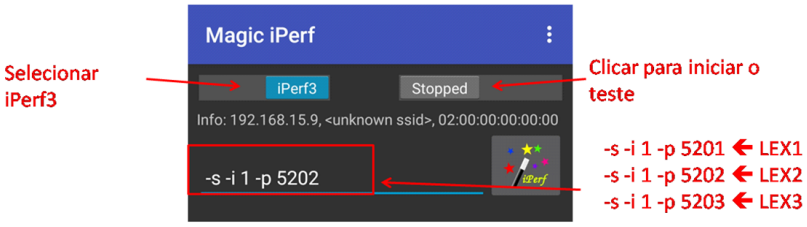

Figura 6.16: Teste de capacidade de *downlink* do setor

- Resultado:Velocidade agregada dos três aparelhos: 22Mbps ou mais.

6.4.4 LTE *uplink* - Teste de capacidade de *uplink* do setor

- Configuração: Servidor IPERF instalado junto ao *core* LXN7100; três aparelhos LEX com *App Magic* IPERF e G-Net-Track Lite; três aparelhos LEX no mesmo setor da eNodeB; Sinal do LTE com SNR > 20.
- Atividades: Deslocar com três terminais LEX até local onde há condição de sinal necessários para os testes (SNR > 20); Checar SNR e setor da eNodeB utilizado pelo LEX através do *App G-Net-Track Lite*; Desligar setores das demais eNodeB, caso necessário; Abrir três sessões no servidor IPERF; Em cada sessão do servidor IPERF iniciar a transmissão de dados usando o IPERF como cliente; Iniciar a transmissão de dados pelo *App Magic* IPERF no 03 LEX. A Figura 6.17 apresenta a configuração no aplicativo IPERF onde o *site* é configurado como servidor. Nesse caso é atribuída uma porta de entrada para cada um dos três LEX. Assim, a direção dos dados é dos três LEX (cliente) para o *site* (servidor).

  iperf3 -s -i 1 –p 5201 Sessão 1
  iperf3 -s -i 1 –p 5202 Sessão 2
  iperf3 -s -i 1 –p 5203 Sessão 3

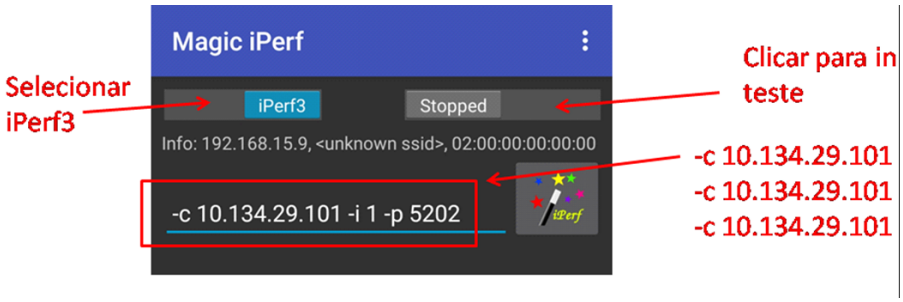

Figura 6.17: Teste de capacidade de *uplink* do setor

- Resultado:Velocidade agregada dos três aparelhos: 11Mbps ou mais.

6.5 Conclusão

Os testes realizados englobaram os testes de aplicação com distribuição de vídeos sobre a rede utilizando diversos dispositivos como o olhos de águia, *drone*, optrônicos e o aparelho LEX 10, integração do LTE com o P25 e os rádios táticos do EB, testes dos aplicativos institucionais do EB, testes de cobertura tanto do *site* fixo quanto do *site* tático móvel. Finalizando, foi realizado o teste de desempenho da rede.

Nesse sentido, comprova-se por meio desses testes que o LTE apresenta uma série de funcionalidades e serviços de banda larga que podem ser utilizados de forma ampla não apenas pelas FA mas também pelos OSP e dessa forma, a tecnologia LTE tem ampla aplicação nos sistemas de C2, nas FA, em particular no EB.

7 Considerações Finais

7.1 Conclusões

Esta dissertação explorou os assuntos relativos a atualização do sistema de banda estreita LMR para um sistema de banda larga LTE para a utilização em comunicações críticas das FA e os OSP. Esse assunto tem a importância fundamentada na questão de que os sistemas LMR não suportam aplicações de banda larga como os serviços de multimídia e dados de alta capacidade. Nesse sentido investigou-se, também, a possibilidade de utilização da tecnologia LTE com uso dual, atendendo as redes de comunicações críticas e a rede de exploração comercial. A dissertação foi realizada em duas etapas distintas, porém complementares.

Na primeira etapa foi realizada uma atividade teórica que investigou as bandas de frequências atribuídas às FA e aos OSP, às redes LMR atuais, os tipos de serviços da rede de banda larga para a Defesa Nacional e OSP, a comparação da tecnologia LTE e LMR, a aplicação operacional da rede LTE pra os projetos do EB, a integração das redes LTE e LMR implementada pelo EB, um estudo de caso da possibilidade de implantação da rede de banda larga LTE compartilhada entre os OSP, FA e a exploração comercial. Nesse estudo foi utilizando, como modelo, a implantação realizada nos EUA com as adaptações para o Brasil. Tudo isso apresentado nos capítulos 2 ao 5.

Na segunda etapa, foram realizados testes práticos, com o objetivo de comprovar as aplicações da rede de banda larga em proveito das necessidades de comunicações de banda larga da Defesa, em particular, o EB, nesse sentido, foram realizados diversos tipos de testes como os de alcance, taxa de dados por setor, serviços de multimídia, distribuição de vídeos e dados pela rede, e finalizando a utilização dos aplicativos institucionais. Tudo isso apresentado no capítulo 6.

Nesse contexto, a dissertação chegou as seguintes conclusões:

- Existe aplicabilidade para os serviços de banda larga para as comunicações críticas em redes da Defesa Nacional e segurança pública, conforme apresentado no capítulo

3;

- Existe a possibilidade de integração entre as redes LTE e LMR e ela já foi implementada pela Defesa Nacional, em particular no EB. Dessa forma, as duas redes podem coexistir, conforme apresentado no capítulo 4;
- Existe grande vantagem na utilização da tecnologia LTE para a Defesa Nacional e segurança pública, conforme apresentado no capítulo 3;
- Existe previsão de utilização dessa tecnologia nos projetos da Defesa Nacional, em particular no EB, conforme apresentado no capítulo 3;
- Existe a possibilidade de utilização das redes LTE de forma compartilhada entre a Defesa Nacional, em particular no EB, segurança pública e a exploração comercial, com o excedente de banda, conforme apresentado no capítulo 5;
- O LTE pode prover os serviços de banda estreita, LMR, ressalvados alguns desafios técnicos, conforme apresentado no capítulo 3;
- O LTE pode se tornar a rede de banda larga unificada e compartilhada entre a Defesa Nacional, em particular no EB e nos OSP, possibilitando uma comunicação integrada entre os órgãos públicos, conforme apresentado no capítulo 3;
- O LTE efetivamente é a possibilidade para as entidades governamentais, nos três níveis, adotarem uma rede unificada com serviços de banda larga de alta capacidade de dados e, ao mesmo tempo, manter a segregação lógica das redes de cada entidade, como apresentado no capítulo 3;
- Existem testes práticos que comprovam a funcionalidade da rede de banda larga LTE nos projetos da Defesa Nacional, em particular no EB, conforme apresentado no capítulo 6.

7.2 Investigações Futuras

Finalmente, podem ser sugeridos alguns tópicos para trabalhos futuros que darão continuidade ao estudo desenvolvido neste projeto. São eles:

- Funcionalidades como ProSe para comunicação de dispositivo a dispositivo sem passar pelo núcleo da rede;
- Diminuição na latência dos serviços de voz PTT;
- Otimização do serviço de voz para comunicações em grupo GCSE;

- Segurança cibernética nas redes heterogênicas nas quais os OSP e FA são apenas usuários do serviço;
- Mecanismos tecnológicos de garantia de prioridade na utilização de uma rede compartilhada;
- Redes heterogêneas baseadas em eNodeB aéreos eNodeB;
- Utilização de sistemas de satélite para fornecer conexão de *backhaul* que fornece acesso LTE aos UE;
- Interoperabilidade de dados entre as redes LMR e LTE.

Referências

[1] Couto, Marcos M e Alberto G Guimarães: *Faixa 5 + 5 mhz para uso na segurança pública no brasil: estudo de casos.* XL Simpósio Brasileiro de Telecomunicações e Processamento de Dados, 2022. 2, 13

[2] Holma, Harri e Antti Toskala: *LTE for UMTS: OFDMA and SC-FDMA based radio access.* John Wiley & Sons, 2009. 11

[3] Moore, Linda KS: *The first responder network (firstnet) and next-generation communications for public safety: Issues for congress*, 2016. 13, 43, 48

[4] NETO, JA de O: *Bridging the digital gap by Universal MBB Service.* HUAWEI, 2013. 15

[5] DA TRINDADE, UEINI CARDOSO: *Estudo sobre a capacidade de cobertura da tecnologia de 4ª geração-long term evolution (lte)-no teatro de operações rural.* O Comunicante, 9(3):44–56, 2019. 15

[6] McGee, Andrew R, Matthieu Coutière e Maria E Palamara: *Public safety network security considerations.* Bell Labs Technical Journal, 17(3):79–86, 2012. 16

[7] Swales, Simon C, Mark A Beach, David J Edwards e Joseph P McGeehan: *The performance enhancement of multibeam adaptive base-station antennas for cellular land mobile radio systems.* IEEE Transactions on Vehicular Technology, 39(1):56–67, 1990. 16

[8] Gupta, Someshwar C, R Viswanathan e R Muammar: *Land mobile radio systems-a tutorial exposition.* institutional repository at Southern Illinois University, 1985. 16

[9] Fantacci, Romano, Francesco Gei, Dania Marabissi e Luigia Micciullo: *Public safety networks evolution toward broadband: Sharing infrastructures and spectrum with commercial systems.* IEEE communications magazine, 54(4):24–30, 2016. 17

[10] Carla, Lorenzo, Romano Fantacci, Francesco Gei, Dania Marabissi e Luigia Micciullo: *Lte enhancements for public safety and security communications to support group multimedia communications.* IEEE Network, 30(1):80–85, 2016. 18

[11] Kumbhar, Abhaykumar, Farshad Koohifar, Ismail Güvenç e Bruce Mueller: *A survey on legacy and emerging technologies for public safety communications.* IEEE Communications Surveys & Tutorials, 19(1):97–124, 2016. 19, 20, 22

[12] Kumbhar, Abhaykumar e Ismail Güvenç: *A comparative study of land mobile radio and lte-based public safety communications.* Em *SoutheastCon 2015*, páginas 1–8. IEEE, 2015. 19, 21

[13] Freire, Débora Vanessa Campos e Ana Clara Cândido: *O aspecto informacional no levantamento de cenários para comunicações críticas em segurança pública no brasil.* Revista Conhecimento em Ação, 5(2):76–97, 2020. 21

[14] Knoll, Thomas Martin: *A combined capex and opex cost model for lte networks.* Em *2014 16th International Telecommunications Network Strategy and Planning Symposium (Networks)*, páginas 1–6. IEEE, 2014. 22

[15] Ahumada Torres, Yesid Alexander e Andrés Saúl Moreno Martínez: *Banda larga móvel privada e sua interacção com as redes de voz da polícia.* Revista Logos Ciencia & Tecnología, 14(1):87–100, 2022. 22

[16] Lin, Xingqin, Jeffrey G Andrews, Amitabha Ghosh e Rapeepat Ratasuk: *An overview of 3gpp device-to-device proximity services.* IEEE Communications Magazine, 52(4):40–48, 2014. 22

[17] Alam, Muhammad, Du Yang, Jonathan Rodriguez e Raed A Abd-Alhameed: *Secure device-to-device communication in lte-a.* IEEE Communications Magazine, 52(4):66–73, 2014. 23

[18] Sakano, Toshikazu, Zubair Md Fadlullah, Thuan Ngo, Hiroki Nishiyama, Masataka Nakazawa, Fumiyuki Adachi, Nei Kato, Atsushi Takahara, Tomoaki Kumagai, Hiromichi Kasahara *et al.*: *Disaster-resilient networking: a new vision based on movable and deployable resource units.* IEEE Network, 27(4):40–46, 2013. 24

[19] Amadeo, Marica, Giuseppe Araniti, Antonio Iera e Antonella Molinaro: *A satellite-lte network with delay-tolerant capabilities: design and performance evaluation.* Em *2011 IEEE Vehicular Technology Conference (VTC Fall)*, páginas 1–5. IEEE, 2011. 25

[20] Chandrasekharan, Sathyanarayanan, Karina Gomez, Akram Al-Hourani, Sithamparanathan Kandeepan, Tinku Rasheed, Leonardo Goratti, Laurent Reynaud, David Grace, Isabelle Bucaille, Thomas Wirth *et al.*: *Designing and implementing future aerial communication networks.* IEEE Communications Magazine, 54(5):26–34, 2016. 25

[21] Gomez, Karina, Sithamparanathan Kandeepan, Macia Mut Vidal, Vincent Boussemart, Raquel Ramos, Romain Hermenier, Tinku Rasheed, Leonardi Goratti, Laurent Reynaud, David Grace *et al.*: *Aerial base stations with opportunistic links for next generation emergency communications.* IEEE Communications Magazine, 54(4):31–39, 2016. 25

[22] Paulson, Anna e Thomas Schwengler: *A review of public safety communications, from lmr to voice over lte (volt e).* Em *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, páginas 3513–3517. IEEE, 2013. 25

[23] Reynaud, Laurent, Karina Gomez Chavez e Tomaso de Cola: *Quality of service for lte public safety networks with satellite backhaul.* Em *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, páginas 1–6. IEEE, 2016. 25

[24] Muraoka, Kazushi, Jun Shikida e Hiroto Sugahara: *Feasibility of capacity enhancement of public safety lte using device-to-device communication.* Em *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, páginas 350–355. IEEE, 2015. 26

[25] Antunes, Emerson de O, Marcos F Caetano, Marcelo A Marotta, Aleteia Araujo, Lucas Bondan, Rodolfo I Meneguette e Geraldo P Rocha Filho: *Soluções otimizadas para o problema de localização de máxima cobertura em redes militarizadas 4g/lte.* Em *Anais do XXVI Workshop de Gerência e Operação de Redes e Serviços*, páginas 152–165. SBC, 2021. 26

[26] Antunes, Emerson de Oliveira: *Soluções otimizadas para implantação de redes militarizadas 4g/lte com máxima cobertura e mínima interferência.* Repositório Institucional da Universidade de Brasília, 2022. 27

[27] Motorola, I: *Long term evolution (lte): A technical overview.* Motorola. Retrieved, 2009. 34

[28] Olsson, Magnus, Catherine Mulligan, Stefan Rommer, Shabnam Sultana e Lars Frid: *SAE and the Evolved Packet Core: Driving the mobile broadband revolution.* Academic Press, 2009. 36, 42

[29] Phunchongharn, Phond, Ekram Hossain e Dong In Kim: *Resource allocation for device-to-device communications underlaying lte-advanced networks.* IEEE wireless communications, 20(4):91–100, 2013. 36, 42

[30] Authority, First Responder Network: *Firstnet.* Reston, VA: First Responder Network Authority. http://www. firstnet. gov/about, 2018. 36, 43, 44

[31] Ferrus, Ramon, Oriol Sallent, Gianmarco Baldini e Leonardo Goratti: *Lte: the technology driver for future public safety communications.* IEEE Communications Magazine, 51(10):154–161, 2013. 37

[32] Biglieri, Ezio, Robert Calderbank, Anthony Constantinides, Andrea Goldsmith, Arogyaswami Paulraj e H Vincent Poor: *MIMO wireless communications.* Cambridge university press, 2007. 37

[33] Díaz Zayas, Almudena, Cesar A García Pérez, Álvaro M Recio Pérez e Pedro Merino: *3gpp evolution on lte connectivity for iot.* Em *Integration, Interconnection, and Interoperability of IoT Systems*, páginas 1–20. Springer, 2018. 38

[34] Hamid, Nafiz Imtiaz Bin, Mohammad T Kawser e Md Ashraful Hoque: *Coverage and capacity analysis of lte radio network planning considering dhaka city.* International Journal of Computer Applications, 46(15):49–56, 2012. 40

[35] Doumi, Tewfik, Mike F Dolan, Said Tatesh, Alessio Casati, George Tsirtsis, Kiran Anchan e Dino Flore: *Lte for public safety networks*. IEEE Communications Magazine, 51(2):106–112, 2013. 41

[36] Kruger, Lennard G: *The first responder network (firstnet) and next-generation communications for public safety: Issues for congress*. Congressional Research Service, 2017. 43

[37] Gallagher, Jill C: *The first responder network (firstnet) and next-generation communications for public safety: Issues for congress*. Congressional Research Service, 2018. 44, 45, 49, 52

[38] Desourdis Jr, Robert I, Rob Dew, Mark O'Brien e Holger Hinsch: *Building the FirstNet Public Safety Broadband Network*. Artech House, 2015. 44

[39] Goldstein, Mark L: *Firstnet: Efforts to establish the public-safety broadband network, statement of mark l. goldstein, director, physical infrastructure issues, testimony before the subcommittee on communications, technology, innovation and the internet, committee on commerce, science, and transportation, us senate*. Em *United States. Government Accountability Office*, número GAO-17-702T em *A*. United States. Government Accountability Office, 2017. 45

[40] Morison, KP e J Calahorrano: *Firstnet case study: How firstnet deployables are supporting public safety*. Em *Police Executive Research Forum, Oct*, 2020. 46

[41] Ricardo[1], Jose e Ugo Dias: *Protocolos de autenticação e controle de acesso para aplicação das forças armadas e Órgãos de segurança pública em redes móveis 4g/lte e 5g*. Revista Ibérica de Sistemas e Tecnologias de Informação. Ed. E49, 2022. 54