Terminal Web Multi-Rede Rádio Tático

João Gabriel Vieira Félix

Dissertação para obtenção do Grau de Mestre em

Engenharia Eletrotécnica e de Computadores

Orientador(es): Professor Doutor João Nuno de Oliveira e Silva
Capitão de Transmissões (Eng) Tiago Filipe Abreu Moura Guedes

Júri

Presidente: Prof. Doutor José Eduardo Charters Ribeiro da Cunha Sanguino
Orientador: Professor Doutor João Nuno de Oliveira e Silva
Vogais: Professor Doutor António Manuel Raminhos Cordeiro Grilo
Capitão de Transmissões (Eng) Luís Filipe Xavier Cavaco de Mendonça Dias

Novembro de 2018

Declaro que o presente documento é um trabalho original da minha autoria e que cumpre todos os requisitos do Código de Conduta e Boas Práticas da Universidade de Lisboa.

Agradecimentos

Quero agradecer à minha família, por me apoiar sempre ao longo deste percurso. Pela educação, princípios e pelos valores que me acompanharam ao longo do meu crescimento como pessoa.

Ao Professor Doutor João Silva por ter estado disponível em inúmeras situações, prestando o seu apoio através do seu vasto conhecimento. A sua ajuda foi motivadora durante todo o trabalho desenvolvido, orientando-me de forma a que conseguisse melhorar as minhas capacidades e atingir os objetivos propostos.

Ao Capitão de Transmissões Paraquedista Tiago Guedes, por me ter incentivado a escolher este tema. A sua ajuda foi basilar para o enquadramento e investigação de aspetos de carácter militar presentes nesta dissertação.

Aos militares da equipa de apoio em engenharia para o projeto sistema de informação e comunicações tático, em Paço de arcos, por toda a disponibilidade.

A todos os meus amigos que durante este tempo acompanharam o desenrolar deste projeto e me incentivaram até o concluir.

Resumo

Atualmente, no Exército Português, quando uma subunidade militar quer comunicar com redes rádio tem de estar fisicamente localizada junto aos rádios que estão a receber/transmitir as comunicações. Na presente dissertação, são abordadas as dificuldades de natureza militar relativas às comunicações. O P/PRC 525 é o rádio tático utlizado nestas comunicações.

Foi então proposto uma solução que facilite o acesso às comunicações e a informação relevante, permitindo assim uma descentralização de recursos humanos e a um requerimento menor de meios materiais. É então uma motivação permitir a vários utilizadores o fator flexibilidade, possibilitando-lhes a comunicação tática a grandes distâncias, assim como a realização de configurações das comunicações à distância.

Sendo a interoperabilidade uns dos fatores que teve mais importância no desenvolvimento desta dissertação, chegou-se à conclusão que a melhor tecnologia a ser usada é voz sobre IP (VoIP). A esta tecnologia utilizou-se WebRTC que permite a comunicação em tempo real através de browsers.

Foi então desenvolvido um sistema, que oferece aos militares uma ferramenta para o controlo de comunicações. Este sistema é composto por dois servidores, um servidor de sinalização que permite o estabelecimento de comunicações e um servidor que contém a restante parte do sistema. O servidor executa troca de informação com rádios militares, nomeadamente o P/PRC 525, assim como a gestão de páginas web.

A solução proposta permite efetuar comunicações com atrasos relativamente baixos em relação à comunicação normal, rádio-rádio, pelo que o sistema desenvolvido apresenta viabilidade para ser utilizado no Exército.

Palavras-chave: Exército Português; Comunicações; Descentralização; Interoperabilidade; Rádio;

Abstract

Currently, in the Portuguese Army, when a military subunit wants to communicate with radio networks it must be physically located next to the radios that are receiving/transmitting the communications. In this dissertation, the military difficulties related to communications are addressed. The P/PRC 525 is the tactical radio used in these communications.

A solution was then proposed that facilitates access to communications and relevant information, thus allowing decentralization of human resources and a lower requirement of material means. It is then a motivation to allow several users the flexibility factor, enabling them to communicate tactically over great distances, as well as making communications configurations at a great distance.

As the interoperability is one of the factors that had more importance in the development of this dissertation, it was concluded that the best technology to be used is voice over IP (VoIP). This technology was used WebRTC that allows the communication in real time through browsers.

A system was developed that offers the military a tool for controlling communications. This system consists of two servers, a signaling server that allows the establishment of communications and a server that contains the remaining part of the system. The server performs exchange of information with military radios, namely the P/PRC 525, as well as the management of web pages.

The proposed solution allows to make communications with relatively low delays in relation to the normal communication, radio-radio, reason why the developed system presents viability to be used in the Army.

Keywords: Portuguese Army; Communications; Decentralization; Interoperability; Radio

Índice

AGRADECIMENTOS V

RESUMO VII

ABSTRACT IX

ÍNDICE XI

LISTA DE FIGURAS XV

LISTA DE TABELAS XVII

LISTA DE SIGLAS E ACRÓNIMOS XIX

1. INTRODUÇÃO 1

1.1 ENQUADRAMENTO DO PROBLEMA E MOTIVAÇÃO 1

1.2 PROBLEMÁTICA – SITUAÇÃO ATUAL 2

1.3 PROPOSTA DE SOLUÇÕES 4

1.4 ESTRUTURA DO DOCUMENTO 5

2. TRABALHO RELACIONADO 7

2.1 REDES TÁTICAS 7

2.1.1 COMPONENTE DE COMUNICAÇÕES - SITACO 7

2.1.2 COMPONENTE DE INFORMAÇÃO 10

2.2 RÁDIO TÁTICO P/PRC 525 10

2.2.1 MODOS ESPECIAIS DE COMUNICAÇÃO 11

2.2.2 INTERFACES 12

2.3 VOIP 13

2.3.1 SINALIZAÇÃO DE CHAMADAS 14

2.3.2 PROTOCOLOS DE COMPRESSÃO ÁUDIO COMUNS EM VOIP 18

2.3.3 PROTOCOLOS DE TRANSPORTE 19

2.3.4 COMUNICAÇÃO SOBRE WEB 20
2.4 VOIP NO P/PRC 525 21
2.5 SISTEMAS DE SUPORTE PARA SINALIZAÇÃO DE CHAMADAS 24
2.5.1 ASTERISK 24
2.5.2 GNU *GATEKEEPER* 25
2.5.3 BIBLIOTECAS VOIP 25
2.5.4 GSTREAMER 26
2.5.5 AVALIAÇÃO 26

3. VOI525 29

3.1 CASOS DE USO 29
3.1.1 CAMPANHA 29
3.1.2 INSTALAÇÕES FIXAS 30
3.1.3 CONTROLO DE ACESSOS 31
3.2 FUNCIONALIDADES 31
3.2.1 INQUÉRITOS 31
3.2.2 REQUISITOS 32
3.2.2.1 Funcionais 32
3.2.2.2 Segurança 32
3.2.2.3 Interoperabilidade 33
3.3 PROPOSTA DE IMPLEMENTAÇÃO 33
3.4 TRABALHO DESENVOLVIDO 34
3.4.1 TECNOLOGIAS 34
3.4.2 PROCESSAMENTO DE ÁUDIO 35
3.4.3 SINALIZAÇÃO 35
3.4.4 CONTROLO RÁDIO 38
3.4.5 HARDWARE DE LIGAÇÃO 39
3.4.6 INTERFACE GRÁFICA 41
3.5 DEMONSTRAÇÃO 43
3.5.1 ALE3G EM FUNCIONAMENTO 43
3.5.2 TESTES DE CAMPO 45
3.6 AVALIAÇÃO 46
3.6.1 TESTE FUNCIONAMENTO BROWSER 47
3.6.2 QUALIDADE DA COMUNICAÇÃO 47

3.6.3 ATRASOS NA COMUNICAÇÃO 49
3.6.4 QUALITATIVA 54
3.7 VALIDAÇÃO DOS REQUISITOS 56

4. DISCUSSÃO 59

5. CONCLUSÃO E TRABALHOS FUTUROS 61

6. REFERÊNCIAS 63

7. ANEXOS I

7.1 ANEXO A – INQUÉRITOS INICIAIS I
7.2 ANEXO B – ESPECIFICAÇÕES DO CABO RG400 V
7.3 ANEXO C – INQUÉRITOS FINAIS VI

Lista de Figuras

Figura 1.1- Funcionamento atual das redes Rádio no Exército Português. 3
Figura 1.2 - Proposta de solução nas redes Rádio do Exército Português. 5
Figura 2.1 Subsistema de Comunicações do SIC-T, baseado em [6]. 8
Figura 2.2 - O SIC-T e os seus subsistemas [6]. 9
Figura 2.3 - Ligação via Ethernet. 13
Figura 2.4 – Protocolos de sinalização VoIP [12]. 14
Figura 2.5 - Arquitetura SIP [14]. 15
Figura 2.6 – Exemplo de Fluxo SIP [48]. 16
Figura 2.7 - Exemplo de troca de protocolos do H.323 [15]. 17
Figura 2.8 - Exemplo da utilização de WebRTC [25]. 20
Figura 2.9 - Exemplo de utilização de WebSocket [49]. 21
Figura 2.10 - Exemplo de rede rádio VoIP ligada apenas a uma rede rádio. 22
Figura 2.11 - Exemplo da ligação entre uma rede rádio ligada a uma rede VoIP utilizando um rádio Gateway que se liga à rede IP. 22
Figura 2.12 – Sistema tipo de comunicações de veículos com ICC-201 [30]. 24
Figura 3.1 - Exemplo Posto de Comando [47]. 29
Figura 3.2 - Índices de atenuações para o cabo RG400 [40]. 30
Figura 3.3 - Exemplo da implementação. 33
Figura 3.4 - Exemplo da arquitetura Web. 34
Figura 3.5 – Exemplo de troca de candidatos. 36
Figura 3.6 - Sinalização das chamadas entre dois terminais 37
Figura 3.7 - Trocas de candidatos ICE. 38
Figura 3.8 - Exemplo de como é exibido ao utilizador as informações obtidas do rádio tático. 39
Figura 3.9 - Legenda painel frontal rádio tático P/PRC 525. 40
Figura 3.10 - Legenda dos componentes do cabo adaptado. 40
Figura 3.11 - Legenda cabo DB9 RS232 [43]. 41
Figura 3.12 - Parte macho do cabo de dados adaptado. 41
Figura 3.13 - Hierarquia de menus. 41
Figura 3.14 - Exemplo chamada em ALE3G. 42
Figura 3.15 - Exemplo de lista com destinatários no modo ALE3G. 43
Figura 3.16 - Modos de comunicação. 43
Figura 3.17 - *Fill gun*. 44
Figura 3.18 - Exemplo de utilização do sistema. Na imagem do mapa de Portugal podemos visualizar o pino que indica onde se encontra o sistema instalado. Na imagem à direita e em cima encontra-se o sistema ligado ao computador, na imagem em baixo vemos um exemplo de um utilizador a usar a aplicação. 44
Figura 3.19 - Montagem veicular. 45

Figura 3.20 - Aplicação a correr no tablet. 46
Figura 3.21 - Comparação de todos os resultados obtidos. 49
Figura 3.22 - Procedimento para avaliação do atraso de propagação do áudio entre dois rádios. 50
Figura 3.23 - Procedimento para avaliação do atraso de propagação do áudio entre a aplicação e o rádio tático. 50
Figura 3.24 Procedimento para avaliação do atraso de propagação do áudio entre o rádio tático e a aplicação. 51
Figura 3.25 – Comparação dos valores para ligação Ethernet. 52
Figura 3.26 - Comparação dos valores para ligação wireless. 53
Figura 3.27 - Comparação dos atrasos em relação à comunicação normal. Entrada áudio browser, saída no rádio. 53
Figura 3.28 - Comparação dos atrasos em relação à comunicação rádio-rádio. 54

Lista de Tabelas

Tabela 2.1- Pontuação do MOS nos vários *Codecs.* 19
Tabela 2.2 - Comparação entre H.323 e SIP a nível da complexidade. 27
Tabela 2.3 - Comparação entre H.323 e SIP a nível da escalabilidade. 27
Tabela 3.1 - Atenuações para cabo RG400. 30
Tabela 3.2 - Resumo inquérito. 32
Tabela 3.3 - Resumo inquéritos. 32
Tabela 3.4 – Funcionamento nos diversos browsers. 47
Tabela 3.5 - Comparação entre os tipos de onda no caso entrada e saída áudio no rádio. 47
Tabela 3.6 - Comparação entre os tipos de onda no caso de entrada de áudio no browser e saída no rádio. 48
Tabela 3.7 - Comparação entre os tipos de onda no caso de entrada de áudio no rádio e saída de áudio no browser. 48
Tabela 3.8 - Avaliação entre rádio-rádio. 50
Tabela 3.9- Avaliação onde a saída de áudio foi no rádio tático. 51
Tabela 3.10 - Avaliação onde a saída de áudio é no browser. 52
Tabela 3.11 - Resumo inquérito. 55
Tabela 3.12 - Resumo inquérito. 55
Tabela 3.13 - Validação dos requisitos. 56
Tabela 3.14 - Resumo da validação dos requisitos. 57
Tabelas 4.1 e 4.2 – Diferença de tempo à comunicação normal saída de áudio no rádio (4.1) e saída de áudio no browser (4.2). 59

Lista de Siglas e Acrónimos

ALE	*Automatic Link Establishment*
AM	Modulação em Amplitude
AO	Área de Operações
API	Interface de Programação de Aplicações
BFM	Bloco de Formação Militar
C2	Comando e controlo
CNR	*Combat Network Radio*
COMSEC	Comunicação Segura
CPU	Unidade Central de Processamento
DFF	*Digital Fixed Frequency*
DTMF	*Dual-Tone Multi-Frequency*
FH	*Frequency Hop*
FM	Modulação em Frequência
FND	Força Nacional Destacada
GPS	*Global Positioning System*
GRP	Ligação a um grupo de rádio da rede
GST	*Gstreamer*
HF	*High Frequency*
HTTP	*Hypertext Transfer Protocol*
ICE	*Interactive Connectivity Establishment*
ID	“Identificação Pessoal”
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPBX	*IP - Private Branch Exchange*
IpoA	*IP over Air*
ITU	União Internacional de Telecomunicações
LAN	*Local Area Network*
MCU	*Multi Control Unit*
MOS	*Mean Opinion Score*
NA	Nó de Acesso
NAT	*Network Address Translation*
NATO	*North Atlantic Treaty Organization*
NT	Nós de Trânsito
NTP	*Network Time Protocol*
OSI	*Open System Interconnection*
P/PRC	*Portugal* / Portable Radio Communications
PAR	Ponto de Acesso Rádio
PBX	*Private Branch Exchange*

PC	Posto de Comando
PCM	*Pulse-code Modulation*
PSTN	*Public Switched Telephone Network*
PTT	*Push to talk*
RAS	*Registration Admission Status*
RF	*Radio Frequency*
RFC	*Request for Comments*
RL	*Rear Link*
RTC	*Real Time Communications*
RTP	*Real-time Transport Protocol*
RoIP	Rádio sobre IP
SAE	Subsistema de Área Estendida
SAL	Subsistema de Área Local
SATCOM	Comunicação por Satélite
SDP	*Session Description Protocol*
SECOM	*Secure Communication*
SIC	Sistema de Informação e Comunicação
SICCE	Sistema de Informação para comando e Controlo do Exército
SIC-T	Sistema de Informação e Comunicação Tático
SIP	*Session Initiation Protocol*
SITACO	Sistema tático de comunicação
SGR	Subsistema de Gestão de Rede
SSR	Subsistema de Segurança de Rede
STN	Ligação a um rádio da rede
STUN	*Session Traversal Utilities for NAT*
SUM	Subsistema de Utilizadores Móveis
TCP	*Transmission Control Protocol*
TO	Teatro de Operações
TRANSEC	Transmissão segura
TURN	*Traversal Using Relays around NAT*
UA	*User Agent*
UHF	*Ultra High Frequency*
VHF	*Very High Frequency*
UDP	*User Datagram Protocol*
URI	*Uniform Resource Identifier*
URL	*Uniform Resource Locator*
VoIP	Voz sobre IP
WAN	*Wide Area Network*

1. Introdução

1.1 Enquadramento do problema e motivação

Desde as origens da humanidade que o ser humano sempre teve a necessidade de comunicar entre si. Para colmatar esta necessidade surgiram algumas soluções, entre as quais as telecomunicações, que simplificam a forma de as pessoas comunicarem entre si, permitindo comunicar em qualquer parte do mundo.

As telecomunicações militares são um exemplo de uma das maiores inovações tecnológicas ao serviço da soberania do Estado Português e do seu povo. Atualmente são usadas no apoio à sociedade civil, quando situações de crise ou catástrofes o justificam. A manipulação das informações em informação, ou seja, em conteúdo consistente e oportuno, emerge como o gene que tudo determina e de quem tudo depende. Neste conceito, a manipulação de informação, a capacidade de utilizar as tecnologias das telecomunicações e da informática para a produção, armazenamento e distribuição da informação, constitui um fator de vantagem [1].

Prevê-se que, no futuro, os conflitos sejam influenciados pela instabilidade causada pela emergência dos estados falhados, pelo extremismo ideológico e terrorismo, pelas ameaças transnacionais e crime organizado, mas também pela disputa de recursos naturais e pelas alterações climáticas, pelos efeitos da globalização e pelas ameaças sistémicas e cibernéticas que poderão causar a disrupção dos estados. As operações futuras terão um forte cariz assimétrico, quer em efetivos quer em tecnologia, e poderão desenrolar-se nas mais variadas áreas de operações. Nesse ambiente operacional, a tecnologia terá um papel determinante na utilização do ciberespaço e da informação, exigindo comunicações e sistemas de informação robustos e eficientes às necessidades das forças militares, desde os altos escalões até ao soldado que contribuam para a superioridade da informação da força. [2]

Nas Forças Armadas no seu conjunto e em cada um dos ramos, em cada nível e ao longo dos vários escalões, o exercício do comando e controlo (C2), a supervisão e a coordenação funcional obrigam a fluxos permanentes de comunicações, para análise das situações de planeamento, de decisão, de difusão de ordens e de conduta. São os sistemas de comunicação os instrumentos fundamentais que, em tempo de paz, contribuem para a prontidão das forças e que, em tempo de guerra, permitem introduzir uma lógica e organização no campo de batalha [3].

O objetivo principal das comunicações militares é servir o C2, ou seja, permitir ao comandante exercer a sua influência pessoal e direta no exercício do C2 das operações. Por sua vez, o objetivo secundário passa por facilitar a troca de informação. Um Sistema de Informação e Comunicações (SIC) [4] superior auxilia os Comandantes a manter a unidade de esforços para aplicar as capacidades das suas forças no tempo e local crítico e a vencer [4].

Os sistemas de comunicações podem classificar-se em sistemas de comunicações estratégicos e táticos. Os primeiros são sistemas permanentes, evolutivos em termos de meios e técnica, mas sempre com o mesmo objetivo, enquanto que os segundos, envolvidos nesta dissertação são os sistemas de comunicações táticos.

Os sistemas de comunicação táticos são sistemas planeados e implantados para apoio de uma unidade em campanha por forma a garantir a ligação entre o Comandante e os vários comandos subordinados, tendo em vista o cumprimento da missão atribuída ao comando apoiado. São sistemas precários, já que o seu emprego acaba quando a missão termina.

O Exército Português tem atualmente um Sistema de Informação e Comunicações Tático (SIC-T) [4], através do sistema de informação para o comando e controlo do Exército, o SICCE [4], e o Sistemas Tático de comunicações (SITACO) [4].

As Comunicações surgem-nos assim como os sistemas que "Transmitem ao cérebro as informações recolhidas e canalizam posteriormente para os músculos as decisões tomadas" [5].

Em termos de sistemas de apoio à decisão, um elevado número de sistemas de comando e controlo, enquanto plataformas do fluxo de informação, constitui-se como uma vantagem para os seus utilizadores [6].

A zona de comunicações num teatro de operações (TO) contém as principais instalações não só de apoio de serviços, mas também de linhas de comunicações que servem o TO. Num TO cada força está projetada segundo os vários escalões militares (brigadas, batalhões, companhias). Cada escalão da força tem a sua rede rádio de combate, onde lhes é possível comunicar entre si. Cada rede rádio tem comunicação para a rede do escalão respetivo, e este acesso só é possível no posto de comando.

Este trabalho é motivado para permitir flexibilidade aos vários utilizadores das redes rádio num posto de comando, nomeadamente ao comandante e ao oficial de operações. Sendo assim, será possível permitir que não tenham de estar fisicamente junto dos mesmos, pelo que o comandante se preocupa com o C2, fazendo uso das comunicações para o conseguir.

1.2 Problemática – Situação Atual

O objetivo primário das comunicações é «SERVIR O COMANDO» [4]. O Comandante é o único responsável, em todas as circunstâncias, por aquilo que a sua unidade executa ou deixa de executar [7].

Os sistemas de comunicações devem ser flexíveis e capazes de se adaptarem rapidamente às alterações dos planos de operações ou da organização para o combate. Devem poder apoiar todas as necessidades do comando e garantirem a segurança das comunicações, no maior grau possível compatível com as considerações de ordem operacional [7].

Atualmente existem diversos problemas nos sistemas de comunicação que não permitem um funcionamento sem restrições, designadamente:

- Inexistência de uma infraestrutura no Exército Português que permita a um comandante estar deslocalizado das redes rádio (longe dos equipamentos rádio) e que lhe permita comunicar de igual forma a um comandante que esteja sempre localizado junto aos rádios. Se um escalão militar quiser comunicar com redes rádio tem de estar fisicamente localizado junto aos rádios que estão a receber/transmitir as comunicações;
- É impossível a deslocalização da operação. No caso da Figura 1.1, se um comandante de um escalão superior estiver em Lisboa e quiser comunicar por voz para uma das redes rádio para uma missão que esteja a decorrer a centenas de quilómetros, não o pode fazer. Atualmente

apenas é possível comunicar utilizando os serviços do subsistema de informação utilizando comunicações militares táticas sem serem as redes rádio de combate, como por exemplo por satélite (SATCOM);

- Impossibilidade de ouvir duas redes rádio em simultâneo, pois apenas é possível escolher uma frequência, que está associada apenas a uma rede rádio;
- Limitação com o afastamento dos equipamentos radiantes, para não denunciar a posição dos postos de comando e na passagem de cablagem de radio frequência até aos rádios existentes no bunker. Presentemente existe a necessidade de forças militares, e não só, estarem localizadas em bunkers. Estas forças estão instaladas em estruturas fortificadas subterrâneas, com o intuito de resistirem a grandes libertações de energia. A ligação entre as antenas e os rádios obrigam à instalação de amplificadores e a perdas de sinal.

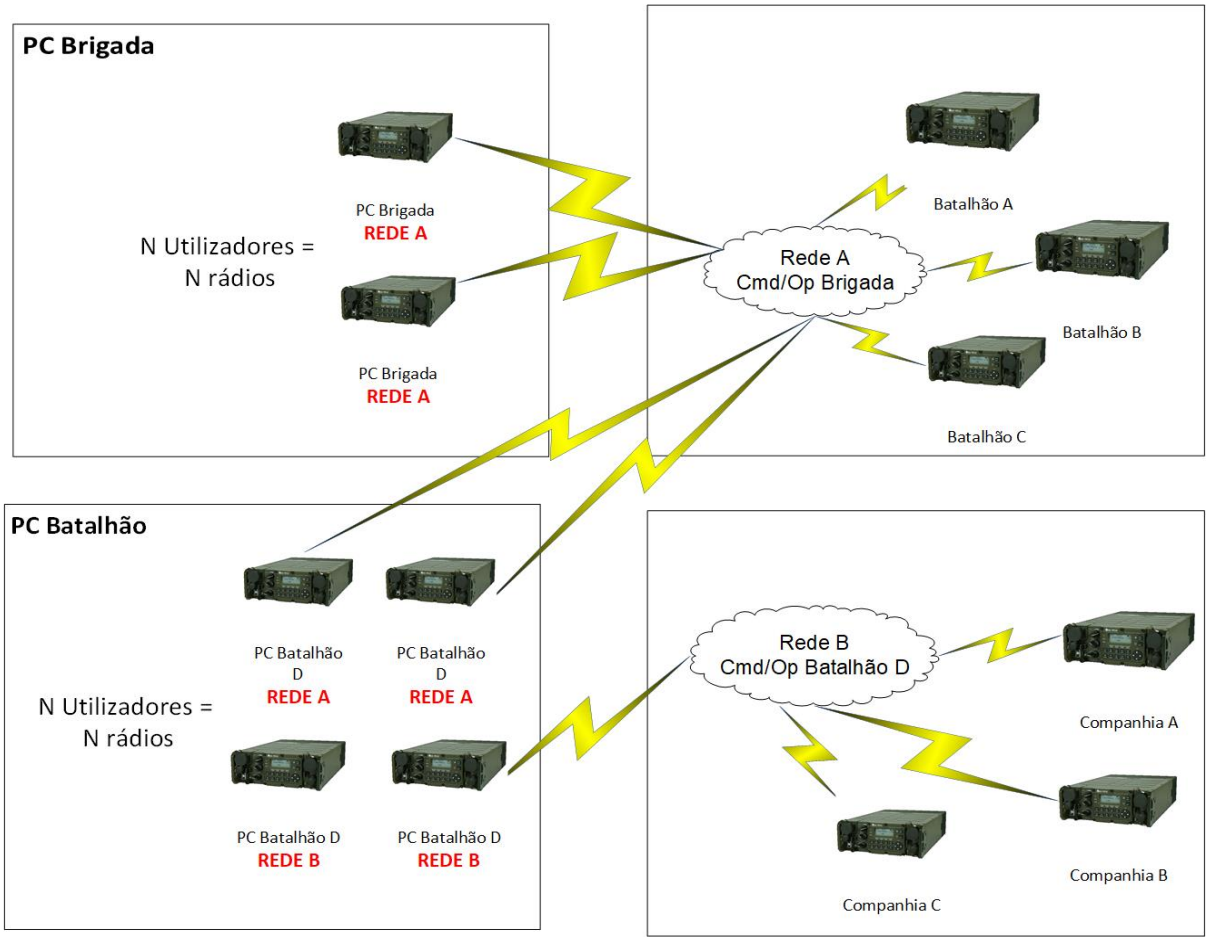


Figura 1.1- Funcionamento atual das redes Rádio no Exército Português.

A Figura 1.1 representa o funcionamento atual de uma rede rádio, como se pode verificar, caso existam N utilizadores, são necessários N rádios, o que é insuportável devido ao custo[1] de um rádio tático militar.

[1] Superior a 30000 € - Referência do custo de um rádio tático multifuncional.

1.3 Proposta de soluções

Quanto à proposta da solução desenvolvida, pretende-se que esta cumpra com as exigências necessárias de forma a corrigir os problemas identificados.

Tendo como base a Figura 1.2, vai existir um rádio que vai funcionar como *gateway*, que, por sua vez, vai estar ligada a uma rede rádio constituída por N rádios. Haverá um servidor, com ligação à intranet tática, ligado ao rádio militar P/PRC-525, tendo acesso a várias redes rádios.

Enquanto os militares se encontram dispersos no seu posto de comando ou noutro sítio no terreno, o servidor está estático num posto de comando a lidar com o processamento da informação. As informações recolhidas pela aplicação Web são enviadas para o servidor, que, posteriormente, as processa ao P/PRC 525 que está instalado nos Postos de Comando.

Foi necessário assegurar vários requisitos na proposta apresentada, como:

- Qualidade de voz – Para VoIP ser aceitável para os utilizadores, o tempo de atraso teve de ser mínimo, em relação à comunicação normal existente;
- Interoperabilidade – Produtos de diferentes marcas têm de operar entre si, portanto têm de comunicar entre si, para que os mais diversos utilizadores possam comunicar. Neste caso de estudo, sendo um ambiente fechado, o Exército Português, este problema não existe no que diz respeito ao VoIP. O esforço incidiu no desenvolvimento de uma aplicação que pudesse correr nos diversos sistemas operativos, Ios, android, etc. A solução mais viável passou por utilizar uma aplicação Web, onde qualquer pessoa com acesso a um browser consiga utilizar a aplicação;
- Segurança – Tem de existir encriptação, para garantir a não captura de pacotes por partes não autorizadas;
- Escalabilidade – O sistema tem de ser flexível para garantir que vários utilizadores se consigam ligar à rede e ou a várias redes.

Na Figura 1.2 é possível observar a escalabilidade proposta, onde N utilizadores conseguem comunicar com uma mesma rede rádio sem necessidade de existirem N rádios táticos, o que se traduz numa elevada poupança de meios.

Nesta representação, os postos de comando existentes têm o sistema desenvolvido instalado, mas podem continuar a comunicar de maneira normal, caso o sistema sofra alguma falha. Estes postos de comando estão ligados à rede de dados do Exército. Assim, um militar que esteja numa unidade do Exército pode aceder a este sistema e realizar comunicações como se se encontrasse fisicamente junto de um rádio, assim como executar configurações nos rádios.

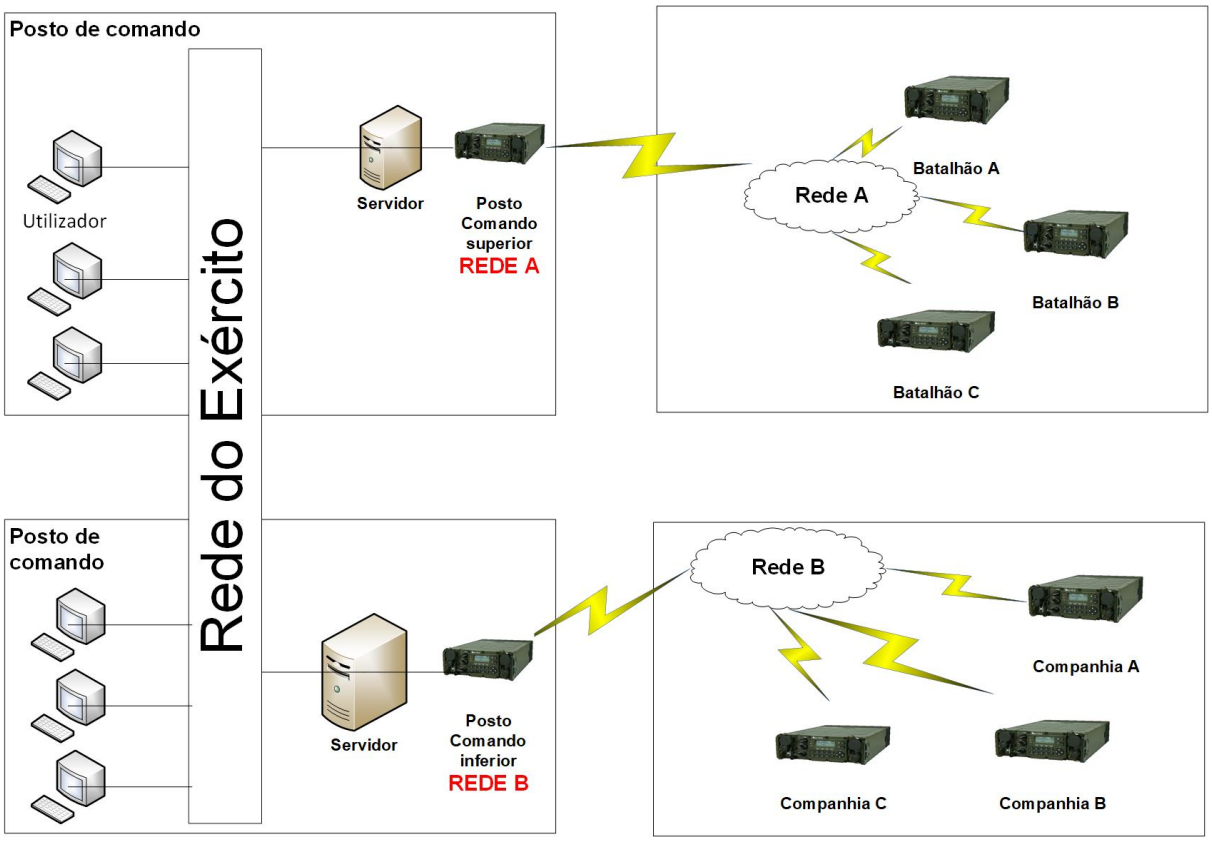


Figura 1.2 - Proposta de solução nas redes Rádio do Exército Português.

1.4 Estrutura do Documento

O presente documento está organizado em cinco capítulos, referentes a tópicos distintos.

O próximo capítulo contém os conceitos necessários para a compreensão das temáticas discutidas nesta dissertação. Inicialmente, começa por falar sobre os tipos de redes táticas. De seguida, sobre o rádio em que este estudo incide, o P/PRC 525, acerca das suas interfaces, os modos de comunicação. Estuda-se ainda o VoIP, os vários protocolos de compressão existentes e os protocolos de controlo de sessão. Por fim, discute-se acerca da comunicação sobre Web e dos vários sistemas de suporte existentes.

No capítulo 3 é apresentado o sistema. São definidos os requisitos de *software* requeridos para o desenvolvimento da solução proposta, a implementação e a avaliação do sistema.

No quarto capítulo, são averiguados os resultados da avaliação deste sistema e as vantagens do seu uso.

Por último, é feita a conclusão de todo o trabalho envolvente nesta dissertação.

2. Trabalho Relacionado

O Exército português tem atualmente rádios táticos que permitem radio sobre IP, RoIP. O sistema existente tem limitações. Quando um comandante usa um telefone IP para realizar uma chamada numa rede rádio, esta rede fica totalmente ocupada, pelo que qualquer rádio que esteja nessa rede não consegue utilizar o rádio, por exemplo para dados.

Existe atualmente hardware que possibilita a interligação de vários sistemas "*push to talk*" a uma rede de comutação existente SIP, como por exemplo o Asterisk PBX. Com este sistema é possível ligar sistemas que permitam VoIP a dispositivos móveis, computadores, tablets, computadores, etc. Esta solução, no entanto, é focada em hardware, não existindo nenhum software que possa colmatar as necessidades do Exército Português. Existe ainda a necessidade, por parte de cada escalão, de alguém com funções de manutenção que saiba vários parâmetros que os rádios em uso atualmente nas Forças Armadas nos podem fornecer, assim como a necessidade de efetuar alterações nas configurações dos rádios. Hoje em dia, caso alguém queira saber estes parâmetros ou alterar configurações tem de se deslocar fisicamente junto de cada rádio, não podendo remotamente aceder a estes dados.

2.1 Redes Táticas

O Sistema de Informação e Comunicações Tático do Exército Português foi concebido para ser flexível perante a crescente complexidade dos sistemas e novas tecnologias de informação. Pretende-se garantir um vínculo entre os soldados no seu ambiente tático e a sua estrutura de comando, pelo que se procurou dotar a estrutura do comando de um acesso sem restrições à informação necessária ao exercício do C2. [4]

O SIC-T é o sistema integrador, no nível tático, de toda a componente de comunicações, de sistemas de informação, de gestão da informação e do conhecimento e de guerra da informação, nesse nível. É um sistema de destinado a apoiar, durante um tempo determinado, uma força-tarefa para uma missão específica, em situação de campanha ou como Força Nacional Destacada (FND) [3]. Trata-se de um sistema modular, eficiente, seguro e flexível, que permite ao comandante ter as ferramentas necessárias ao comando. Além disso, fornece mobilidade e uma adaptabilidade à logística e às unidades de combate.

O SIC-T, como foi já referido, subdivide-se em dois sistemas. No subsistema de informação, no qual o sistema principal é o SICCE, e no SITACO.

2.1.1 Componente de Comunicações - SITACO

Como foi descrito acima, os sistemas de comunicações táticos são planeados e implantados para apoio de uma unidade em campanha por forma a garantir a ligação entre o Comandante e os vários Comandos Subordinados, tendo em vista o cumprimento da missão atribuída ao comando apoiado. São sistemas precários, pois a sua "vida" acaba assim que a missão termina.

No sistema SITACO definem-se dois tipos de utilizadores, os móveis e os fixos. Os utilizadores móveis baseiam-se essencialmente em sistemas de comunicação rádio, pois são estes que garantem flexibilidade e mobilidade no apoio a estes utilizadores. Este sistema deve:

- Permitir a transmissão de voz, dados, mensagens e vídeo;
- Interoperabilidade, o sistema deve ser interoperável com os sistemas de comunicações estrangeiro (ao nível da NATO), assim como os sistemas de comunicações dos outros ramos das Forças Armadas;
- Segurança – o sistema deve permitir a circulação de qualquer tipo de informação classificada até NATO SECRET [5].

A arquitetura deste sistema está estruturada em cinco subsistemas, designadamente o Subsistema de Área Estendida (SAE), Subsistema de Área Local (SAL), Subsistema de Utilizadores Móveis (SUM), Subsistema de Segurança de rede (SSR) e o Sistema de Gestão de Rede (SGR).

A Figura 2.1 permite compreender melhor a relação destes subsistemas.

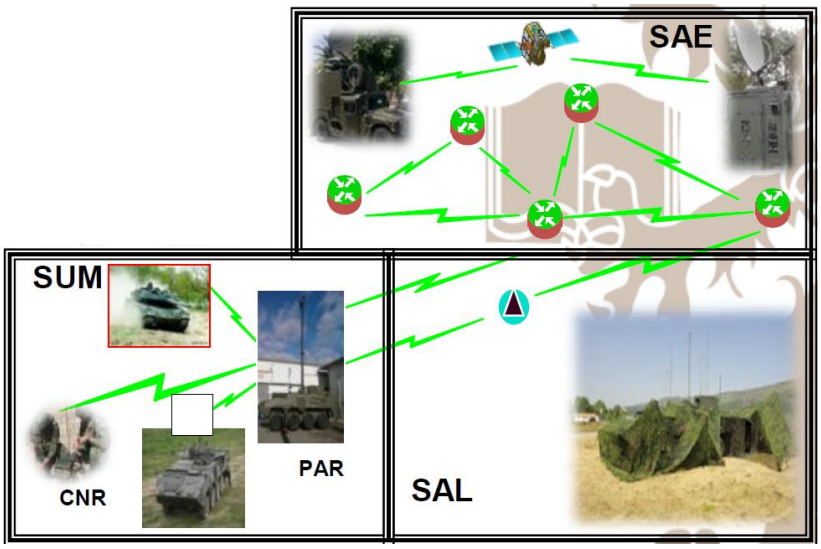


Figura 2.1 Subsistema de Comunicações do SIC-T, baseado em [6].

1. O SAE constitui a espinha dorsal do SITACO. Integrando os módulos Nó de Trânsito (NT) e *Rear-Link* (RL), é constituído por um conjunto de nós de comutação interligados através de links rádio multicanal (feixes hertzianos) ou, excecionalmente, por terminais de satélite de banda larga. Estes nós estabelecem sempre, no mínimo, duas ligações, permitindo assim caminhos alternativos para a informação [4].
2. O Objetivo dos SAL é fornecer a um grupo de utilizadores, normalmente ao nível dos comandos numa área restrita, usualmente os postos de comando (PC), diversas categorias de serviço (voz, dados, mensagens e vídeo) disponíveis na rede, e garantir o acesso à estrutura dorsal da rede ao SAE através do conjunto de nós de acesso (NA) [4].
3. O SUM tem a finalidade de realizar a interligação com os utilizadores dispersos na Área de Operações (AO). Estes utilizadores podem atingir distâncias na ordem de dezenas de quilómetros. Os utilizadores destes sistemas podem comunicar entre sim e ter acesso aos SAL e SUM. Através de Redes Rádio de Combate (CNR), sistemas rádio independentes das unidades

de combate que se baseiam em canais *half-duplex*. O exército Português tem atualmente como rádio principal o P/PRC-525. Portanto as Redes Rádio Digitais, são redes independentes para comunicações de pacotes de dados e devem ter a possibilidade de retransmissão. O acesso rádio através de Canal Seletivo, constitui o acesso de canal único para utilizadores de rádio móvel, através do PAR em duplex [8]. Estes utilizadores são integrados na rede tática através do PAR. O SUM integra estes módulos PAR e os utilizadores da CNR equipados com o P/PRC 525. A função principal do PAR é a interligação do rádio tático em ambiente IP, através de chamadas de voz por marcação automática para a rede IP, de chamadas seletivas para o rádio e de um serviço de dados com implementação da internet tática. Esta integração IP/Rádio no PAR é implementada de modo a flexibilizar o sistema, pois permite atribuir, de forma dinâmica, os rádios ao serviço de voz ou de dados (internet tática) até ao máximo de seis rádios [4].

4. O SGR é responsável pela cobertura transversal de todo o sistema, desempenhando funções de administração e controlo. O SGR constitui-se como o "cérebro" da rede [4].
5. O SSR, Figura 2.2 é responsável pela cobertura transversal a toda a estrutura do SIC-T e implementa diferentes níveis de segurança nas redes [4].

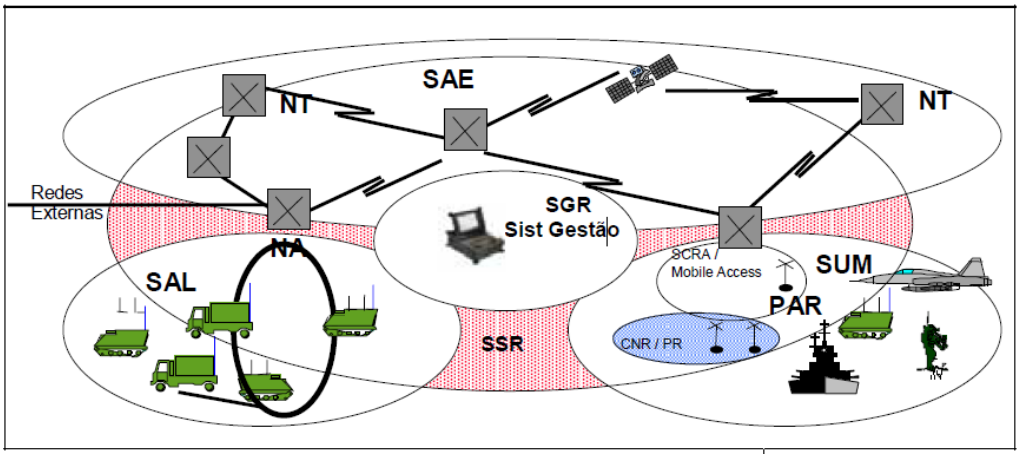


Figura 2.2 - O SIC-T e os seus subsistemas [6].

A solução proposta vai incidir no subsistema de utilizadores móveis, pois é este que faz a interligação com os dispersos utilizadores na Área de Operações. É também neste subsistema que os utilizadores podem comunicar entre si e ter acesso aos SAL e SUM, através de CNRs.

2.1.2 Componente de informação

O SICCE é o esqueleto do sistema de C2, implementado no exército a nível operacional e tático. A sua finalidade em ambientes operacional é a de fornecer aos comandantes dos vários escalões táticos toda a informação de que necessitam para cumprir a sua missão, quando e da forma que melhor lhes servir [8]. O objetivo é permitir aos mais altos escalões um suporte eficaz no planeamento, reduzindo assim ao mínimo o tempo consumido, e libertando o pessoal para a concentração nas tarefas essenciais.

Este sistema deverá ser flexível e móvel, garantindo uma adaptação a todo o tipo de missões atribuídas às forças operacionais. Deve ainda ser fiável, assegurando eficácia e confiança, sendo seguro e normalizado, e garantindo a interoperabilidade com outros sistemas de C2.

2.2 Rádio Tático P/PRC 525

O P/PRC 525 é um transcetor tático usado no Exército Português que permite uma grande flexibilidade em termos de bandas de frequências. O rádio foi construído com o objetivo de cumprir comunicações táticas. Tem a opção de comunicação de alta segurança, através de várias configurações que permitem encriptação e salto de frequência. É possível transmitir voz analogicamente ou digitalmente. O radio oferece soluções para todos os aspetos das comunicações táticas, operando em diferentes bandas de frequência cobrindo as faixas de HF, VHF e UHF com aplicação em diversos cenários, através da sua capacidade de configuração por via de software e hardware internos. O rádio é empregue na estruturação de sistemas complexos que possibilitam comunicação por dados, interligação entre redes analógicas e digitais, redes WAN e LAN, computadores e outros equipamentos terminais de dados [9].

O protocolo de IP através do “ar” (IPoA) permite ao rádio a capacidade de realizar comunicações IP, através da integração de rádios nas infraestruturas de rede, tendo estes a atuar como routers entre redes com fios e redes do ar – RF [9].

O protocolo de transporte em tempo real, RTP, é usado nos pacotes de transporte através da rede IP. Os pacotes RTP estão codificados com o *codec* G.711. O protocolo da sessão de inicialização (SIP) é usado para iniciar, modificar e terminar a sessão de chamada RTP e fazer o uso do protocolo da descrição de sessão para definir os parâmetros [9].

Atualmente, numa conversão de fluxo de voz entre um rádio e uma rede VoIP, o radio *gateway* é responsável pela conversão entre o fluxo de voz (rede rádio) e o fluxo RTP (rede IP). Do lado da rede IP, a voz é enviada em pacotes RTP codificados com o *codec* G.711. Da parte da rede rádio, a comunicação de voz é realizada utilizando a forma de onda respetiva e um *Vocoder* (codificador vocal com diferentes ritmos de transmissão, adaptados às bandas de frequências e à largura de bada) da rede rádio [9].

A comunicação entre o rádio *gateway* e os outros rádios da mesma rede acontece através de protocolos proprietários; no entanto, as definições SIP numa rede não são configuráveis. Apenas o rádio *gateway* implementa SIP.

O rádio tem um intervalo de frequência de operação de 1.5 a 511.9 MHz. O espaçamento entre canais pode variar, mas tipicamente em FM o valor típico é de 25KHz.

2.2.1 MODOS ESPECIAIS DE COMUNICAÇÃO

Existem modos no rádio considerados especiais, entre eles os que nos interessam são:

- SECOM-H
- SECOM-V
- ALE3G

SECOM-H

Uma rede de SECOM-H é um modo de comunicação em salto de frequência na banda de HF.

Este modo é um sistema de comunicação orientado para o estabelecimento de ligações físicas (dois rádios estão prontos a comunicarem entre si) e lógicas (um participante está a transmitir e um ou mais participantes estão a receber essa transmissão) que opera em voz e dados com proteção COMSEC e TRANSEC (Transmissão segura – saltos na frequência).

As características e procedimentos deste tipo de rede são agrupadas da seguinte forma:

- Características de comunicação (mesmo grupo de frequência para salto);
- Características de sincronização (mesma hora e Data);
- Características de segurança (mesma chave segura);
- Características de configuração (mesmo serviço).

As redes em SECOM-H são constituídas por rádios configurados com “Hopsets”, endereço de rede e endereço do rádio na rede, parâmetros de utilização do SECOM-H e chaves para TRANSEC e COMSEC. Todos os rádios envolvidos numa rede deste tipo devem ter os mesmos parâmetros, designadamente Data e hora, Hopset, KeySet (chave de COMSEC e TRANSEC) e Endereço de Rede.

SECOM-H suporta dois tipos de endereçamento, um em que estabelece uma ligação com um determinado rádio da rede, STN e outro em que estabelece uma ligação com um determinado grupo de rádio da rede, GRP [9].

COMSEC e TRANSEC em SECOM-H

A COMSEC para voz e dados é fornecida pela cifra antes da transmissão e pela decifra após a receção para a transmissão de dados e voz cifrada.

As chaves de COMSEC são utilizadas para cifrar os dados úteis a serem transmitidos em cada salto.

A TRANSEC é fornecida pelo salto em frequência. As frequências variam de 1.5 MHz a 29.999990 MHz. As frequências que são escolhidas para serem usadas nos saltos são armazenadas nos “Hopsets”. As frequências são escolhidas aleatoriamente por algoritmos com este propósito e controlados pela chave de TRANSEC, pela hora, pelo tipo de ligação e pelo endereço dos rádios que participam na rede. As chaves TRANSEC são utilizadas para selecionar a sequência de saltos de frequências do “*Hopset”.*

Um *Keyset* é constituído por uma chave de COMSEC E TRANSEC. Estes devem ser idênticos em todos os rádios da mesma rede. São criados num equipamento específico, gerador de chaves e são manipulados pela aplicação de configuração dos rádios.

Para garantir uma comunicação segura, todos os rádios participantes numa rede têm de estar ajustados para a mesma data e hora. Tal é conseguido através do GPS [9].

SECOM-V

Uma rede de SECOM-V é um modo de comunicação em salto de frequência na banda de VHF/UHF.

O modo de comunicação SECOM-V tem as mesmas características e procedimentos do modo de comunicação SECOM-H. Neste caso, a COMSEC é fornecida para a transmissão de dados e voz.

A TRANSEC é fornecida pelo salto em frequência. O intervalo das frequências nos Hopsets pode ser de 30 a 108 MHZ ou 121 a 512 MHz. O valor mínimo para o incremento da frequência nos Hopsets é de 25KHz. O SECOM-V implementa dois modos de salto em frequência, um que utiliza todas as frequências disponíveis no Hopset, *Frequency Hop* (FH) e outro, o *Digital Fixed Frequency* (DFF), em que utiliza apenas uma frequência pré-definida [9].

ALE3G

Este é um modo que permite o rápido estabelecimento de uma ligação, pois é realizado o varrimento dos canais de forma síncrona em todos os rádios da rede ALE3G, admitindo que todos os radio da rede estejam temporalmente síncronos. Para atingir este sincronismo é usado um relógio temporal fornecido pelo GPS, ou *Network Time Protocol* (NTP), em todos os rádios da rede. As chamadas suportadas neste modo são as chamadas individuais, chamadas *Broadcast,* e as chamadas de grupo. As redes de ALE3G possuem dois rádios a um máximo de 127 rádios.

Cada estação numa rede ALE possui um endereço único. Sempre que uma estação é chamada, o respetivo endereço é transmitido pelo rádio no canal selecionado. Quando a estação chamada identifica o seu endereço, esta estação interrompe a pesquisa de canais e responde à estação que chamou. As estações transmitem uma confirmação (*nos dois sentidos*) e as duas estabelecem uma ligação. É possível visualizar no display das duas estações que os rádios têm a ligação estabelecida e podem passar a transmissão de informação. Se o COMSEC estiver ligado para uma rede neste modo, todas as comunicações realizadas são seguras e as comunicações não seguras são evitadas [9].

2.2.2 Interfaces

O rádio P/PRC 525 tem várias interfaces e ferramentas que permitem fazer uma adaptação entre sistemas para se obter um produto que tem partes comuns aos dois sistemas, a nossa solução e o próprio rádio [9].

Ethernet

Esta interface permite enviar comandos para o rádio e obter dados deste, assim como carregar configurações para o rádio tático.

O administrador do sistema atribui um endereço a cada rádio, sendo cada endereço único. Esta atribuição de IP's permite várias funcionalidades, como o controlo do rádio remotamente via Ethernet, atualização do software do rádio via Ethernet e ainda a operação de uma rede IPoA.

Na Figura 2.3 é possível visualizar um exemplo em que um utilizador utiliza o computador para configurar um rádio tático via IP.

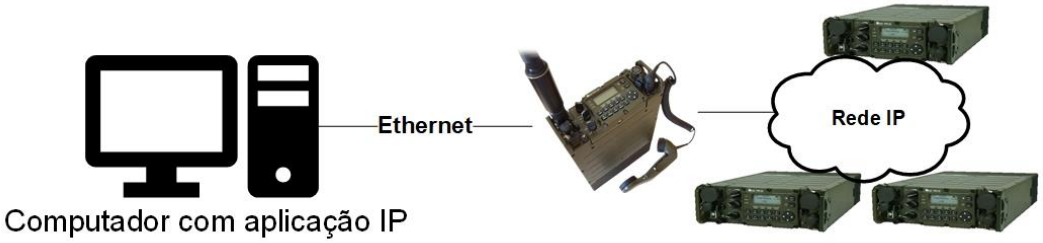


Figura 2.3 - Ligação via Ethernet.

Interfaces de áudio

O radio tem duas ligações possíveis para interagir com o áudio. A do microauscultador e uma ligação de dados. Cada uma destas ligações tem vários pinos que podem ser de interesse. São eles:

Ficha microauscultador

- AUDIO_RX – Ativa a saída de áudio para os auscultadores;
- AUDIO_TX – Ativa a entrada de microfone;
- PTT1 – entrada de push to talk (PTT).

Estes pinos vão ser utilizados para conseguir aceder aos rádios remotamente.

Ficha de dados

- LINE_TX – Linha de entrada de áudio;
- LINE_RX – Linha de saída de áudio;
- PTT2 – Entrada de PTT.

O radio tem ainda um conector da antena GPS, este vai ser necessário para testar modos de comunicação como o ALE3G [9].

2.3 VOIP

Voz sobre o Protocolo da internet (VoIP) é uma forma de comunicação que permite realizar chamadas telefónicas através de uma ligação de internet em vez das típicas linhas telefónicas. O acesso básico ao VoIP normalmente permite que se estabeleçam ligações para outras pessoas que também possam receber chamadas através da internet. O VoIP tem-se tornado uma opção bastante atraente de comunicação para os consumidores, dada a tendência de taxas mais baixas para serviços de banda larga e a rápida adoção de ofertas de internet cada vez mais rápidas.

A comunicação VoIP é enviada em pacotes (blocos de dados) por redes locais e redes de longa distância, ao contrário dos cabos tradicionais de cobre.

Os *codecs* são os métodos de operação responsáveis por transformar a transmissão de voz analógica em pacotes digitais para ocorrer a transferência de dados pela rede. Os *codecs* determinam a qualidade do som e a largura de banda necessária para enviar os pacotes pela rede [10].

2.3.1 Sinalização de Chamadas

A sinalização é a parte de endereçamento de VoIP. Quando é necessário estabelecer uma chamada através da rede existem certos parâmetros que são necessários saber.

Os principais protocolos VoIP são SIP e H.323, responsáveis pela criação, manutenção e eliminação de sessões de chamadas. São também responsáveis pela negociação dos parâmetros das sessões, como os *codecs* e largura de banda [11].

Na Figura 2.4 está uma representação dos protocolos mais usados VoIP do modelo OSI. É possível verificar que a camada transporte pode utilizar dois protocolos diferentes, dependendo dos protocolos utilizados nas camadas superiores.

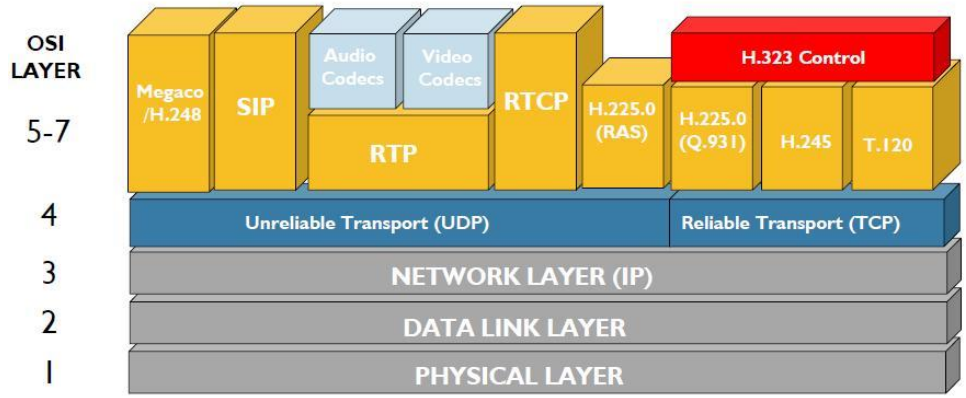


Figura 2.4 – Protocolos de sinalização VoIP [12].

Session Initiation Protocol

O *Session Initiation Protocol* (SIP) é um protocolo da camada aplicação que pode estabelecer, modificar e terminar sessões VoIP. A arquitetura deste protocolo é similar à HTTP, no que diz respeito a protocolos cliente-servidor, URIs e a mensagens baseadas em texto. Os pedidos são gerados pelo cliente e enviados para o servidor.

O protocolo SIP tem mensagens INVITE e ACK que definem o processo de abertura de um canal fidedigno sobre o qual as mensagens de controlo podem ser transferidas. Este protocolo por si só garante fiabilidade e não depende da ligação TCP. O SIP depende do Protocolo de descrição de sessão (SDP). Trata-se de um protocolo que descreve a sessão multimédia com o objetivo de comunicar a sessão, realizar o convite de sessão e outras formas de iniciar a sessão multimédia. O SDP inclui o tipo de média (áudio, vídeo), o protocolo de transporte, o formato da média (MPEG vídeo, H.261…), a informação que permite receber a média, como os endereços e portas. O protocolo suporta a descrição de sessões que permite aos participantes concordarem num conjunto de média compatíveis. SIP também suporta a mobilidade dos utilizadores, fazendo o redireccionamento para a localização atual do utilizador [13].

O SIP permite:

- Localização do utilizador – Determina qual o sistema terminal a ser usado para comunicação;
- Disponibilidade do utilizador – Define a disponibilidade do utilizador convidado para entrar nas comunicações;
- Configuração de Chamada – A conversa é estabelecida e os fluxos de média são transportados;
- Capacidades dos utilizadores – Determina os meios e parâmetros de média a serem usados;
- Controlo de sessões – Transferência e término de sessões, modificação dos parâmetros das sessões e adição de serviços.

Os sistemas SIP têm vários componentes, entre eles podem-se destacar, os *User Agents* (UA), servidores de rede e *Gateways*. Na Figura 2.5 é possível observar os vários componentes destes sistemas

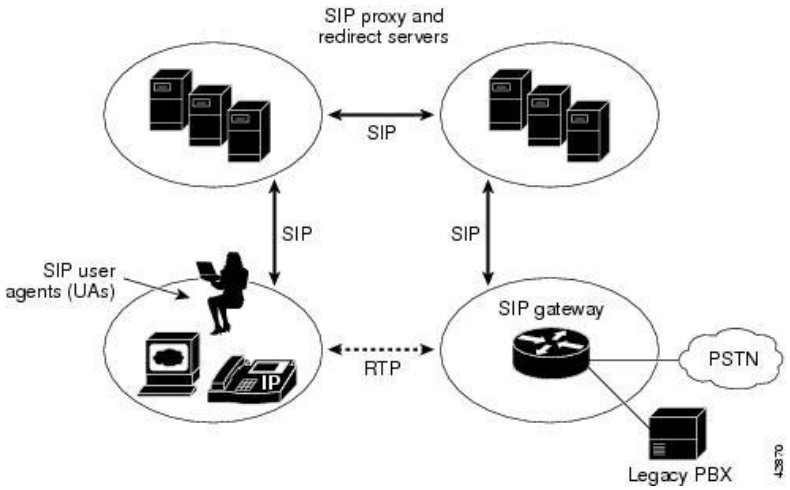


Figura 2.5 - Arquitetura SIP [14].

Os UA desempenham funções de um cliente que inicia o pedido SIP e de um servidor de UA, que contacta o utilizador quando um pedido SIP é recebido e devolve uma resposta em nome do utilizador [13].

Os servidores de rede são:

- Servidores de registo que recebem, autenticam e aceitam pedidos REGISTER de utilizadores SIP;
- Servidores *proxy,* que, quando recebem pedidos, os encaminham para o próximo servidor, que tem mais informação acerca da localização da conferência;
- Servidores de redireccionamento, que, ao receberem novos pedidos, determinam qual o próximo servidor e devolvem esses endereços ao cliente, em vez de os reencaminharem para o próximo servidor.

Os *gateways* permitem que UA se conectem a diferentes redes, como por exemplo a PSTN.

Este protocolo tem diversas mensagens, usadas para a comunicação entre o cliente e o servidor SIP. São exemplos dessas mensagens:

- INVITE – convida um utilizador para uma chamada;
- BYE – para terminar uma ligação entre dois sistemas terminais;
- ACK - para uma troca fidedigna de mensagens;

- REGISTER – fornece informação acerca da localização do utilizador para um servidor de registos SIP.

Os remetentes e destinatários são identificados por endereços SIP. Quando um utilizador realiza uma chamada, necessita de conhecer o servidor a quem fazer o pedido. O remetente pode contactar diretamente o destinatário, ou pode fazê-lo indiretamente através de servidores de redireccionamento. O Identificador de chamada no cabeçalho da mensagem SIP apenas identifica a chamada [13] .

Os terminais SIP são identificados por um URL SIP, que tem o formato utilizador@host. Estes endereços podem ser de um único utilizador ou de um grupo.

O cliente pode enviar o pedido a um servidor proxy SIP ou pode enviar o pedido diretamente ao endereço IP e porta correspondente ao seu URI.

Uma vez realizada a ligação entre as partes, o utilizador pode enviar pedidos ao servidor. Chama-se a uma transação SIP quando um pedido obtém respostas. OS pedidos podem ser enviados via TCP ou UDP.

Um convite bem-sucedido consiste em dois pedidos, uma mensagem INVITE procedida de um ACK. Depois de o destinatário aceitar a participação na chamada, o remetente confirma que recebeu a reposta com um ACK

O remetente pode mudar de localização ao longo do tempo. Estas localização podem ser registadas dinamicamente no servidor SIP. Quando é pedido ao servidor a localização do remetente, este devolve uma lista das possíveis localizações.

Na Figura 2.6 é possível observar um exemplo de fluxo SIP entre dois UAs, com recurso a um servidor.

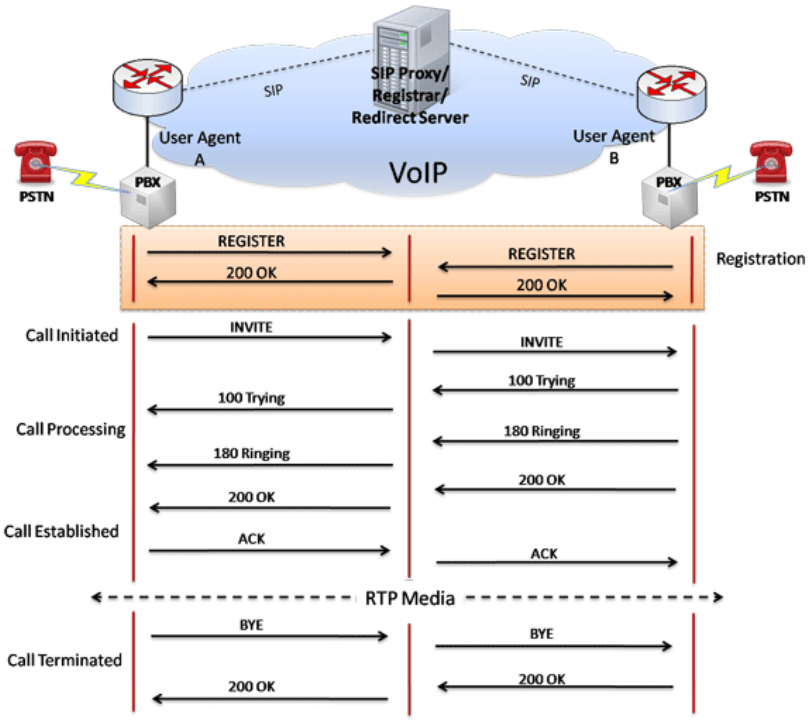


Figura 2.6 – Exemplo de Fluxo SIP [48].

H.323

O protocolo H.323 faz parte das recomendações ITU. Este protocolo de sinalização tem quatro componentes lógicos que permitem a comunicação, especificamente Terminais, *Gateways*, *Gatekeepers* e *Multipoint Control Units* (MCUs).

Os *Gatekeepers* são entidades na rede que proporcionam vários serviços, como a tradução de endereços e o controlo de acessos na rede para os terminais H.323, os *gateways* e MCU. Estes podem também permitir o controlo da largura de banda e são opcionais numa rede deste tipo.

Esta entidade tem algumas funções obrigatórias, entre elas:

- Tradução de endereços: traduz números "ID" em endereços IP (por exemplo 123@domain.com);
- Controlo de admissão: Mensagens de registo H.225 (admissão) e do estado (RAS);
- Controlo de largura de banda [15].

Protocolos de H.323

Os protocolos de H.323 dividem-se em três áreas principais:

- Sinalização RAS (H.225);
- Controlo e configuração das chamadas (H.225);
- Sinalização de controlo de média e de transporte (H.245).

Na Figura 2.7 esta representado a troca dos vários protocolos de H.323.

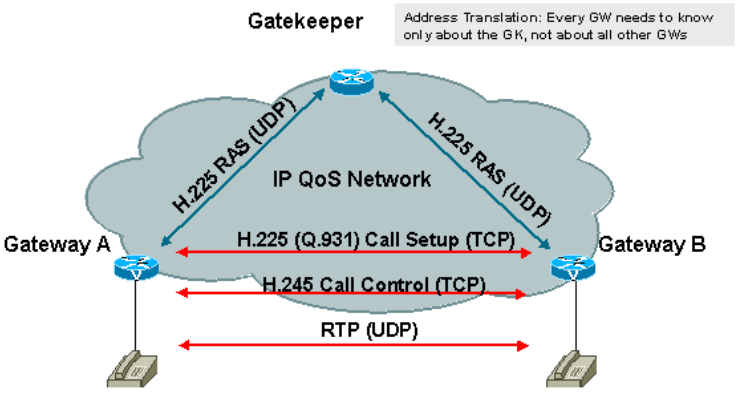


Figura 2.7 - Exemplo de troca de protocolos do H.323 [15].

Sinalização H.225 (RAS)

Este é um protocolo de sinalização usado entre *gateways* e *gatekeepers*. As mensagens RAS são enviadas através de UDP. Os procedimentos definidos pelos canais RAS são:

- Descoberta de Gatekeepers;
- Admissões, alterações de largura de banda, status e término de chamadas;
- Registo de sistemas terminais [16].

A sinalização de controlo é usada para configurar ligações entre terminais de H.323 [15].

Controlo de média e transporte H.245

O H.245 lida com as mensagens de controlo entre entidades H.323. Os procedimentos estabelecem canais lógicos para a transmissão de áudio, vídeo e dados. O H.245 é usado para negociar recursos de canais, tais como:

- Controlo de fluxos;
- Mensagens de compatibilidade [15].

Na Figura 2.8 esta representada uma visão geral dos protocolos de H.323

2.3.2 Protocolos de compressão áudio comuns em VoIP

A compressão de áudio digital permite o armazenamento e transmissão eficiente de dados de áudio. As várias técnicas de compressão de áudio oferecem diferentes níveis de complexidade, qualidade de áudio e quantidade de compressão de dados.

G.711 PCM

O G.711 PCM [17] é um protocolo com um ritmo binário de 64kbps. É o protocolo nativo as redes de telefone digitais modernas. Usar este *codec* para VoIP permite ter a melhor qualidade de voz, pois é este o *codec* utilizado em PSTN. Tem também a menor latência pois não há necessidade de utilizar buffers, o que requeria custos de processamento. A desvantagem é a maior necessidade de largura de banda do que em outros *codecs*, até 84Kbps, incluindo os cabeçalhos e UDP e IP. Este é também um protocolo suportado pela maioria dos fornecedores de VoIP.

Embora as conversões de digital para analógico afetem todas as redes de voz, as redes VoIP que usem este *codec* são tão resistentes aos problemas causados com esta conversão como as redes de telefone atuais.

G.726

O protocolo G.726 [18] é semelhante ao G.711, pois tem as suas bases na rede PSTN. Este *codec* é usado principalmente quando existe a necessidade de economizar largura de banda. O ritmo binário standard é de 32Kbps, tendo quase a mesma qualidade do G.711. Também suporta ritmos de 16, 24 ou 40Kbps.

G.729

Oferece qualidade a uma taxa de transmissão bastante pequena, de 8Kbps. No entanto, é um *codec* caro em termos de tempo de processamento de CPU. Há assim algumas limitações, existindo telefones VoIP que só conseguem lidar com um canal, chamada G.729, de cada vez. Isto pode fazer com que as chamadas falhem se o utilizador tentar colocar chamadas em simultâneo [19].

OPUS

Opus é um *codec* de áudio de livre utilização definido pelo IETF RFC 6176. Este suporta codificação constante ou variável entre 6kbit/s a 510kbit/s, tamanhos de amostras de 2.5ms a 60ms e

várias taxas de amostragem de 8khz (largura de banda de 4khz) a 48Khz (largura bada de 20Khz, onde toda a faixa auditiva do sistema auditivo humano pode ser reproduzida) [20].

Os sistemas de voz sobre IP podem sofrer com problemas significativos de qualidade de chamadas e gestão de desempenho. A qualidade da chamada pode ser afetada por ruido, distorção, ecos, falhas na fala e numa variedade de outros problemas.

Existe uma forma de quantificação da performance de voz nos *codecs*, denominada "*mean opinion scores*" (MOS). Estes testes são dados a um grupo de ouvintes e estes, dão a cada amostra uma classificação de 1 a 5 de má a excelente, respetivamente [21].

Tabela 2.1- Pontuação do MOS nos vários *Codecs.*

Método de Compressão	Bit Rate (Kbps)	Tamanho amostra (ms)	Pontuação MOS
G.711	64	0.125	4.1
G.726	32	0.125	3.85
G.729	8	10	3.92

O rádio P/PRC 525 usa internamente o *codec* G.711, sendo este o que apresenta uma melhor pontuação segundo a Tabela 2.1.

2.3.3 Protocolos de transporte

A camada de transporte do modelo OSI é responsável pela transferência de dados entre duas máquinas. Esta camada controla o fluxo de dados entre a origem e o destino dos dados.

UDP

O *User Datagram Protocol* (UDP) é um protocolo que não fornece garantia de entrega dos pacotes, ou seja, os pacotes são enviados e o remente não espera pela confirmação da sua entrega. O remente continua a enviar os próximos pacotes. Se o destinatário não receber os pacotes, não pode pedir para que sejam reenviados. Este protocolo é utilizado quando a velocidade é o maior requisito e a correção de erros não é necessária. UDP é utilizado principalmente em *streams* e aplicações de chamadas em tempo real [22].

TCP

O *Transmission Control Protocol* (TCP), ou protocolo de controlo de transmissão, tem, por sua vez, correção de erros, isto é, identifica pacotes que não chegam ao destinatário. Este protocolo é desenhado para tornar as ligações sólidas, ou seja, tem a habilidade de recuperar automaticamente de uma falha e reenvia pacotes que não tenham chegado ao destinatário [23].

RTP

Real-time transport protocol (RTP) ou protocolo de transporte em tempo real é um protocolo utilizado em aplicações de tempo real, que, como o nome indica, entrega pacotes de dados em tempo real. Normalmente as aplicações utilizam este protocolo sobre UDP. Este protocolo, por si só, não fornece nenhum mecanismo para garantir a entrega dos dados a tempo, assim como não fornece outras garantias que assegurem a qualidade de serviço. Os números de sequência que este protocolo inclui permitem ao destinatário reconstruir a sequência dos pacotes enviados. Normalmente a quantidade de voz que existe em apenas um pacote RTP é de 20ms [24].

2.3.4 Comunicação sobre Web

WebRTC [20], como o nome indica, significa comunicações em tempo real na Web. É um projeto "*open source*", que permite aos browsers e a aplicações móveis comunicações em tempo Real através de uma simples API.

Atualmente este projeto suporta diversos browsers nos vários sistemas operativos, desde Windows até android. Não são necessários *plugins* para aceder ao microfone, e o fluxo de áudio é direto de browser para browser. A comunicação em tempo real, RTC, é sustentada de raiz pelos browsers. Este sistema possibilita a interoperabilidade com serviços existentes de VoIP e até PSTN [20].

WebRTC não tem protocolos de sinalização standards, mas pode ser utilizado SIP por exemplo. Na camada transporte é usado HTTP ou WebSockets [25].

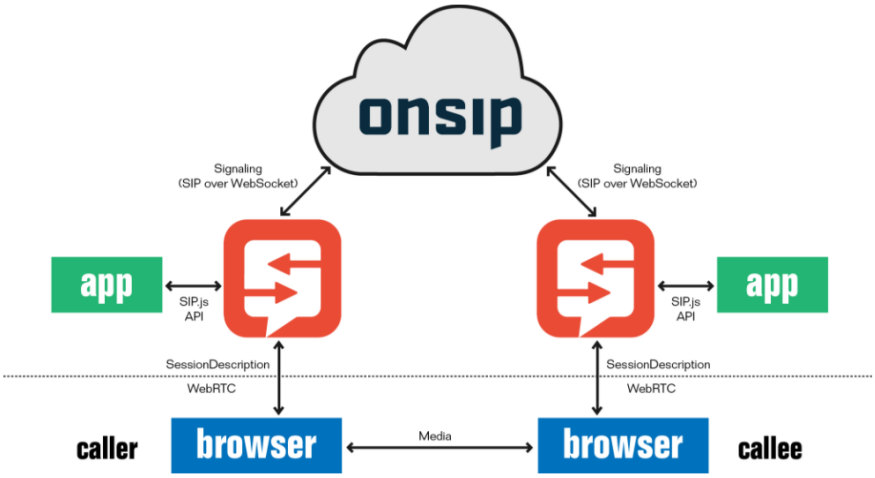


Figura 2.8 - Exemplo da utilização de WebRTC [25].

Na Figura 2.8 está descrito um exemplo onde a sinalização circula através da internet para configurar o fluxo média WebRTC entre browsers.

O projeto WebRTC foi desenhado para trabalhar em peer-to-peer para que os utilizadores possam comunicar pelo caminho mais curto. No entanto, tem de lidar com redes reais, por exemplo aplicações clientes que necessitem de comunicar através de *gateways* NAT e firewalls. As ligações peer-to-peer necessitam de apoio caso as ligações diretas sofram falhas. O STUN identifica cada utilizador e encontra uma boa ligação entre eles. Primeiro faz um pedido ao servidor, que tem o

protocolo STUN ativo. Depois, o servidor responde com o endereço IP do cliente, permitindo que o cliente possa facilmente identificar-se com o seu endereço.

Caso as firewalls não permitam tráfego STUN, é necessário recorrer ao protocolo TURN. O protocolo TURN adiciona uma retransmissão entre os clientes. Esta retransmissão funciona como uma ligação peer to peer entre os utilizadores. Assim sendo, o utilizador obtém a sua informação através do servidor TURN. Posteriormente, este servidor obtém e redireciona todos os pacotes para o utilizador respetivo. Este protocolo usa-se quando não há alternativas [26].

A encriptação é obrigatória para todos os componentes WebRTC. As aplicações JavaScript apenas podem ser usadas através de origens seguras. Não há mecanismos de sinalização definidos para evitar a redundância e para maximizar compatibilidades de tecnologias [27].

O *WebSocket é* um protocolo em que tanto o cliente como o servidor trocam mensagens em ambas as direções. Este protocolo define uma "*connection handshake*", baseada em HTTP, que é enviada pelo cliente e o servidor envia a resposta. Uma vez que o acordo entre as partes está realizado, a ligação é atualizada de HTTP para o protocolo WebSocket. Durante a *connection handshake* o cliente e o servidor concordam com o protocolo da aplicação que vai ser usado pelo WebSocket. Este protocolo de aplicação define o formato e a semântica das mensagens a serem trocadas pelos sistemas terminais. Uma vez que a resposta é obtida do servidor, tanto o cliente como o servidor reutilizam a ligação TCP para enviarem mensagens WebSocket e frames de controlo entre eles. Esta ligação pode ser utilizada para enviar múltiplas mensagens [28].

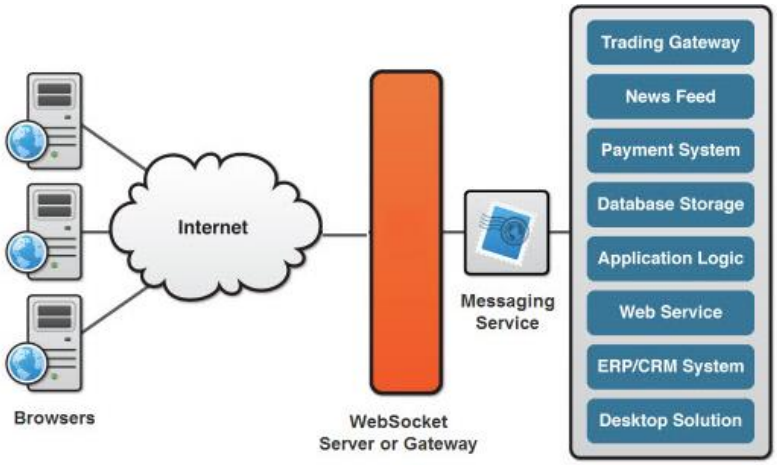


Figura 2.9 - Exemplo de utilização de WebSocket [49].

Na Figura 2.9 é possível observar a utilização de WebSockets para a troca de dados entre os browsers e os diversos serviços.

2.4 VOIP no P/PRC 525

A funcionalidade do serviço VoIP permite a um rádio realizar comunicações de voz com um utilizador VoIP externo através da rede IP. Este utilizador é um dispositivo com capacidade IP tal com um telefone VoIP [9].

As operações remotas são um caso usual do serviço VoIP, onde além da voz sobre IP, o controlo remoto do rádio também é realizado via IP.

O serviço VoIP pode ser usado para uma comunicação de voz entre um utilizador VoIP externo e uma rede rádio. Para este propósito, como é possível observar na Figura 2.10, um rádio na rede rádio tem como função *Gateway* VoIP. O rádio *gateway* VoIP é ligado via Ethernet a uma rede IP e manuseia chamadas originadas na rede rádio ou dirigidas à rede rádio. Qualquer rádio na rede pode ter a função de *Gateway* VoIP [9].

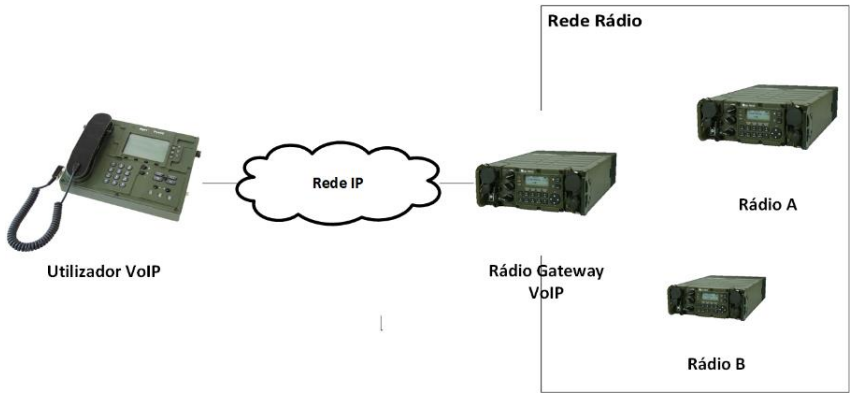


Figura 2.10 - Exemplo de rede rádio VoIP ligada apenas a uma rede rádio.

Na Figura 2.11 é possível observar um outro exemplo; neste caso os rádios A, B e C estão em comunicação. O rádio A está configurado como *gateway* e ligada a uma central VoIP PBX através da interface Ethernet.

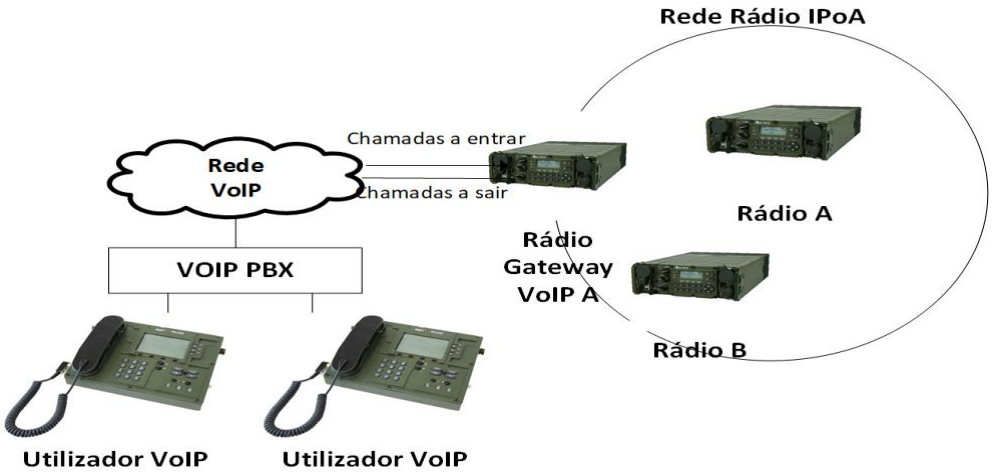


Figura 2.11 - Exemplo da ligação entre uma rede rádio ligada a uma rede VoIP utilizando um rádio Gateway que se liga à rede IP.

Não é necessário ligar um rádio *Gateway* a um PBX, pode ligar-se apenas um telefone ponto a ponto com um *Gateway*. Neste caso, se ligarmos um PBX, este fornece *voice prompt* a informar o chamador e o chamado acerca da chamada de rádio e sobre como proceder com o PTT do telefone, sendo uma vantagem para ambos os utilizadores. Podem ser utilizados dois PBX para ligar duas redes rádio sobre VoIP [9].

A comunicação entre o radio *gateway* e os outros rádios do grupo é um protocolo proprietário. Contudo, as definições SIP numa rede CNR não são configuradas. Apenas o rádio *gateway* implementa SIP-*gateway* com o PBX [9].

As chamadas de entrada na rede rádio permitem ligação a um dos rádios da rede ou a todos através de BROADCAST. Caso seja do interesse fazer uma chamada particular, é necessário enviar um convite SIP explicitamente para a estação de destino. Apenas existe uma sessão de voz em cada instante, pois o rádio *Gateway* rejeita chamadas adicionais. Nas chamadas de saída o funcionamento é o mesmo, podendo o utilizador escolher *broadcast* ou não [9].

Existem certas restrições que são gerais. Na Figura 2.11, por exemplo, todos os rádios pertencentes à mesma rede rádio devem ter as mesmas definições: a forma de onda, taxa de transmissão, dados VoIP, etc. O rádio VoIP *Gateway* apenas é capaz de manusear uma sessão de chamada SIP de cada vez [9].

O rádio tático permite comunicações de voz sobre dados IP. Este modo permite que o sistema interrompa uma transmissão de dados IP, através da ação do PTT do microtelefone, passado a uma transmissão de voz. Este serviço está disponível em SECOM -V ou SECOM -H [9].

Como foi mencionado, a voz tem prioridade aos dados IP, pelo que permite ao utilizador iniciar uma ligação de voz enquanto configurada para uma ligação de dados IP.

A comunicação é realizada ponto a ponto para o grupo, o que na prática é um problema, pois caso exista uma comunicação toda a rede está ocupada. Assim, não existe possibilidade de efetuar nenhuma troca de dados adicional na rede rádio.

Integração VoIP e P/PRC 525

Atualmente existe o ICC-201 IP INTERCOM SYSTEM [29] em operação no Exército Português. Na Figura 2.12 é possível observar um exemplo da sua utilização. Trata-se de uma infraestrutura de hardware e de aplicações de software que permitem comunicações locais entre viaturas, abrigos e possibilitam o acesso ao equipamento rádio [30]. As comunicações de voz e dados são suportadas pelo ar, fio de cobre e fibra ótica. Este sistema suporta voz, dados e acesso remoto, assim como cancelamento de ruído. É ainda suportado uma consola para o utilizador com uma interface que permite obter relatórios de “status”, ativação de recursos online e operações VOIP. Esta interface é executada num computador incorporado no ICC-201 ou noutra plataforma de dados externa que seja robusta. A unidade central do ICC-201 possui VoIP que permite a integração de sinais de radio analógicos, telefones táticos e de veículos em redes VoIP. Esses utilizadores podem “ligar” para números de telefone usando a funcionalidade de DTMF, já que a central deteta a sinalização DTMF e configura a chamada VoIP. Inversamente ocorre o mesmo, ou seja, os utilizadores da rede VoIP podem chamar um grupo específico, como uma rede rádio, um telefone tático ou uma combinação destes. Esta Central suporta também registos SIP integrados com recursos de IPBX.

Há uma grande variedade de sistemas terminais, desde terminais de comando a terminais de simples usuários, com ou sem wireless [29].

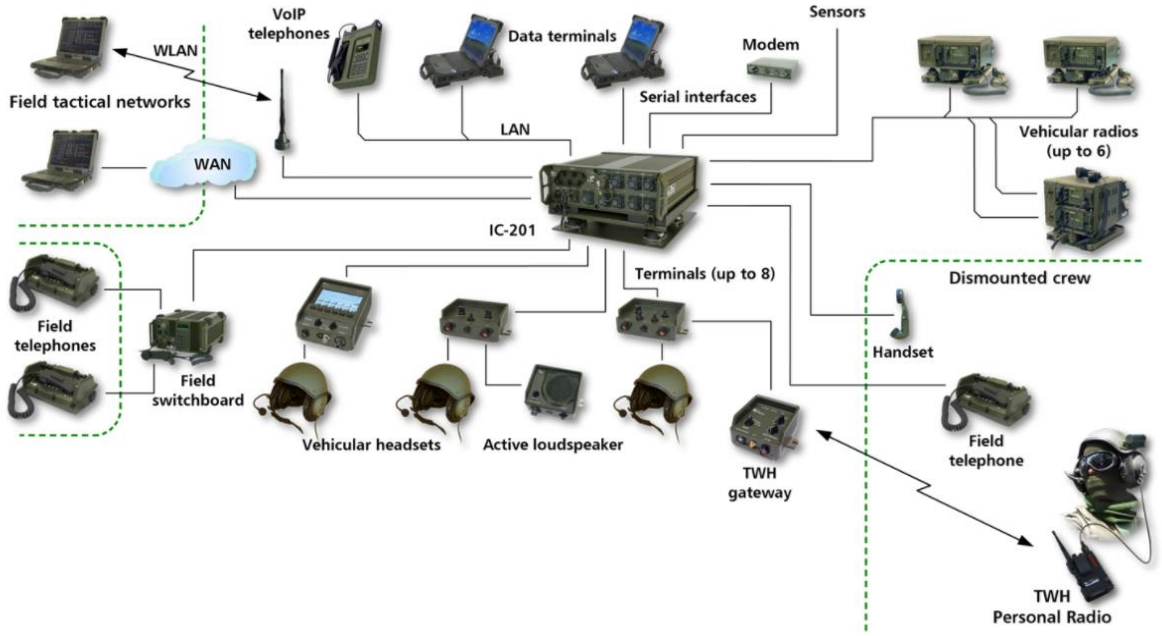


Figura 2.12 – Sistema tipo de comunicações de veículos com ICC-201 [30].

No Exército Português este sistema é utilizado em viaturas táticas militares onde o ruído exterior é bastante elevado e há necessidade de os utilizadores utilizarem auscultadores entre si. Serve também de *switch* e router básico para ligar computadores ou outros dispositivos. Existem várias configurações carregadas, e a consola serve para escolher qual a configuração a utilizar (por exemplo, escolher se para além de se falar internamente também se pode ouvir no auscultador o rádio A ou B, e se se pode fazer PTT no rádio A ou B). Em termos de VoIP este sistema é semelhante ao P/PRC 525, na medida em que regista uma extensão SIP por rede rádio. Ou seja, não permite ouvir e falar sem ocupar a rede, e não tem qualquer interface informática configurável por aplicação browser.

2.5 Sistemas de suporte para sinalização de chamadas

Existem várias aplicações focadas para a comunicação de voz sobre IP, entre elas vão ser destacadas duas *open source*, cada uma mais vocacionada para cada protocolo de controlo de sessão, SIP e H.323.

2.5.1 Asterisk

Asterisk é uma plataforma telefónica que permite a construção de aplicações de comunicação. Este software transforma um computador comum em um servidor de comunicações e alimenta sistemas IP PBX, *gateways* VoIP, etc. [31]. Há vários protocolos nativos deste software, entre eles SIP e H.323.

O Asterisk é construído por módulos. Um módulo é um componente passível de ser carregado que fornece uma funcionalidade específica. Os módulos que constituem esta plataforma podem ser de vários tipos: aplicações, tradutores de *codecs*, módulos de teste e interpretadores de diversos formatos.

Esta plataforma é capaz de comunicar com um vasto número de diferentes tecnologias. Em geral, estas comunicações são feitas através de ligações de rede; no entanto, ligações mais tradicionais, como as PSTN, requerem hardware específico [32].

2.5.2 Gnu *gatekeeper*

O Gnu *Gatekeeper*s é um *gatekeeper* H.323. Este *gatekeeper* fornece serviços de controlo de chamadas para sistemas terminais H.323 e é uma parte integral da maioria da comunicação baseada em H.323. Uma vez que H.323 e SIP são protocolos VoIP incompatíveis, não é possível utilizar telefones SIP diretamente. Todavia, há *gateways* que permitem a ponte entre estes dois protocolos.

De acordo com a recomendação H.323, um *gatekeeper* deverá prover os seguintes serviços:

- Tradução de Endereços;
- Controlo de Admissão;
- Controlo da Banda Larga;
- Sinalização das Chamadas;
- Autorização de Chamadas;
- Gestão da banda larga;
- Gerenciamento das Chamadas.

Este software implementa muitas destas funções [33].

2.5.3 Bibliotecas VoIP

Os programas VoIP, são usados para orientar chamadas de voz semelhantes às típicas chamadas telefónicas através de redes IP.

SIP.js [34] é uma biblioteca SIP completa, escrita em JavaScript. Esta biblioteca possibilita a utilização do WebRTC para incorporar áudio na aplicação, sendo rápida e leve, e permite adicionar uma pilha de sinalização SIP às aplicações WebRTC [34]. Tem ainda as seguintes características:

- Regista UA SIP através de WebSockets;
- Cria sessões multimédia de áudio e vídeo;
- Envia mensagens instantâneas;
- A maior parte dos browsers são compatíveis com esta biblioteca;
- SIP.js foi testado com o Asterisk.

JsSIP [35] é uma biblioteca para construir sistemas terminais SIP em ambientes Web. Com esta biblioteca é possível enviar e receber chamadas multimédia assim como mensagem de texto em páginas Web. Para correr JsSIP são necessários WebSockets. Esta biblioteca é ainda compatível com a maioria dos browsers, bem como com o software Asterisk, embora ainda apresente erros com as mensagens REGISTER do protocolo SIP [35].

2.5.4 Gstreamer

O Gstreamer [36] é uma estrutura que permite criar aplicações média de fluxo contínuo. A estrutura do Gstreamer foi projetada para facilitar o desenvolvimento de aplicações que trabalham com áudio ou vídeo ou ambos.

Esta *framework* é baseada em vários *plugins* que permitem a utilização de vários *codecs.* Os *plugins* podem ser ligados e organizados através de uma pipeline. Esta pipeline define o fluxo de dados.

Especificamente, o Gstreamer permite [36]:

- Uma arquitetura de plugins, permitindo adicionar várias funções às aplicações;
- Uma arquitetura de pipelines, ou seja, permite encadear vários processos de uma forma organizada.

Os plugins do Gstreamer podem ser classificados em:

- Manipulação de protocolos, por exemplo RTP;
- Codecs, codificadores e descodificadores;
- Filtros, que permitem adicionar efeitos aos dados;

O Gstreamer está organizado em vários pacotes que continuam em desenvolvimento:

- gst-plugins-base: um conjunto essencial de elementos;
- gst-plugins-good: um conjunto de plugins de boa qualidade;
- gst-plugins-ugly: um conjunto de plugins de boa qualidade que podem causar problemas;
- gst-plugins-bad: um conjunto de plugins que precisam de mais qualidade;
- Outros pacotes.

Os elementos são a classe mais importante de objetos no Gstreamer. Um elemento tem uma função específica, que pode ser a leitura de dados de um arquivo, a decodificação desses dados ou a saída desses dados para a placa de som, por exemplo. Ao encadear vários elementos, é possível criar uma *pipeline* que pode realizar uma tarefa específica, por exemplo reprodução ou captura de média [36].

Os blocos são as entradas e saídas de elementos, onde é possível ligar outos elementos. Estes têm recursos específicos de manipulação de dados, pelo que um bloco pode restringir o tipo de dados que passam por eles. Um bloco pode ser comparado a um *jack* de áudio.

As pipelines permitem a sincronização entre os elementos [36].

2.5.5 Avaliação

Das várias aplicações e protocolos vão ser escolhidos os que melhor se adaptam às necessidades para a resolução do problema apresentado.

SIP vs H.323

Na Tabela 2.2 é possível observar uma breve comparação destes dois protocolos, a nível da sua complexidade [37]:

Tabela 2.2 - Comparação entre H.323 e SIP a nível da complexidade.

Critério	H.323	SIP	Escolha/Razão
Mensagens	Complexas, demasiadas mensagens para funcionalidades semelhantes	Respostas logicamente numeradas para extensões. Conjunto menor de mensagens para a mesma funcionalidade	SIP - Tempo e extensibilidade
Reutilização de código	H.323 e H.32x	SIP e Web	SIP – mais modular
Métodos para implementar serviços	Pode suportar todos	Pode suportar todos	Equivalente
Sinalização das chamadas	Suporta	Suporta	SIP – mais rápido e menor complexidade

Na Tabela 2.3 é possível observar uma breve comparação destes dois protocolos, a nível da sua escalabilidade [38]:

Tabela 2.3 - Comparação entre H.323 e SIP a nível da escalabilidade.

Critério	H.323	SIP	Escolha/Razão
Suporte WAN	Sim	Sim	Equivalente
Grande quantidade chamadas	Sim	Sim	Equivalente
Processamento de mensagens	Mensagens mais pequenas, mas maior sobrecarga de processamento	Mensagens maiores, mas menor sobrecarga de processamento	Equivalente

Vantagens SIP

Permite uma mobilidade dos utilizadores, que podem deslocar-se dentro da mesma rede sem restrições, pois é atribuído apenas um identificador a cada utilizador. Este protocolo possibilita a escalabilidade da rede, pois a estrutura SIP permite um aumento dos componentes com facilidade. O SIP também tem a facilidade de ter uma representação textual, o que torna o protocolo mais amigo do utilizador. Olhando para o futuro, as estatísticas dizem que o protocolo SIP cada vez mais está a substituir o protocolo H.323, o que antecipa uma utilização mais generalizada deste protocolo, que, por sua vez, reúne um maior número de pessoas que saibam manuseá-lo [39]. O Exército Português tem visto a diminuição do seu efetivo, o que dificulta a instrução especializada de um protocolo complexo, H.323. Assim sendo, nesta dissertação o protocolo será o SIP.

Asterisk vs Gnu *Gatekeeper*

Dado que no tópico SIP vs H.323 se chegou à conclusão que o mais indicado para este projeto é o SIP, opta-se também por escolher a aplicação *open source* Asterisk, por ser mais dirigida ao SIP, enquanto o Gnu *Gatekeepers* apenas permite a utilização de H.323.

No entanto na implementação final deste sistema não se utilizou nenhum dos protocolos analisados, SIP e H.323. Optou-se por utilizar WebRTC e protocolos de sinalização próprios, pois dado as características do sistema desenvolvido, as soluções utilizadas facilitaram a implementação do mesmo.

3. VOI525

O nome escolhido para o sistema desenvolvido é VOI525 pois é a união do nome VOIP, tecnologia usada no desenvolvimento do sistema e o nome do modelo do rádio para o qual o sistema foi vastamente testado embora funcione com qualquer rádio genérico.

VOI525 é um sistema que permite comunicar através de browsers com rádio P/PRC 525. Este sistema permitir comunicar com N redes rádio. Permite ainda a configuração do rádio assim como a visualização de dados deste.

Este sistema está pensado para ser utilizado por duas classes de utilizadores: os operadores e os responsáveis pelas comunicações.

3.1 Casos de Uso

VOI525 pode ser aplicado em vários cenários reais no Exército Português. O sistema é flexível e móvel, garantindo uma adaptação a todo o tipo de missões. Assim temos aplicações deste sistema em missões temporárias e em casos de longa duração.

3.1.1 Campanha

O posto de comando é um órgão devidamente estruturado e organizado, composto pelo Comando, pelo Estado-Maior e pelos meios de comunicações onde se desenrola o processo de decisão. O posto de comando tem várias funções, desde a conduta das operações em curso, o apoio às operações em curso, o planeamento das operações futuras, e a manutenção das forças.

Em campanha existem vários oficiais com funções distintas que necessitam de comunicações via rádio, de que são exemplos o oficial de pessoal que aconselha o comandante ou o oficial de operações que aconselha sobre as possibilidades de apoio às operações.

Na Figura 3.1 podemos observar o exemplo de um posto de comando. Verifica-se ainda que as antenas estão colocadas nas viaturas táticas. Assim, os militares responsáveis pelas comunicações têm de se deslocar às viaturas para comunicar e os operadores para verificar as configurações dos rádios.

Figura 3.1 - Exemplo Posto de Comando [47].

Em campanha, como foi referido, pode existir a necessidade de vários oficiais, no mesmo posto de comando, terem de comunicar para a mesma rede rádio assim como a necessidade de ambos ouvirem as comunicações que existem numa mesma rede. Atualmente para o conseguirem, são precisos N rádios, conforme o número de utilizadores. Os altos custos de casa rádio justificam que a utilização desta aplicação se torne uma mais-valia.

Pode também ser indispensável a oficiais de Estado Maior a possibilidade de conseguirem ouvir várias redes rádio, o que atualmente não é possível. Com esta solução, estes oficiais vão ter à sua disposição uma interface gráfica, através de uma aplicação Web, que pode ser acedida através de qualquer dispositivo que tenha acesso à Web.

É ainda possível que estejam deslocalizados do rádio; no melhor caso, um comandante que não possa estar no Teatro de Operações pode estar a ouvir as comunicações em qualquer instalação onde exista acesso à rede do Exército. Para tal, os utilizadores têm de fazer login, e, conforme os seus privilégios, varia o número de redes com quem podem comunicar.

No presente e no futuro há sempre a necessidade de ter comunicações em qualquer ponto do País. Como é natural, há zonas em que, ao longo de vários quilómetros, em que não existe movimento populacional, ou seja, não existem os meios convencionais, nomeadamente telecomunicações. Sendo assim, para ser possível existirem comunicações nas zonas que o Exército possa ocupar, são necessárias antenas para haver um fluxo bidirecional de comunicações entre duas zonas.

3.1.2 Instalações fixas

Temos ainda algumas zonas ocupadas com proteção de bunker, ou seja, instalações subterrâneas que se encontram a metros da superfície. Neste caso, os meios rádios encontram-se dentro dos bunkers, local onde se encontra a Força, protegida. A distância entre os rádios terminais e a antena de receção das telecomunicações é na ordem das dezenas de metros, o que induz a elevadas perdas no cabo coaxial [40], consultar anexo B.

Na Figura 3.2 verificam-se os índices de atenuação para cada 30.48 metros (100 pés).

Attenuation k1 (db/100ft) @ 23 deg C	0.426		Attenuation (typical) at any Frequency
Attenuation k2 (db/100ft) @ 23 deg C	0.0012		=k1 x SqRt (FMHz) + k2 x (FMHz)

Figura 3.2 - Índices de atenuações para o cabo RG400 [40].

Na Tabela 3.1 verificam-se as atenuações para várias frequências e distâncias.

Tabela 3.1 - Atenuações para cabo RG400.

Atenuação (dB)	Comprimento (m)			
Frequência (MHz)	1	10	30	60
1.5	0	0.2	0.5	1
100	0.2	1.5	4.3	8.6
250	0.3	2.3	7	13.9
350	0.3	2.8	8.3	16.6
500	0.4	3.4	10	20

Conclui-se com a Tabela 3.1 que, tendo como frequência base 250 MHz, para uma distância de 1 metro, obtém-se uma atenuação em relação ao comprimento do cabo coaxial, sem contar com outras atenuações de adaptadores de 0.3 dB. Se a distância for de 60 metros para a mesma frequência obtém-se uma atenuação de 13.9 dB. Portanto, com o sistema, é possível substituir praticamente todos os metros de cabo coaxial por cabo de rede, evitando perdas de aproximadamente 13.6 dB caso se utilize por exemplo um cabo de 1 metro em vez de 60 metros.

Com esta solução é possível colocar o rádio P/PRC 525 a uma distância considerável do bunker, assim como deste sistema. Caso o inimigo utilize guerra eletrónica para efetuar a triangulação do sinal rádio e ataque as coordenadas do nosso sistema radiante, o bunker continua seguro visto que o inimigo vai continuar sem saber a posição dos bunkers.

3.1.3 Controlo de acessos

Atualmente, num posto de comando, um oficial que necessite de comunicar ou se desloca até ao rádio que está ligado à rede rádio a que quer comunicar ou pede para transmitir a mensagem a outro camarada, o que, por vezes, não pode ser possível devido aos diferentes níveis de acesso da informação.

Nas instalações fixas existem algumas dezenas de pessoal das mais diversas categorias do Exército Português, desde a praça ao oficial general. Como é compreensível, existem vários níveis de segurança, ou seja, diferentes níveis de acesso a certa informação. É então necessário integrar no software proposto um gestor de acessos, que possa dar a devida permissão a devido utilizador.

Hoje em dia não há controlo de acessos que garanta que quem utilizou o rádio foi o militar correto e autorizado.

3.2 Funcionalidades

Para saber quais as funcionalidades, requisitos do VOI525 que seriam mais importantes para os utilizadores realizaram-se inquéritos a futuros utilizadores.

3.2.1 Inquéritos

Antes do início do desenvolvimento do sistema procedeu-se a um inquérito a vários militares de diversas patentes do Exército Português das mais diversas funções. O universo a quem foi pedido para responder ao inquérito foi abrangente no que diz respeito às funções que desempenham - desde o Comando/Chefe de Estado Maior aos Estados Maiores do Pessoal, Informações, Operações, Logística, Comunicações, às equipas de Engenharia, aos militares que realizam as configurações dos rádios táticos. Os inquéritos podem ser consultados no anexo A.

Realizaram-se várias questões, designadamente:

1. Os inquiridos acham útil que uma aplicação possa permitir o acesso remoto (ouvir/transmitir) a um Rádio?
2. É útil uma funcionalidade que permita ouvir todas as redes rádio a que se tenha permissão?
3. É necessário que um operador dos rádios tenha acesso às informações destes remotamente?

4. É importante que a rede rádio continue desocupada quando se realizam chamadas IP para a rede?
5. É pertinente que um utilizador consiga fazer PTT (remoto através da aplicação) para as redes rádio a que tem acesso?

Na Tabela 3.2, cuja avaliação teve por base uma escala de 1 (nada útil) a 5 (extremamente útil), e na Tabela 3.3, em que a avaliação pedida era afirmativa (sim) ou negativa (não), é possível observar um resumo dos resultados obtidos nos inquéritos. Verificamos que as grandes percentagens se encontram nos valores de 4 e 5, ou seja, os inquiridos acham úteis os requisitos propostos.

Tabela 3.2 - Resumo inquérito.

Questão/Avaliação	1	2	3	4	5
1ª	0%	0%	15%	35%	50%
2ª	0%	5%	15%	30%	50%
3ª	5%	0%	5%	40%	50%

Tabela 3.3 - Resumo inquéritos.

Questão/Avaliação	Sim	Não
4ª	80%	20%
5ª	100%	0%

3.2.2 Requisitos

Após a realização dos inquéritos procedeu-se à escolha dos requisitos necessários para o sistema, divididos, posteriormente, em requisitos funcionais, de segurança e de interoperabilidade.

3.2.2.1 Funcionais

R1 - Os utilizadores, principalmente da categoria de oficiais, podem comunicar com as redes táticas a partir do seu Web Browser;

R2 - Os oficiais devem ter a funcionalidade de conseguirem comunicar com as várias redes rádio que existam;

R3 - Os militares mais vocacionados para a parte da manutenção dos rádios, os operadores, devem conseguir observar na aplicação o estado destes, assim como realizar configurações, tudo remotamente;

R4 – Garantir que a qualidade das chamadas entre aplicação-rádio e rádio-aplicação é suficientemente boa.

3.2.2.2 Segurança

R5 –Sistema sobre HTTPS;

R6 - Níveis de autorização. Cada utilizador tem de realizar a autenticação para conseguir utilizar a aplicação. Sendo assim, vão existir diferente níveis de autorização, que vão corresponder a cada utilizador;

R7 - O operador consegue visualizar os registos das chamadas e das alterações efetuadas;

R8 - Comunicação segura. A comunicação SECOM garante segurança devido ao salto em frequência, que dificulta a quem queira intercetar as comunicações o seu sucesso. Todos os rádios envolvidos neste tipo de comunicação têm de ser os mesmos parâmetros: Data e hora, Hopset, KeySet (chave de COMSEC e TRANSEC) e Endereço de Rede.

3.2.2.3 Interoperabilidade

R9 - Iteração com o P/PRC 525 através de uma aplicação Web (utilização de browsers);

R10 – Capacidade de comunicar a longas distâncias do rádio (principal);

R11 - Comunicação Voz – integrado com o modelo clássico, PTT;

R12 - Não sobreposição à comunicação normal;

R13 - Opção de múltiplas Redes rádio;

R14 – Permitir que vários utilizadores consigam comunicar com as várias redes, garantindo assim uma redução de meios.

3.3 Proposta de implementação

Arquitetura

Na Figura 3.3 está ilustrada a implementação deste sistema. Podemos verificar que o servidor está ligado a vários rádios, sendo que cada rádio representa uma rede rádio. Existem ainda vários browsers que representam a ligação de vários utilizadores às redes rádio.

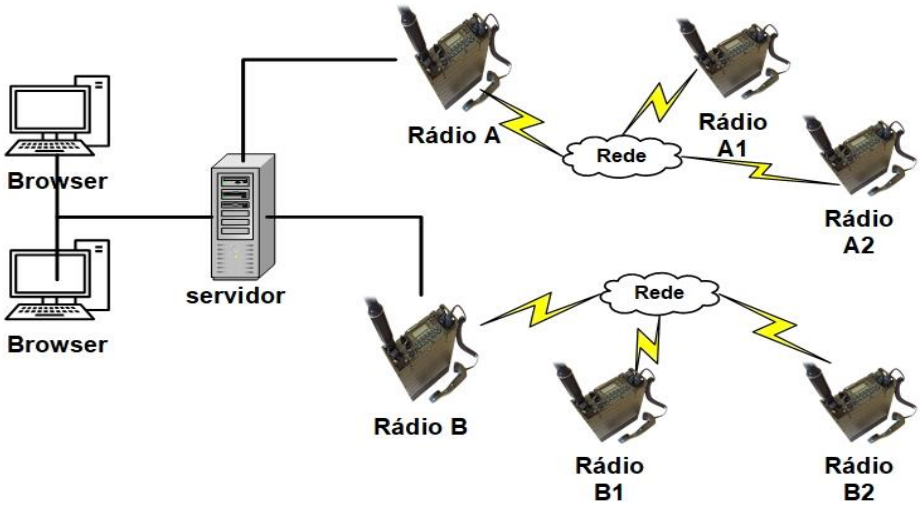


Figura 3.3 - Exemplo da implementação.

Na Figura 3.4 está ilustrada a arquitetura Web. Os rádios têm uma ligação de dados que fornece a entrada e saída de áudio. Estas ligações estão ligadas ao servidor. Existe ainda uma ligação RS232 que permite controlar o PTT do rádio, e uma entrada Ethernet que permite enviar e receber comandos do rádio tático.

O ecrã inicial é aquele onde o utilizador tem de efetuar a autenticação, antes de poder aceder a qualquer outro ecrã. Conforme a autenticação efetuada o utilizador tem acesso a diferentes configurações.

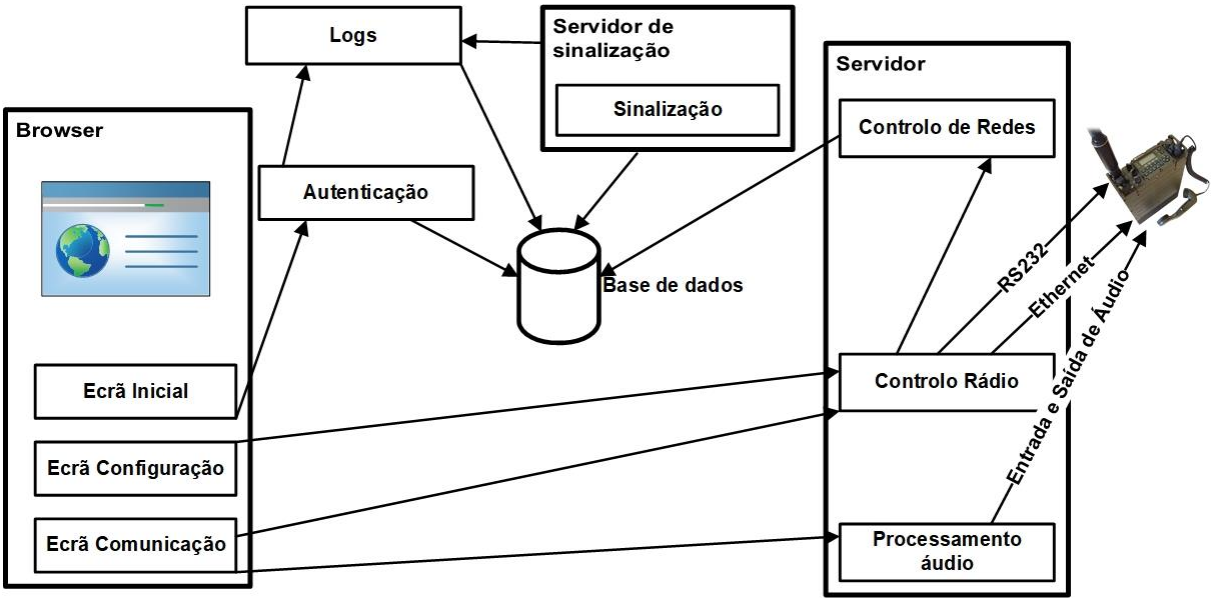


Figura 3.4 - Exemplo da arquitetura Web.

Caso este efetue uma autenticação de operador tem acesso ao controlo rádio. Caso faça autenticação como utilizador de comunicações vai ter acesso ao controlo rádio, assim como ao gstreamer.

3.4 Trabalho desenvolvido

Este subcapítulo é destinado à apresentação de algumas matérias enunciadas ao longo da explicação do sistema desenvolvido. Graças às tecnologias usadas no desenvolvimento desta solução, foi possível simplificar sistemas/processos que outrora levariam a implementações mais complexas.

3.4.1 Tecnologias

Foram utilizadas diversas linguagens no desenvolvimento deste sistema, desde Python a HTML, JavaScript e linguagem C.

Neste sistema existem dois servidores, um deles o de sinalização, baseado num existente [41], que permite o registo dos utilizadores para que possam realizar comunicações entre o gstreamer e a aplicação JS em browsers. Antes de iniciarem uma chamada, os utilizadores precisam de se registarem no servidor de sinalização. Este servidor tem de se manter aberto durante toda a chamada. Utilizou-se ainda outro servidor através da framework Flask, que permite criar um servidor com diferentes páginas Web.

O software utilizado para o processamento do áudio foi o Gstreamer. Este é uma framework que permite criar aplicações de *media* em tempo real, e que é pensada para facilitar a criação de aplicações que utilizem áudio e vídeo [36].

O Flask é uma framework web escrita em Python. Esta ferramenta tem a flexibilidade da linguagem de programação Python e prevê um modelo para o desenvolvimento Web. A framework mencionada será o servidor principal da aplicação.

As tecnologias utilizadas para o desenvolvimento da interface gráfica foram HTML e JavaScript.

3.4.2 Processamento de áudio

Para a utilização deste sistema foi necessário criar um ambiente dentro do próprio *ubuntu* para a instalação de várias bibliotecas necessárias. Utilizaram-se vários *plugins* do gstreamer (gst), entre eles gst-*plugins*-base - que são os básicos -, gst-*plugins*-good, ugly e bad. Estes três últimos apresentam vários problemas, ou seja, funcionam apenas em algumas distribuições Linux e necessitam de mais qualidade, daí a necessidade de utilizar um ambiente diferente devido à instabilidade de alguns *plugins*.

Foi utilizado o Gstreamer 1.14, lançado no dia 19 de março de 2018. Foi neste lançamento que este software permitiu o uso de WebRTC.

O módulo de processamento de áudio foi implementado usando o sistema Gstreamer. Este sistema permite integrar diferentes placas de som. Com esta característica é possível controlar diferentes redes rádio. Este sistema permite ainda alterar entre vários codecs de compressão de aúdio.

O protocolo utilizado com esta framework foi o RTP.

3.4.3 Sinalização

Como referido anteriormente, WebRTC permite a troca de dados entre dois dispositivos. A ligação é estabelecida através da negociação das partes, num processo chamado sinalização. O processo de sinalização necessita de pelos menos dois clientes e de uma terceira parte a que chamamos servidor, a partir do qual é possível executar a negociação através de mensagens. Neste projeto foi utilizado uma tecnologia diferente do habitual. Normalmente a comunicação é realizada entre browser-browser, mas neste caso o objetivo é comunicação entre browser e a aplicação gstreamer. Foi importante utilizar o esquema browser-aplicação, pois só assim é possível a comunicação com as diferentes placas de som e diferentes controlador PTT, o que é necessário para desenvolver o sistema proposto. Utilizou-se como ponto de partida ficheiros existentes na plataforma GitHub [41].

Depois do mecanismo para a troca de mensagens, o servidor de sinalização, estar criado é necessário um protocolo para definir a construção das mensagens. Neste caso foram usados objetos JSON para comunicar com os clientes. O conteúdo das mensagens especifica o tipo de menagens, assim como informação adicional para permitir manipular as mensagens adequadamente [42].

Quando se inicia o processo de sinalização, é criada uma oferta pelo remetente. Esta oferta inclui uma descrição de sessão, no formato SDP, e é necessário entregá-la ao destinatário, que, por sua vez, responde com uma resposta que também contém uma descrição SDP. O servidor de sinalização utiliza WebSockets para transmitir estas mensagens de oferta e resposta, que têm os seguintes campos:

- **type** – o tipo pode ser de oferta ou resposta;
- **name** – O nome do remetente;

- **target** – O nome do destinatário;
- **sdp** – String SDP.

A partir deste momento os participantes sabem quais os *codecs* e os parâmetros que irão ser usados para a realização da chamada. Estes ainda não sabem o como transmitir a informação. É neste momento que é necessário usar o *Interactive Connectivity Establishment* (ICE) [42].

Cada mensagem ICE sugere um protocolo de comunicação (TCP ou UDP), endereço IP, número da porta, tipo de ligação (por exemplo se o IP especificado é do próprio utilizador ou de um servidor de retransmissão), juntamente com outras informações necessárias para vincular os dois utilizadores.

Depois de haver a troca de uma oferta e resposta, os dois utilizadores começam a troca de candidatos ICE para negociar a ligação entre eles. Todos os candidatos ICE descrevem um método que o remente é capaz de usar para comunicar. Cada par de utilizadores envia candidatos na ordem em que vão sendo descobertos e continua a enviá-los até ficar sem sugestões, mesmo que o fluxo de dados já tenha iniciado.

Quando os dois pares concordam com um candidato compatível, a SDP desse candidato é usada por cada utilizador para criar uma ligação, através da qual os dados (áudio) começam a fluir. Ao longo da comunicação, se estes concordarem que existe um candidato melhor, ou seja, com um desempenho mais alto, o fluxo de dados pode ser alterado conforme necessário. Por exemplo, se a ligação de rede deteriorar um ou os dois utilizadores podem diminuir a resolução dos dados.

Cada candidato ICE é enviado para outro utilizador através de uma mensagem JSON através do servidor de sinalização para o utilizador remoto. Cada mensagem candidato inclui:

- **type** - o tipo da mensagem: *“new-ice-candidate”;*
- **target** – O nome do remetente com o qual se está a negociar;
- **candidate** – *string* candidato da SDP, descrevendo o método de ligação proposto. Não é necessário examinar o conteúdo desta *string*. Mas sim reencaminhar para o destinatário usando o servidor de sinalização. [42]

  Na Figura 3.9 está um exemplo dos candidatos trocados entre os terminais.

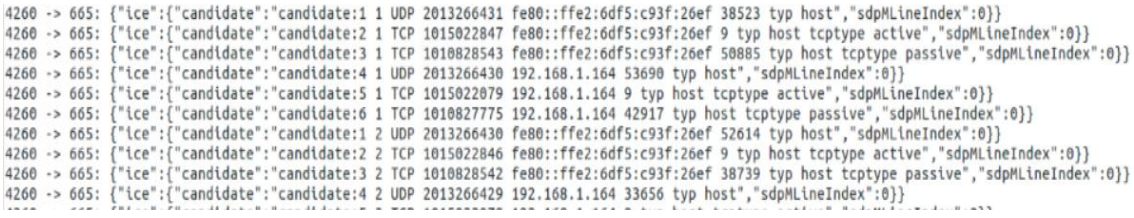


Figura 3.5 – Exemplo de troca de candidatos.

Apresenta-se como exemplo a sinalização das chamadas entre dois terminais, utilizadores. O P/PRC 525 e um soldado.

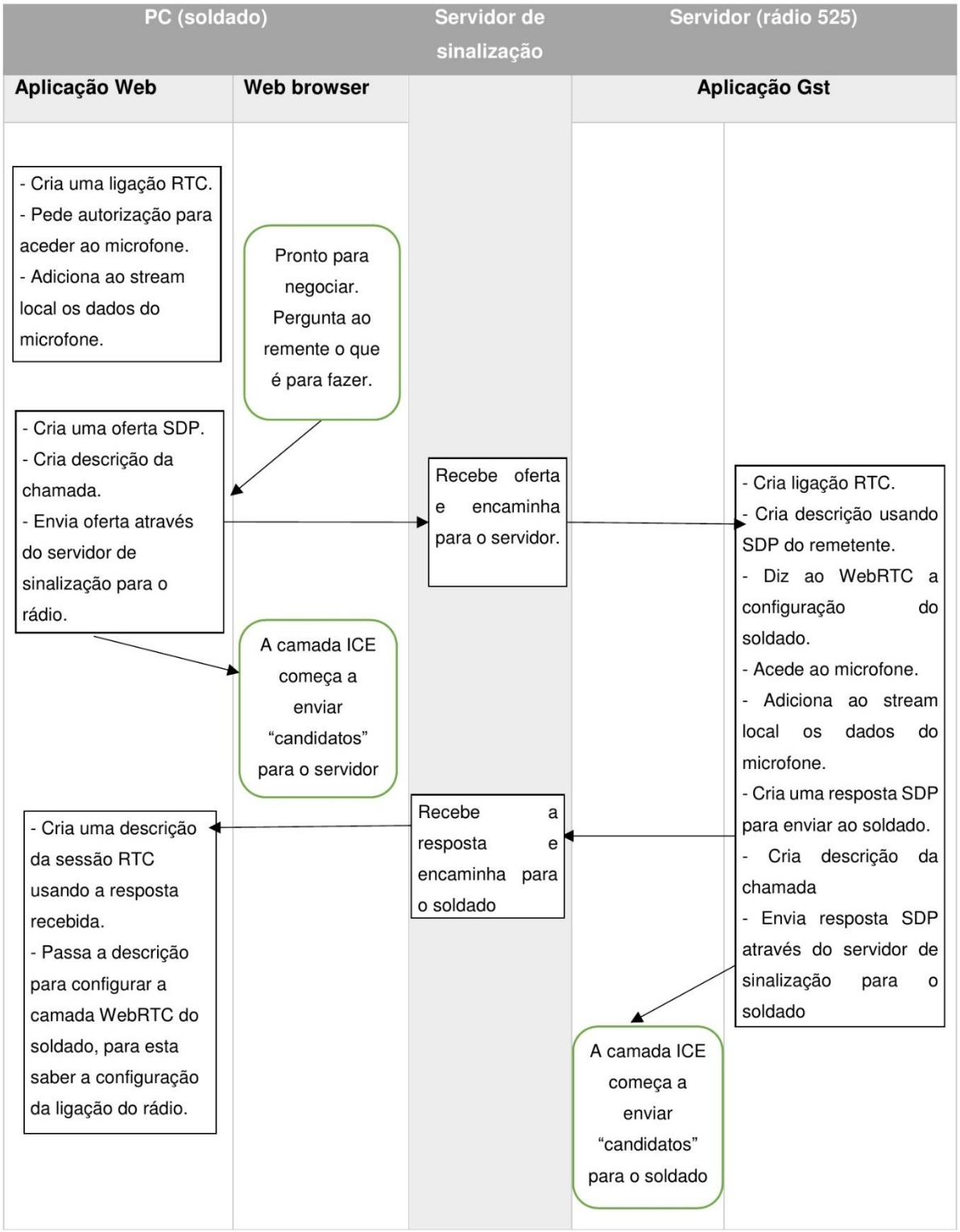


Figura 3.6 - Sinalização das chamadas entre dois terminais

Processo de trocas de candidatos ICE

Quando a camada ICE de cada utilizador começa a enviar candidatos são trocadas várias mensagens:

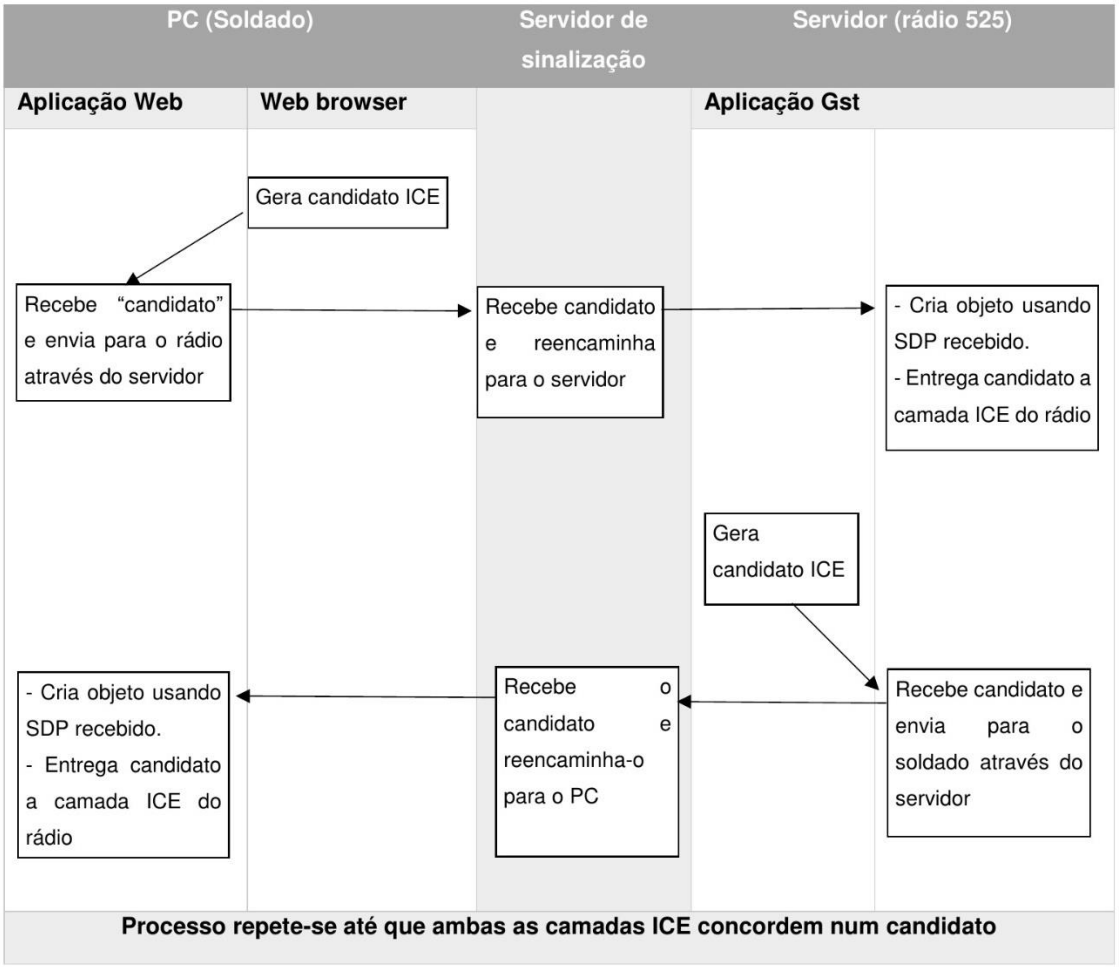


Figura 3.7 - Trocas de candidatos ICE.

3.4.4 Controlo Rádio

É necessário controlar o rádio para ter acesso às mais variadas funções. É essencial ter acesso ao PTT do rádio assim como às informações que sejam possíveis retirar deste. É ainda imprescindível conseguir enviar comandos para o rádio de forma a alterar configurações remotamente.

O botão PTT foi desenvolvido para funcionar de duas maneiras, uma pensada para ser usada em aparelhos táteis e uma outra para ser utilizada em computadores portáteis e fixos.

Caso seja para utilizar em terminais com teclado físico, o botão pode ser ativado pressionando a tecla "espaço". Assim que o utilizador deixa de premir a tecla a comunicação é terminada, mas não a ligação, caso o modo seja ALE3G. Neste caso, o utilizador também pode ativar o botão clicando com rato num botão próprio, tendo de carregar novamente para desativar o PTT. Para este caso, o modo mais prático é carregando na tecla predefinida, pois dá a sensação que está a utilizar o PTT como se fosse em comunicação normal. Neste caso não existe o risco de o utilizador se esquecer do botão ligado e, assim, empastelar as comunicações.

Caso seja para utilizar em sistemas tácteis o utilizador carrega no botão existente para ativar e desativar o PTT.

Gestão de várias redes

O programa C tem o sistema gstreamer a correr dentro do mesmo. Assim sendo, é possível adicionar várias placas de som permitindo adicionar várias redes rádio ao servidor.

Obtenção de dados do rádio

O rádio 525 permite a comunicação IP com um PC para obter vários dados. O servidor Python no Flask acede às informações do rádio através de *sockets*. Para iniciar a ligação é necessário criar uma ligação TCP IP. Este IP tem de pertencer à mesma rede do rádio. É ainda necessário definir uma porta e à necessária uma ligação por cabo Ethernet entre o servidor e o rádio tático.

Depois de se realizarem várias questões a sargentos e oficiais do exército português optou-se pela visualização de algumas das informações que é possível obter do rádio P/PRC 525.

Entre todas os parâmetros possíveis os que são visualizadas na aplicação são:

- Potência.
- Bateria.
- Tipo de Onda.
- Nome do rádio a operar.
- Frequência.
- Estado da chamada.

Na Figura 3.8 verificamos um exemplo do menu que é visualizado pelos utilizadores. Esta informação é atualizada de 10 em 10 segundos.

Informações obtidas do rádio

Bateria em %	Tipo de onda	Nome rádio	Frequência (Hz)	Potência (mW)	Estado Chamada
O rádio está ligado à corrente	Fixed Frequency	gRS37	63775000	1	

Figura 3.8 - Exemplo de como é exibido ao utilizador as informações obtidas do rádio tático.

3.4.5 Hardware de ligação

O servidor comunica com o P/PRC 525 através de cabo Ethernet, de cabo RS232 e de cabo de dados que permite o acesso ao áudio.

Os equipamentos físicos necessários para a instalação do sistema são:

- Rádio e respetivos equipamentos.
- Servidores (computador)
- Cabo Ethernet.
- Cabo desenvolvido.

Para ter acesso ao áudio através da porta de dados foi necessário desenvolver um cabo que permitisse o acesso a este, assim como acesso ao PTT.

Na Figura 3.9 é possível visualizar o painel frontal do rádio tático P/PRC 525. Foi necessário adaptar uma nova ficha de dados de forma a conseguir controlar o PTT e a aceder ao áudio do rádio.

Figura 3.9 - Legenda painel frontal rádio tático P/PRC 525.

Na Figura 3.10 é possível verificar os vários componentes do cabo adaptado. Pode-se verificar que ao cabo de dados foram adicionados dois jack's de entrada e saída de áudio que se ligam ao computador-servidor.

Figura 3.10 - Legenda dos componentes do cabo adaptado.

Foi ainda adicionado um cabo DB9 RS232 que permite controlar o PTT através da ativação do pino quatro, como é possível constatar na Figura 3.11.

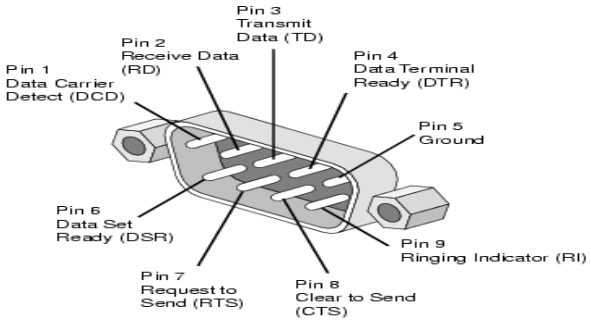


Figura 3.11 - Legenda cabo DB9 RS232 [43].

Na Figura 3.12 é possível verificar o terminal do cabo adaptado onde se confirma que dos 22 pinos existentes apenas se usaram 6, foram eles:

- Entrada áudio
- Saída áudio
- PTT
- Restantes três pinos são massas. Cada uma correspondendo a um dos outros 3 pinos. Estas massas encontram-se todas interligadas.

Figura 3.12 - Parte macho do cabo de dados adaptado.

3.4.6 Interface gráfica

Na Figura 3.13 visualizamos a hierarquia de menus existente na aplicação.

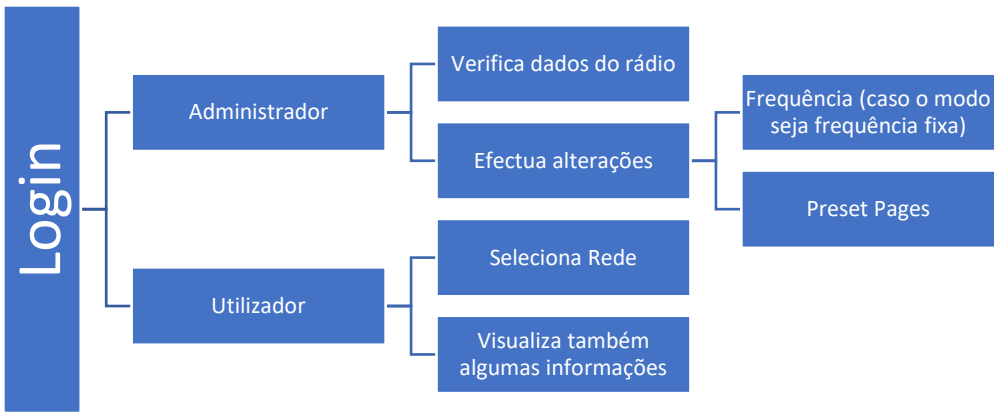


Figura 3.13 - Hierarquia de menus.

Com a Figura 3.13 é possível compreender que a cadeia de operações possíveis se inicia com o login. Este esta associado a dois modos possíveis, o de utilizador de comunicações e o de administrador. Quando se realiza o login como administrador, existe a possibilidade de visualizar informações do rádio e de efetuar alterações no mesmo, de frequência e de *Preset Pages*. As *Preset Pages* são “páginas” pré-configuradas. O utilizador poder alterar fisicamente o comutador do rádio para alternar entre estas páginas. Agora este também o pode realizar através da aplicação Web.

Caso seja o login de utilizador, este pode selecionar a rede com a qual quer comunicar e também tem a oportunidade de visualizar informações do rádio.

No modo ALE3G, o estabelecimento de chamadas tem várias fases - chamada em progresso, chamada ativa e falha de chamada. O utilizador deste sistema verifica todos estes estados no browser e sabe quando pode falar, pois quando entra no modo chamada ativa aparece uma imagem com a informação de que pode falar. Na Figura 3.14 pode-se visualizar um exemplo do menu que a aplicação apresenta para o modo ALE3G.

Figura 3.14 - Exemplo chamada em ALE3G.

Neste modo aparece ainda um botão que permite ao utilizador desligar a chamada. Nos restantes modos estudados, estes botões não são necessários pois a chamada está sempre ativa, bastando ao utilizador premir o botão PTT para comunicar.

O responsável pelas comunicações pode ainda, neste modo, selecionar qual o destinatário para o qual quer efetuar a chamada. Na Figura 3.15 está representado um exemplo gráfico desse menu.

Figura 3.15 - Exemplo de lista com destinatários no modo ALE3G.

A Figura 3.16 permite visualizar o esquema das opções disponíveis para cada modo de comunicação.

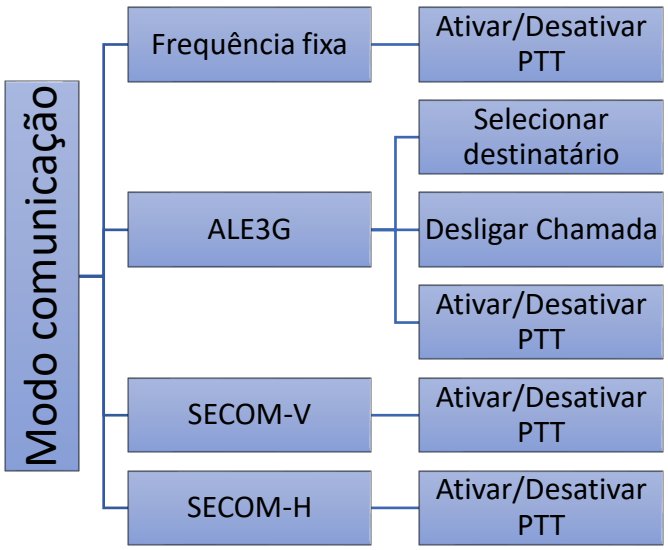


Figura 3.16 - Modos de comunicação.

3.5 Demonstração

Ao longo do desenvolvimento deste sistema foram sendo realizados vários testes com operadores militares. Existiu ainda uma demostração em campo do sistema em funcionamento.

3.5.1 ALE3G em funcionamento

O modo ALE3G no rádio tático é o mais funcional no que diz respeito à sua utilização no Exército Português. O rádio permite que lhe seja carregado as configurações através da *fill gun* (Figura 3.17) um grande número de terminais rádio. A *fill gun* tem um funcionamento idêntico a uma *pen* comum, mas é mais robusta e tem um adaptador para a transferência de dados para o rádio tático.

Figura 3.17 - *Fill gun*.

Um caso prático deste modo é a utilização de um rádio, em que o utilizador consegue alternar entre vários destinatários. No visor do rádio, quando selecionamos o contacto a quem queremos comunicar e depois de premirmos o PTT que inicia a chamada, são mostradas várias mensagens, entre elas:

- CALL_TO_IN PROGRESS
- CALL_ACTIVE
- CALL_FAILED

Através da aplicação desenvolvida, o utilizador pode visualizar no browser os vários destinatários possíveis e selecionar aquele com quem quer estabelecer uma chamada. Depois disto, a chamada começa a ser estabelecida e o utilizador é avisado sobre quando é que pode começar a comunicar.

Um caso prático desta utilização é a possibilidade de instalar este sistema num rádio que esteja colocado num ponto estratégico, onde tenha carregado nas suas configurações os contactos das várias unidades do Exército. Assim, um utilizador que esteja colocado em qualquer unidade do Exército e que esteja ligado à rede de dados deste ramo das forças armadas consegue comunicar para qualquer parte do país, incluindo ilhas. Vejamos, por exemplo:

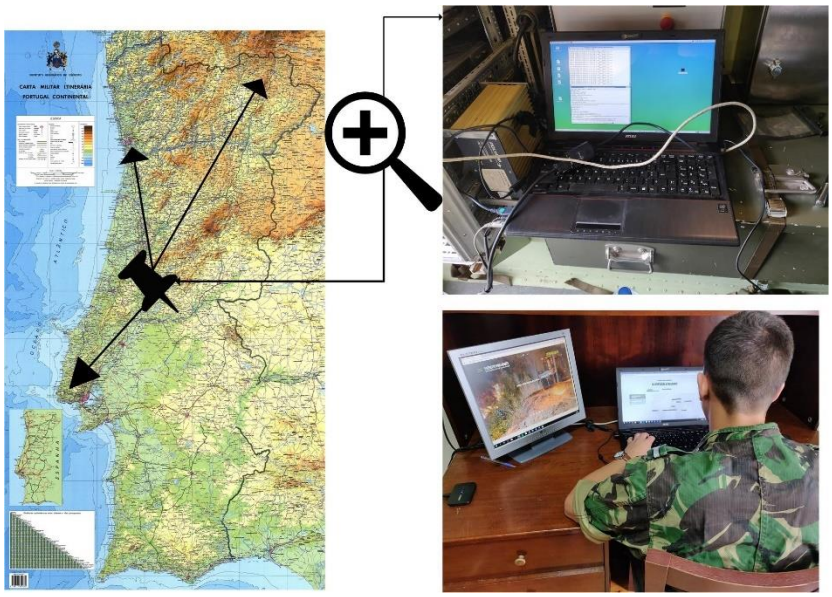


Figura 3.18 - Exemplo de utilização do sistema. Na imagem do mapa de Portugal podemos visualizar o pino que indica onde se encontra o sistema instalado. Na imagem à direita e em cima encontra-se o sistema ligado ao computador, na imagem em baixo vemos um exemplo de um utilizador a usar a aplicação.

3.5.2 Testes de Campo

Campo militar Santa Margarida

Durante o dia 10 de julho de 2018, no terceiro Bloco de Formação Militar (BFM) da Academia Militar, foram executados alguns testes ao sistema, com o propósito de determinar se o sistema desenvolvido, numa face inicial, era uma solução simples e de fácil manuseamento.

Para estes testes, foi utilizado a seguinte cablagem:

- Cabos Ethernet para montagem RJ-45;
- Cabo de dados para ligação do rádio ao computador.

No terreno encontrava-se a decorrer um exercício militar, Leão 18, no qual os alunos simulam ações militares. Este sistema foi testado num grupo de militares de transmissões. Existiam viaturas militares nos quais estava uma montagem veicular do rádio tático, como se pode ver na Figura 3.19. Este rádio estava ligado a uma rede rádio onde era possível comunicar com os vários postos de comando das subunidades subordinadas.

Figura 3.19 - Montagem veicular.

Como se observa, o computador portátil estava ligado ao P/PRC 525 através do cabo RJ-45, onde previamente se criou uma ligação com o IP do rádio para se encontrarem na mesma rede, permitindo a troca de dados entre ambos. Utilizou-se ainda o cabo de dados para controlar o PTT e para se ter acesso ao áudio de entrada e saída. Para efeitos de teste utilizou-se um tablet para aceder à aplicação através de wireless. Usou-se também um router que serviu de ponto de acesso para permitir a ligação do tablet ao servidor.

Assim, os militares que estavam a operar o rádio não necessitavam de se encontrar dentro da viatura militar. A rede wireless foi usada na demonstração devido à facilidade da montagem. Em uso real deve ser usada rede cablada, de modo a garantir segurança.

Neste exercício o sistema estava apenas a funcionar para frequência fixa, mas foram realizadas perguntas a sargentos e oficiais que deram a sua aprovação no que diz respeito à perceção das comunicações.

Na Figura 3.20 encontra-se uma fotografia com a aplicação a correr no tablet.

Figura 3.20 - Aplicação a correr no tablet.

Paço de arcos

Foi na Equipa de Apoio em Engenharia para o Projeto SIC-T que a parte de testes ao longo do desenvolvimento deste trabalho foi testada. Enquanto que no exercício Leão 18 apenas se testou a frequência fixa, na unidade de Paço de Arcos foi possível testar todas as outras formas de onda. Nesta unidade também se realizaram testes através de ligação física de IP, onde se verificou que o sistema também funciona. Foi ainda testada a funcionalidade de alterações de parâmetros do rádio, como a alteração de frequências. Nesta unidade contou-se com a ajuda de vários militares, que, ao longo do desenvolvimento de trabalho, deram vários contributos sobre quais as funcionalidades que achavam necessárias e quais as que poderiam ser mais úteis no Exército Português. Foram ainda estes militares que ajudaram a realizar os vários testes de qualidade do áudio.

3.6 Avaliação

Neste subcapítulo, são abordados os aspetos referentes à avaliação das funcionalidades apresentadas pelo sistema.

As formas de onda a que este sistema foi desenvolvido e testado são: SECOM-V, SECOM-H, frequência fixa e ALE3G. Foram estas formas de onda pois são as mais utilizadas no dia a dia do Exército. Nos subcapítulos seguintes foram realizados diversos testes para compreender a eficácia do sistema desenvolvido.

3.6.1 Teste Funcionamento Browser

Os browsers mais comuns são o Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explorer, Opera e Safari [44].

Procedeu-se à instalação de todos os browsers, exceto o Safari e I.E. Na Tabela 3.4 verifica-se que o sistema funciona em todos os browsers testados.

Tabela 3.4 – Funcionamento nos diversos browsers.

Browser	Firefox	Chrome	Edge	Opera
Funciona	✔	✔	✔	✔

3.6.2 Qualidade da comunicação

Para realizar a avaliação quantitativa foi escolhido um teste idêntico ao MOS, ou seja, uma avaliação dada pela opinião pessoal dos próprios utilizadores. As gamas de valores para avaliação variavam entre 0 e 5 onde 0 corresponde a péssima qualidade e 5 a excelente qualidade.

Para esta avaliação foi pedido a 10 utilizadores que ouvissem áudio e avaliassem a respetiva qualidade. Para estes testes foi lido aos utilizadores o mesmo texto. Este texto foi composto por cerca de 20 palavras.

O objetivo destes testes foi a avaliação de três casos de estudo:

- Comunicar através do browser e o utilizador ouvia no rádio militar
- Comunicar através do P/PRC 525 e o utilizador ouvia na aplicação.
- Comunicar através do P/PRC 525 e o utilizador ouvia num rádio tático

O último teste tem o objetivo de realizar uma comparação do novo sistema para a comunicação já existente e dita normal.

Os testes foram realização através de ligação wireless entre o servidor e o terminal (onde de acedeu à aplicação) e através de cabo Ethernet.

Nas tabelas seguintes é possível verificar os resultados das avaliações realizadas.

1. **Entrada e saída de áudio no rádio tático.**

Tabela 3.5 - Comparação entre os tipos de onda no caso entrada e saída áudio no rádio.

Tipo comunicação	Pontuação MOS (cabo)
Frequência fixa	4,57
ALE3G	4,14
SECOM-V	5
SECOM-H	4,57

Os resultados da Tabela 3.5 foram os esperados. Os modos SECOM têm uma pontuação elevada pois a transmissão da voz é digital. O modo frequência fixa também obtém uma pontuação idêntica à comunicação digital. O modo ALE3G foi o que apresentou uma pontuação mais baixa.

2. Entrada de áudio no browser, saída no rádio.

Tabela 3.6 - Comparação entre os tipos de onda no caso de entrada de áudio no browser e saída no rádio.

Tipo comunicação	Pontuação MOS (cabo)
Frequência fixa	4,43
ALE3G	3,71
SECOM-V	4,57
SECOM-H	4,43

Neste caso, Tabela 3.6, os modos SECOM mantêm-se com uma pontuação mais elevada, a par da frequência fixa. Já o modo ALE3G é o que tem uma pontuação inferior, mas superior à média da escala de avaliação, 2.5.

3. Entrada de áudio no P/PRC 525, saída no browser.

Tabela 3.7 - Comparação entre os tipos de onda no caso de entrada de áudio no rádio e saída de áudio no browser.

Tipo comunicação	Pontuação MOS (cabo)
Frequência fixa	3,71
ALE3G	2,43
SECOM-V	3,29
SECOM-H	3,14

Como se pode verificar na Tabela 3.7, o modo frequência fixa foi o que apresentou um melhor resultado. Os modos SECOM mantêm-se com uma elevada pontuação. O ALE3G neste caso tem uma pontuação inferior a 2.5.

Na Figura 3.21 encontra-se um resumo das três tabelas anteriores.

Em todos os modos é possível chegar à mesma conclusão: o melhor resultado é na comunicação normal. Logo de seguida quando a saída de áudio ocorre no rádio e por fim no browser.

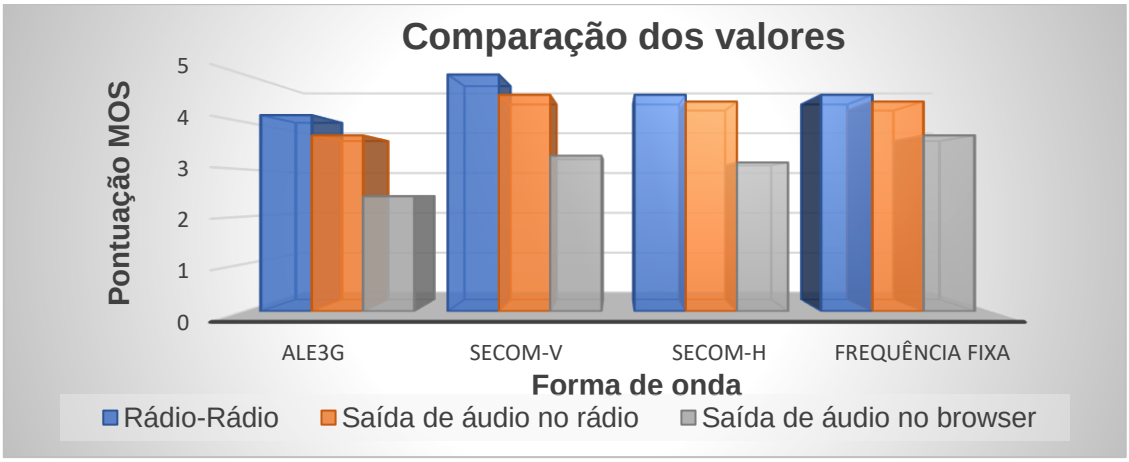


Figura 3.21 - Comparação de todos os resultados obtidos.

O melhor resultado é na comunicação normal, pois os componentes que existem durante as comunicações são aqueles para o qual o rádio foi pensado e construído, apenas o próprio rádio, as antenas e o próprio microauscultador.

O segundo lugar que obtém uma melhor pontuação é na comunicação do browser para o rádio. Conclui-se que o microfone utilizado no browser tem uma melhor qualidade e menos interferências do que o microfone do microauscultador do rádio.

Por último surge a comunicação do rádio para o browser, que obtém uma qualidade inferior, pois o equipamento de entrada de áudio do P/PRC 525 introduz algumas interferências. Assim, como os altifalantes do browser permitem um volume superior ao dos altifalantes do rádio, estas interferências são amplificadas.

Era interessante ter previamente realizado gravações de áudio a sair do terminal com o browser e do auscultador do rádio tático, e só depois pedir aos utilizadores para avaliarem essas faixas de áudio. Assim os utilizadores, caso tenham sido influenciados nos testes realizados, teriam avaliado as faixas sem saberem qual o caso que estavam a avaliar.

3.6.3 Atrasos na comunicação

Um dos aspetos mais importantes e decisivos para a empregabilidade deste sistema é a duração dos atrasos na comunicação, dado que se existir um atraso que não permita uma comunicação fluente não se justifica a sua utilização.

Para avaliar este problema foi criado um teste que permite medir os atrasos na comunicação nos vários cenários. Avaliou-se o atraso do áudio entre o emissor, e o recetor usando dois rádios táticos, um rádio e o browser, e, por último, entre um browser e um P/PRC 525.

Foi necessário um som que fosse rápido e forte o suficiente para que fosse detetado pelo microfone e que tivesse uma intensidade suficiente para ser emitido através do microfone do rádio P/PRC 525. A solução encontrada foi o uso de uma aplicação android, “Gerador de Freqüência” [45], que gera frequências. A frequência que apresentou melhores resultados foi de 1.9KHz. O software utilizado para analisar o áudio foi o *Sonic Visualizer*.

Avaliação entre dois rádios P/PRC 525

Na Figura 3.22 está um esquema da avaliação entre dois rádios P/PRC 525.

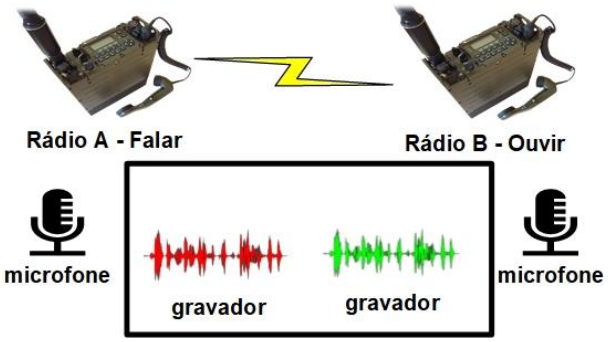


Figura 3.22 - Procedimento para avaliação do atraso de propagação do áudio entre dois rádios.

Os passos para conseguir chegar aos valores concretos foram, sucessivamente

1. Colocação de microfones juntos dos auscultadores dos rádios P/PRC 525.
2. Início da gravação dos áudios dos microfones
3. Utilização de um gerador de frequências num rádio, que serviu de emissor.
4. Comparação dos espectros do áudio e análise da diferença entre o sinal emitido e recebido.

Depois de realizar estes passos procedeu-se à análise espectral do áudio para medir o atraso entre a emissão do ruído produzido pelo gerador de frequências e do som recebido pelo rádio tático.

Na Tabela 3.8 é possível verificar os valores obtidos para o caso rádio-rádio, ou seja, os valores normais durante uma comunicação tática nos diversos modos.

Tabela 3.8 - Avaliação entre rádio-rádio.

Tipo comunicação	Atraso (s)
Frequência fixa	0.117
ALE3G	0.126
SECOM-V	0.715
SECOM-H	1.328

Avaliação para entrada de áudio no browser e saída no rádio.

Na Figura 3.23 está uma demonstração da avaliação entre um browser e entre o rádio militar.

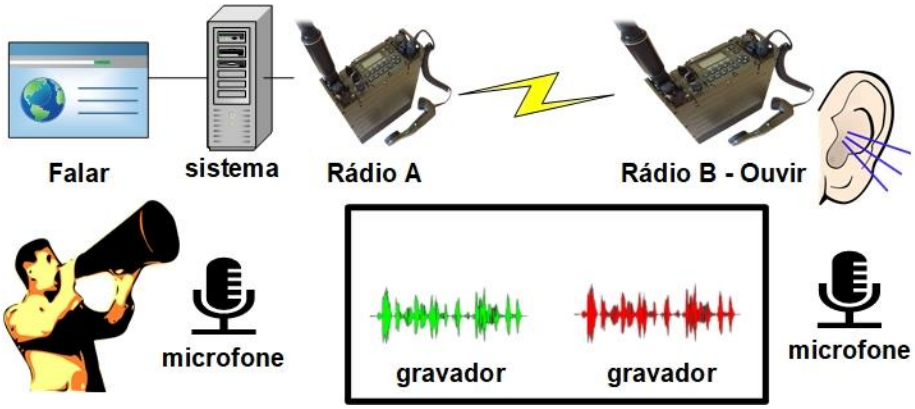


Figura 3.23 - Procedimento para avaliação do atraso de propagação do áudio entre a aplicação e o rádio tático.

Para este caso seguiram-se, ordenadamente, os seguintes passos:

1. Colocação de microfones juntos dos auscultadores do rádio P/PRC 525 e do browser;
2. Início da gravação dos áudios dos microfones;
3. Utilização de um gerador de frequências junto ao browser que serviu de emissor;
4. Comparação dos espectros do áudio e análise da diferença entre o sinal emitido e recebido.

Por fim, procedeu-se novamente à análise espectral do áudio para se conseguir calcular o atraso entre emissão e receção.

Na Tabela 3.9 podemos observar os valores obtidos.

Tabela 3.9- Avaliação onde a saída de áudio foi no rádio tático.

Tipo comunicação	Atraso (s) (cabo)	Atraso (s) (wireless)
Frequência fixa	0.415	0.39
ALE3G	0.4	0.413
SECOM-V	1.106	1.105
SECOM-H	1.702	1.904

Avaliação para entrada de áudio no rádio P/PRC 525 e saída browser.

Na Figura 3.24 está uma demonstração da avaliação entre um rádio tático e entre a aplicação web.

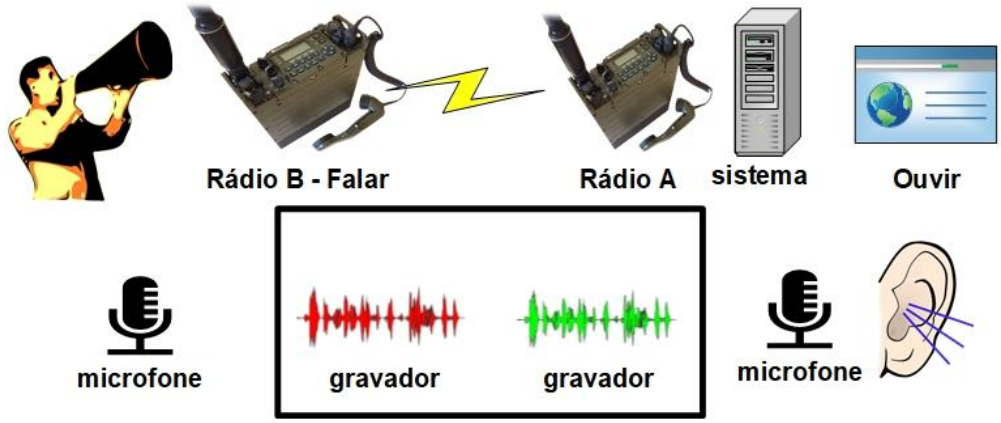


Figura 3.24 Procedimento para avaliação do atraso de propagação do áudio entre o rádio tático e a aplicação.

Para este caso seguiram-se os seguintes passos:

1. Colocação de microfones juntos dos auscultadores do rádio P/PRC 525 e do browser;
2. Início da gravação dos áudios dos microfones;
3. Utilização de um gerador de frequências junto do microauscultador do rádio que serviu de emissor;
4. Comparação dos espectros do áudio e análise da diferença entre o sinal emitido e recebido.

Na Tabela 3.10 seguinte podemos observar os valores obtidos.

Tabela 3.10 - Avaliação onde a saída de áudio é no browser.

Tipo comunicação	Atraso (s) (cabo)	Atraso (s) (wireless)
Frequência fixa	0.406	0.392
ALE3G	0.395	0.386
SECOM-V	1.078	1.103
SECOM-H	1.585	1.834

Comparação dos valores para ligação Ethernet

Na Figura 3.25 é possível observar um gráfico que compara, para cada tipo de forma de onda, os diversos atrasos entre cada modo de utilização possível, em ligação por cabo, relativamente à comunicação normal (barras azuis).

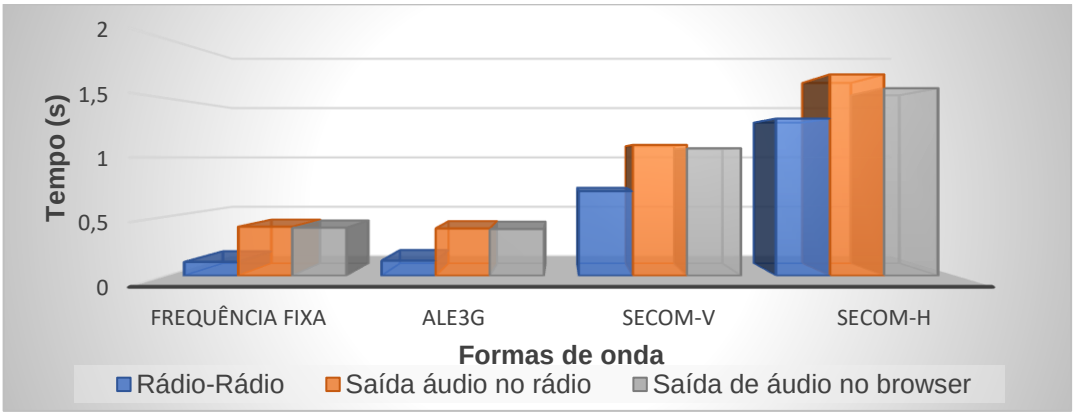


Figura 3.25 – Comparação dos valores para ligação Ethernet.

Como era de esperar, o modo de utilização que apresenta menores atrasos em todas as formas de onda é o rádio-rádio, pois, uma vez mais, os componentes existentes neste modo de utilização são os de origem, não havendo nenhum componente a causar atrasos. Sendo este o modo para o qual os rádios estão construídos é uma observação esperada. Os modos em que a transmissão de dados não é digital apresentam valores de atraso na comunicação menores. Nestas formas de onda, ALE3G e frequência fixa verificamos que a circulação de áudio nos dois sentidos quando se utiliza este sistema é idêntica no que diz respeito aos atrasos.

Nas formas de onda cujos dados são transmitidos digitalmente existe um maior atraso nas comunicações, o que também é expectável, considerando que o rádio precisa de tempo para processar os dados.

Em todas as formas de onda podemos ainda verificar que existe um maior atraso quando o utilizador comunica através do browser. Esta diferença de atrasos é mínima e pode ter ocorrido devido a erros de medição.

Comparação dos valores para ligação sem fios.

Na Figura 3.26 é possível observar um gráfico que compara para cada tipo de forma de onda os diversos atrasos entre cada modo de utilização possível em ligação wireless.

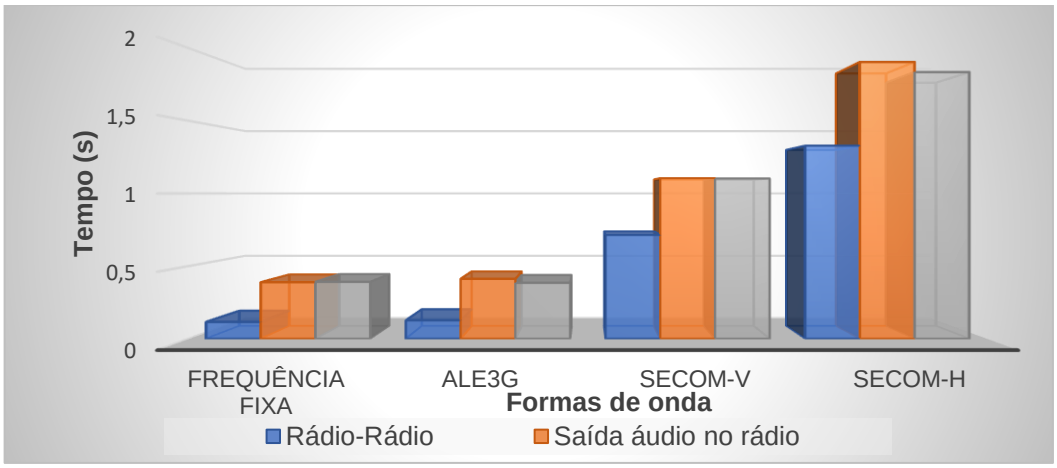


Figura 3.26 - Comparação dos valores para ligação wireless.

Os modos em que a transmissão de dados não é digital apresentam os valores de atraso na comunicação menores, como na ligação por cabo.

Já os modos em que a comunicação é digital apresentam atrasos idênticos nas duas situações possíveis.

Tanto na ligação por cabo como na ligação sem fio, o modo de utilização que apresenta menores atrasos em todas as formas de onda é o rádio-rádio, já que, mais uma vez, não há nenhum componente a causar atrasos. Os modos em que a transmissão de dados não é digital apresentam os valores de atraso na comunicação menores. Nas formas de onda onde os dados são transmitidos digitalmente existe um maior atraso nas comunicações, como na ligação por cabo.

Nestes resultados não há uma diferença tão acentuada em relação ao atraso ser maior quando o utilizador comunica através do browser, embora seja superior. Esta diferença de atrasos é mínima e pode ter ocorrido devido a erros de medição.

Diferença dos atrasos em relação à comunicação normal

Entrada áudio no browser e saída no rádio

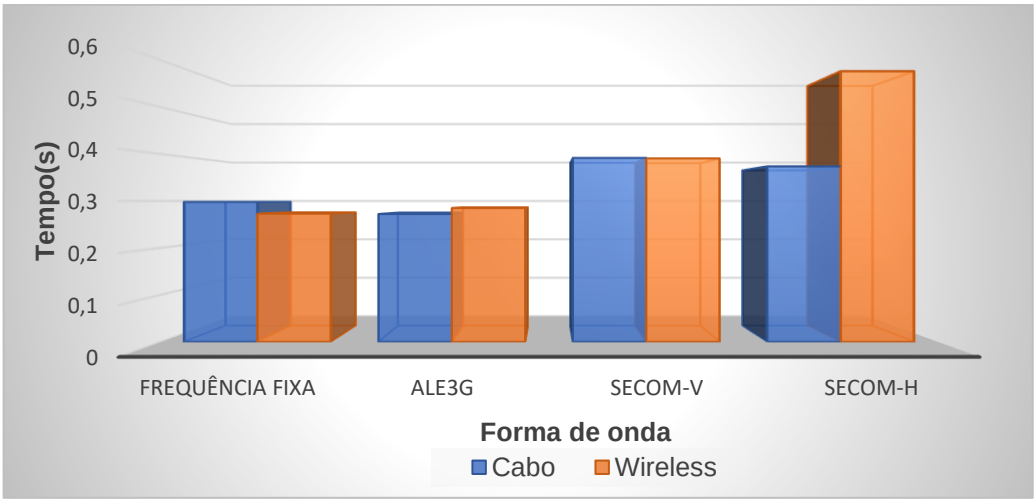


Figura 3.27 - Comparação dos atrasos em relação à comunicação normal. Entrada áudio browser, saída no rádio.

Na Figura 3.27 verificamos que os atrasos onde existe maior diferença de tempo em relação à comunicação normal é a SECOM. No total, a maior diferença em relação à comunicação normal é de cerca de 600 ms, em SECOM-H.

Dentro da mesma forma de onda onde existe uma maior discrepância de valores também é em SECOM-H, na qual se verifica uma diferença superior a 200 ms quando se utiliza o sistema com ou sem fio. Nas ligações sem fios ocorrem mais interferências no envio dos dados. Assim, caso existam mensagens enviadas através de TCP pode existir o reenvio destas mensagens o que causa atrasos na comunicação.

Diferença dos atrasos em relação à comunicação normal

Entrada áudio no rádio e saída no browser

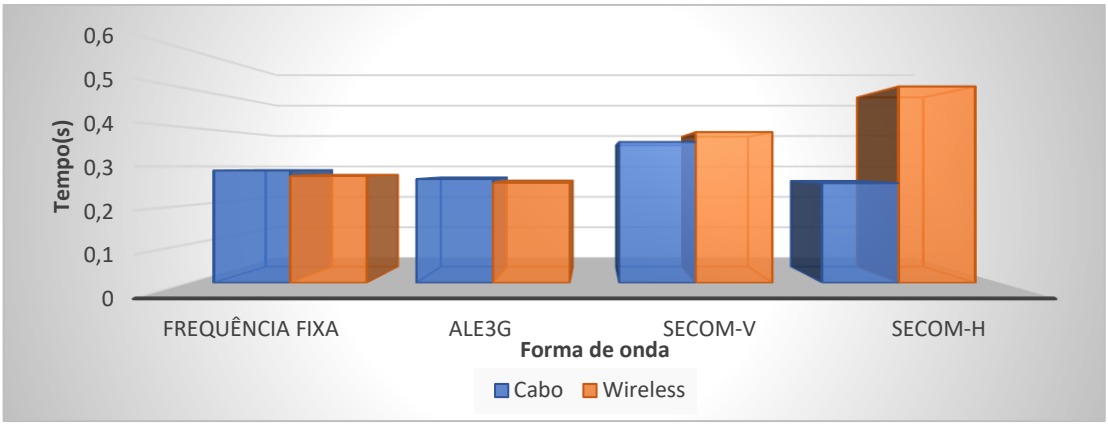


Figura 3.28 - Comparação dos atrasos em relação à comunicação rádio-rádio.

Na Figura 3.28 verificamos, novamente, que a maior discrepância de valores, em relação à forma de ligação (com ou sem fio), acontece em comunicação SECOM-H, na qual se constata também uma diferença superior a 200ms, dentro da mesma forma de onda. Mais uma vez nas ligações sem fios pode existir o reenvio de mensagens o que causa atrasos na comunicação. No total, a maior diferença em relação à comunicação normal é de cerca de 500 ms, em SECOM-H.

Quando a comunicação é analógica, o maior atraso, seja com ou sem fio, em relação à comunicação normal é menor a 320ms, o que é um valor suportável. Na comunicação digital, o maior atraso é de 520 ms um valor considerável, mas que, testando o sistema na prática, não se revela como um atraso que realmente prejudique a comunicação.

3.6.4 Qualitativa

O objetivo desta avaliação qualitativa é obter resultados no que diz respeito à necessidade dos utilizadores finais deste sistema, bem como à sua opinião e expectativas.

Foi assim realizada uma série de inquéritos, disponíveis no anexo C, a seis militares (dois capitães, um tenente, dois primeiros-sargentos e um sargento-ajudante) do exército português que tiveram já contacto com o sistema desenvolvido. Os inquéritos eram compostos por questões e afirmações com avaliação inerente, designadamente:

1. O botão PTT pode ser ativado de duas maneiras: pressionando uma tecla do teclado, sendo o funcionamento idêntico ao do PTT do rádio, ou premindo um botão virtual para ativar/desativar. Avalie de 1 a 5 a sua usabilidade (facilidade de uso).
2. Com este sistema é possível alterar as frequências (modo frequência fixa) e as Preset Pages. Estas configurações são suficientes? Se não, quais considera serem fundamentais?
3. Considera importante a comunicação dita normal ser possível, em conjunto com este sistema desenvolvido, para o caso deste falhar?
4. As informações do rádio a que a aplicação permite aceder são suficientes para este tipo de sistema (bateria, potência, tipo de onda, frequência, estado da chamada (ALE3G))?

Na Tabela 3.11, em que avaliação pedida foi de uma escala de 1 (nada útil) a 5 (extremamente útil), e na Tabela 3.12, cuja avaliação solicitada era “sim” ou “não”, é possível observar um resumo dos resultados obtidos nos inquéritos. Verificamos que as grandes percentagens se encontram nos valores de 4 e 5, o que revela que os inquiridos acham úteis as funcionalidades implementadas.

Tabela 3.11 - Resumo inquérito.

Questão/Avaliação	1	2	3	4	5
1ª	0%	0%	0%	33.3%	66.7%
4ª	0%	0%	0%	33.3%	66.7%

Tabela 3.12 - Resumo inquérito.

Questão/Avaliação	Sim	Não
2ª	66.7%	33.3%
3ª	83.3%	16.7%

3.7 Validação dos Requisitos

Neste subcapítulo procedeu-se à validação dos requisitos propostos a serem cumpridos no subcapítulo 3.2.2. O resultado dessa validação pode ser encontrado na Tabela 3.13.

Tabela 3.13 - Validação dos requisitos.

Requisitos:	Validação
R1	Os utilizadores conseguem comunicar com as redes táticas a partir do seu Web Browser. Foi testada ligação wireless e Ethernet.
R2	Os utilizadores conseguem comunicar com as diversas redes rádio existentes
R3	Os militares mais vocacionados para a parte da manutenção dos rádios, os operadores, conseguem observar na aplicação o estado destes, assim como realizar configurações, tudo remotamente. Com o desenvolvimento deste sistema, os militares conseguem realizar a manutenção básica dos rádios, visualizando vários parâmetros, assim como realizar diversas configurações, desde a alteração de frequências como das -*Preset Pages*, e, por sua vez, alternar entre as várias formas de onda dos rádios. O PRC/525 possui no seu modo básico de funcionamento 100 *Preset Pages* pré-programadas, 10 delas selecionadas através do comutador existente no painel do rádio. Todas as *Preset Pages* são configuradas num programa próprio, *Mission Planner*, e são depois transferidas para o rádio. O utilizador do sistema desenvolvido consegue também realizar a alteração de *Preset Pages,* não havendo necessidade de este alterar o comutar fisicamente.
R4	O sistema garante a qualidade necessária das chamadas entre aplicação-rádio e rádio-aplicação. Os resultados do MOS mostram que a qualidade da comunicação usando VOI525 é semelhante à da comunicação usando apenas rádios.
R5	A aplicação web corre sobre o protocolo HTTPS, o que garante que os dados sejam transmitidos por meio de uma ligação criptografada e que verifique a autenticidade do servidor e do cliente por meio de certificados digitais. Este foi também pensado para ser corrido em rede segura, ou seja, na rede de dados do exército. Assim sendo, se a própria rede for segura a segurança está garantida.
R6	O sistema desenvolvido tem gestão de acessos para garantir que apenas pessoas autorizadas têm acesso ao mesmo.
R7	O sistema criado tem ainda o registo das alterações efetuadas, permitindo ao operador consultar os registos das chamadas assim como as alterações efetuadas.
R8	O sistema funciona nos modos SECOM
R9	O sistema está desenvolvido como foi proposto, ou seja, a aplicação final é acedida através do browser. Assim, o objetivo é permitir que qualquer utilizador com acesso a um terminal browser consiga trabalhar com o sistema sem a necessidade de instalação de vários programas

R10	Foi testada a utilização do sistema a grandes distâncias através de IP, conseguindo-se utilizar o sistema. A rede do exército oferece segurança e ligação para longas distâncias.
R11	O sistema tem um botão PTT idêntico ao modelo normal
R12	Os utilizadores conseguem também utilizar a comunicação normal em conjunto com o sistema, caso ocorra alguma falha no sistema
R13	O sistema permite ainda integrar várias redes rádio
R14	O protótipo desenvolvido tem um *bug* que apenas permite comunicar com um browser para cada rede rádio. Foi desenvolvida uma aplicação JavaScript que permite que vários utilizadores consigam comunicar com o rádio tático, mas apenas com o áudio numa direção, no sentido browser-rádio. Futuras versões permitirão com este sistema, que vários utilizadores possam comunicar em ambas as direcções.

Na Tabela 3.14 encontra-se o resumo da validação de todos os requisitos propostos.

Tabela 3.14 - Resumo da validação dos requisitos.

Funciona? / Requisitos	Sim	Não
R1	✓	
R2	✓	
R3	✓	
R4	✓	
R5	✓	
R6	✓	
R7	✓	
R8	✓	
R9	✓	
R10	✓	
R11	✓	
R12	✓	
R13	✓	
R14		✗

4. Discussão

O sistema desenvolvido acaba por se tornar numa grande ferramenta em relação aos sistemas atuais. O requisito da interoperabilidade que permite a comunicação através do browser a partir de qualquer terminal que permita o acesso a estes tornou-se na maior inovação deste sistema no Exército Português.

Uma das maiores vantagens para os comandantes e gestores relativamente aos sistemas atuais é a possibilidade de poder configurar os rádios táticos, assim como comunicar com este sem serem necessários uma instalação e sistema operativo específico, sendo preciso apenas um terminal com acesso à rede IP. Este sistema foi pensado para ser utilizado na rede de dados do exército, de forma a garantir um melhor controlo de acessos.

Embora o requisito da escalabilidade não tenha sido implementado no seu pleno, o sistema resolve vários problemas e acrescenta uma grande mobilidade aos vários utilizadores. Se o objetivo do utilizador for realizar a configuração do rádio ou aceder às suas informações, podem fazê-lo vários utilizadores.

A comunicação propriamente dita está atualmente a funcionar nos dois sentidos apenas com um utilizador, o que por si não deixa de trazer vantagens. Este bug pode dever-se ao facto do Gstreamer permitir a tecnologia WebRTC muito recentemente. Imaginemos que está um rádio montado a alguns metros em terreno bastante irregular e de difícil acesso, encontrando-se aí por razões táticas ou técnicas. O utilizador pode aceder a esse rádio e efetuar as comunicações normalmente como se estivesse a operá-lo fisicamente.

Neste momento, o sistema desenvolvido pode ser usado no problema encontrado no capítulo 3 dos bunkers. Podemos assim garantir que não existem grandes perdas devido ao cabo coaxial, assim como foi reduzido o custo da ligação, pois os cabos coaxiais têm um preço superior aos cabos de rede. Foi aumentada a segurança dos militares que estejam a trabalhar dentro de instalações subterrâneas, pois este sistema dificulta, em caso de guerra eletrónica, a triangulação e, por consequência, localização das fortificações. Garante-se assim a segurança dos utilizadores e das próprias instalações.

Quanto à viabilidade do sistema verificamos na Tabela 4.1 para a situação em que a saída de áudio ocorre no rádio que a maior diferença é em wireless para o modo de comunicação SECOM-H, tendo o valor de 0.6 segundos. Na Tabela 4.2, para a situação em que a saída de áudio ocorre no browser, a maior diferença é também na ligação sem fios e tem o valor de 0.51 segundos.

Tabelas 4.1 e 4.2 – Diferença de tempo à comunicação normal saída de áudio no rádio (4.1) e saída de áudio no browser (4.2).

Saída áudio Rádio	Cabo (s)	Sem fios (s)
Frequência fixa	0,30	0,3
ALE3G	0,27	0,28
SECOM-V	0,39	0,39
SECOM-H	0,37	0,58

Saída áudio Browser	Cabo (s)	Sem Fios (s)
Frequência fixa	0,29	0,28
ALE3G	0,27	0,26
SECOM-V	0,36	0,39
SECOM-H	0,26	0,51

Estas diferenças quanto à ligação ser através de cabo ou sem fios podem dever-se ao WebRTC. Como se verificou quando há negociação de ambos os utilizadores existem trocas de mensagens. Estas podem utilizar UDP ou TCP, conforme as configurações de rede. Caso as trocam utilizem TCP o destinatário tem de receber todos os dados enviados, ou seja, podem ocorrer atrasos no processamento do áudio, pois o remente só continua o processo depois de garantir que foram recebidos todos os dados enviados. Nas ligações sem fios é evidente que ocorrem mais interferências no envio dos dados, logo os atrasos obtidos são também superiores quando a ligação é sem fios.

Os tipos de comunicação em SECOM obtiveram uma boa pontuação MOS pois a transmissão dos dados é digital. Em frequência fixa o áudio também é bastante percetível. Por sua vez, no modo ALE3G o áudio tem menos qualidade. A menor pontuação MOS do modo ALE3G em relação ao modo de frequência fixa é devida à diferente modulação utilizada nestes modos de comunicação. No modo de frequência fixa foi utilizada modulação em frequência, enquanto em ALE3G foi utilizada modulação em amplitude. A modulação AM tem uma qualidade de som inferior, mas pode ser transmitida a maiores distâncias, enquanto que a modulação FM tem menos interferências que a modulação AM, garantindo uma qualidade de som superior apesar de a distância de transmissão que esta modulação permite ser menor.

No capítulo dois, aquando do estudo do trabalho relacionado, foi mencionado o protocolo SIP e H.323, assim como os softwares que permitiram trabalhar com estes protocolos. Contudo devido ao facto de os rádios utilizarem o PTT para iniciar e encerrar comunicações, e estando estes em receção constantemente, chegou-se à conclusão de que os sistemas utilizados facilitavam bastante o desenvolvimento do sistema final, assim como ao seu manuseamento.

Os softwares utilizados para desenvolver o produto final encontram-se em fases de desenvolvimento, pelo que o não sucesso do requisito da escalabilidade pode estar associado a este fator, dado que os *plugins* utilizados ainda não são estáveis e encontram-se em desenvolvimento, por serem *open source.*

Um problema encontrando nas comunicações é a existência de eco, mas este é praticamente instantâneo. Quando se comunica rádio-rádio, comunicação normal, estes apresentam um pequeno eco. Quando se utilizam as comunicações com o sistema desenvolvido, este eco é superior pois os altifalantes dos terminais normalmente têm uma potência superior, que acaba por amplificar o eco.

5. Conclusão e Trabalhos Futuros

Toda a investigação e trabalho desenvolvidos no âmbito desta dissertação abrangem um tema com aspetos problemáticos presentes no dia-a-dia do Exército Português.

Este problema consiste numa falta de integração de meios de comunicações e capacidade de adaptação às novas tecnologias nos tempos atuais. Capacidade de adaptação no que diz respeito à necessidade dos comandantes se encontrarem à distância dos postos de comando, na capacidade de ter acesso a informações relevantes dos equipamentos táticos (os rádios) na capacidade de efetuar alterações remotas e tudo através de browsers. De igual modo, este problema dificultava a ação de comando dos líderes de uma força.

Com base nos sistemas de informação e comunicação estudados dentro do Exército, foi projetada uma solução que implementa um conceito de sistema de comunicações e acesso a informação de meios rádio aplicável no panorama atual do Exército.

Numa primeira instância, este sistema procura colmatar os problemas previamente levantados, ao cumprir com os objetivos definidos no capítulo I. O resultado deste cumprimento materializou-se numa ferramenta de comando e controlo para os comandantes de operações e situações táticas enquadrados nesta temática. Para este sistema, foram aplicados requisitos de *software* com as implicações práticas associadas a estes tipos de situações.

Ou seja, foi desenvolvido um sistema baseado num modelo cliente-servidor, em que a aplicação cliente se encontra programada para *browsers*, utilizados pelos militares no terreno, ou em qualquer instalação fixa com acesso à rede do Exército, de modo a garantir segurança e controlo de acessos, enquanto o servidor processa toda a informação proveniente desses e guarda todos os registos das alterações e operações efetuadas. Além disso, foram desenvolvidos os perfis de acesso para os responsáveis das comunicações e para os operadores, de forma a conceder permissões diferentes a cada perfil de acesso.

Além das vantagens descritas no capítulo anterior, o objetivo da dissertação foi cumprido ao conseguir resolver o problema descrito no capítulo I. Apesar de esta solução não se encontrar inteiramente pronta no que diz respeito à escalabilidade, sendo necessárias algumas melhorias para a sua estabilidade e integração na rede atual do Exército, funcionou como demonstrador das potencialidades e como prova de conceito da integração de comunicação digital (WebRTC) com a rede de comunicação tática.

Em trabalhos futuros, a principal característica a ser implementada é a escalabilidade, de forma a permitir o fluxo bidirecional de áudio para N utilizadores. Outra característica importante será a tentativa de utilizar diversos *codecs* para reduzir o tempo de processamento e, por sua vez, diminuir os atrasos nas comunicações.

Devido à limitação de material no momento do desenvolvimento deste sistema, não foi possível testar a integração de múltiplos rádios num servidor. Será importante também realizar este teste.

6. Referências

[1] Fundação Portuguesa das Comunicações, *TELE-COMUNICAÇÕES MILITARES - Inovação e Soberania Nacional,* Maiadouro, 2008.

[2] Ribeiro, Cor Tm (Eng.º) Carlos J. Oliveira, "Plano de Implementação Redes Táticas de Rádio de Combate," 2017.

[3] A. Geraldes, "Importância Estratégica das Telecomunicações," Instituto da Defesa Nacional, Lisboa, 1994.

[4] J. A. Barrosa, "O Sistema de Informação e Comunicações Táctico (SIC-T)," Institudo de Estudos Superiores Militares, Lisboa, 2007/2008.

[5] L. Rosa, "O sistema de Comando e Controlo das Unidades da componente terrestre do sistema de forças," Institudo de Altos Estudos Militares, Lisboa, 1999.

[6] "Exército Português, Publicação Doutrinária do Exército 3-00 - Operações, Lisboa: Ministério da Defesa Nacional," 2002.

[7] Estado Maior do Exército, Operações RC 130-1 Cap IV, Exército Porutuges, 1987.

[8] Academia Militar, Proelium, Lisboa: Centro de Audiovisuais do Exército, 2005.

[9] Empresa de Investigação e desenvolvimento de electrónica, RÁDIO TÁCTICO HF/VHF/UHF TR-525 Manual de Operação e Manutenção.

[10] M. DESANTIS, "Understanding Voice over Internet Protocol," US-CERT, US, 2008.

[11] "PLURALSIGHT," [Online]. Available: https://www.pluralsight.com/blog/it-ops/voip-signaling-protocols. [Acedido em 14 11 2017].

[12] M. Elgindy, "Telecomunications blog," [Online]. Available: https://gsmcommunications.blogspot.com/2012/04/voip-protocols.html. [Acedido em 05 Setembro 2018].

[13] D. Baron, "SIP Basics," Massachusetts Institute of Technology, Massachusetts, 2005.

[14] CISCO, "CISCO," [Online]. Available: https://www.cisco.com/c/dam/en/us/td/i/000001-100000/40001-45000/42501-43000/42870.ps/_jcr_content/renditions/42870.jpg. [Acedido em 05 01 2018].

[15] CISCO, "CISCO," 25 Setembro 2014. [Online]. Available: https://www.cisco.com/c/pt_br/support/docs/voice/h323/5244-understand-gatekeepers.html. [Acedido em 20 02 2018].

[16] P. E. Jones, "Overview of H.323," 04 2007. [Online]. Available: https://hive2.hive.packetizer.com/users/packetizer/papers/h323/overview_of_h323.pdf.

[17] UNION, INTERNATIONAL TELECOMMUNICATION, "Pulse Code Modulation (PCM) of voice frequencies," 1993.

[18] INTERNATIONAL TELECOMMUNICATION UNION, Recommendation G.726, Geneva, 1990.

[19] “Voip-info.org,” 7 4 2011. [Online]. Available: https://www.voip-info.org/wiki/view/ITU+G.729. [Acedido em 21 11 2017].

[20] “WebRTC,” [Online]. Available: https://webrtc.org/. [Acedido em 2 12 2017].

[21] “VoIP: An In-Depth Analysis Chapter7,” [Online]. Available: http://cdn.ttgtmedia.com/searchVoIP/downloads/VoIP%5B1%5D.In.Depth.Analysis.Ch7.pdf. [Acedido em 2 12 2017].

[22] Internet Engineering Task Force (IETF) , “ UDP Usage Guidelines,” *Request for Comments: 8085 ,* Março 2017.

[23] Information Sciences Institute University of Southern California, “TRANSMISSION CONTROL PROTOCOL,” 1981.

[24] IETF, “RTP: A Transport Protocol for Real-Time Applications,” *Request for Comments: 3550 ,* Julho 2003.

[25] “The Business Voice,” onsip, [Online]. Available: https://www.onsip.com/blog/webrtc-signaling. [Acedido em 24 11 2017].

[26] Tutorials Point (I) Pvt. Ltd., “WebRTC,” 2015.

[27] “Real time Communication with WebRtc,” [Online]. Available: https://codelabs.developers.google.com/codelabs/webrtc-web/#0. [Acedido em 2 12 2017].

[28] B. Castillo e M. Villegas, “The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP),” 01 2014. [Online]. Available: https://tools.ietf.org/html/rfc7118. [Acedido em 24 11 2017].

[29] “EID,” [Online]. Available: http://www.eid.pt/documentos/catalogos/online/icc-201_icc-251_ed9.pdf. [Acedido em 4 12 2017].

[30] “EID,” [Online]. Available: http://www.eid.pt/prod/17/icc-201_ip_intercom_system. [Acedido em 14 11 2017].

[31] “Asterisk,” 2017. [Online]. Available: http://www.asterisk.org/get-started. [Acedido em 05 12 2017].

[32] L. M. J. V. M. Russel Bryant, Asterisk The Definitive Guide, USA: O’Reilly Media, Inc, 2013.

[33] L. C. G. Lustosa, “OpenH323 Gatekeeper - The GNU Gatekeeper,” 24 09 2003. [Online]. Available: https://www.gnugk.org/gnugk-manual-pt.html. [Acedido em 30 11 2017].

[34] J. Criscuolo, E. Green, J. Frazier e W. Mitchell, “SIP.js,” [Online]. Available: https://sipjs.com/aboutus/. [Acedido em 21 12 2017].

[35] J. L. Millán, I. B. Castillo e S. I. Corretgé, “JSSIP,” [Online]. Available: http://jssip.net/documentation/faq/. [Acedido em 02 01 2018].

[36] S. B. A. W. S. K. Wim Taymans, “GStreamer Application Development Manual (1.10.1)”.

[37] P. Papageorgiou, “SIP, A Comparison of H.323 vs SIP,” University of Maryland at College Park, 2001.

[38] R. Arora, “Voice over IP : Protocols and Standards,” [Online]. Available: https://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols/index.html#2.2-H.323-Protocol. [Acedido em 11 11 2017].

[39] V. Soares, P. Neves e J. Rodrigues, “Past, Present and Future of IP Telephony,” em *International Conference on Communication Theory, Reliability, and Quality of Service*, Portugal, 2008.

[40] Florida RF Labs, “RG400 Cable Specifications M17/128-RG400”.

[41] N. Chauha, “GitHub,” 2017 10 21. [Online]. Available: https://github.com/centricular/gstwebrtc-demos/blob/master/signalling/simple-server.py. [Acedido em 01 05 2018].

[42] Firefox, “Signaling and video calling,” 28 08 2018. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API/Signaling_and_video_calling. [Acedido em 02 09 2018].

[43] DB9, “DB9 Pinout,” [Online]. Available: http://db9-pinout.com. [Acedido em 2 Agosto 2018].

[44] “statcounter,” 07 2018. [Online]. Available: http://gs.statcounter.com/browser-market-share/desktop/worldwide/#monthly-201801-201801-bar. [Acedido em 26 08 2018].

[45] Google, “GooglePlay,” Hoel Boedec, [Online]. Available: https://play.google.com/store/apps/details?id=com.boedec.hoel.frequencygenerator&hl=pt. [Acedido em 07 Outubro 2018].

[46] H. Chaouchi, Wireless and Mobile Network Security, London: ISTE Ltd, 2009.

[47] “Hawai ARMY,” [Online]. Available: http://www.hawaiiarmyweekly.com/storage/2015/02/A3_3BCT_TOCEX_002_w.jpg. [Acedido em 24 07 2018].

[48] “GL Communications,” [Online]. Available: https://www.gl.com/images/sip-protocol-tester-maps-web-sip-call-procedure.gif. [Acedido em 2018 Janeiro 12].

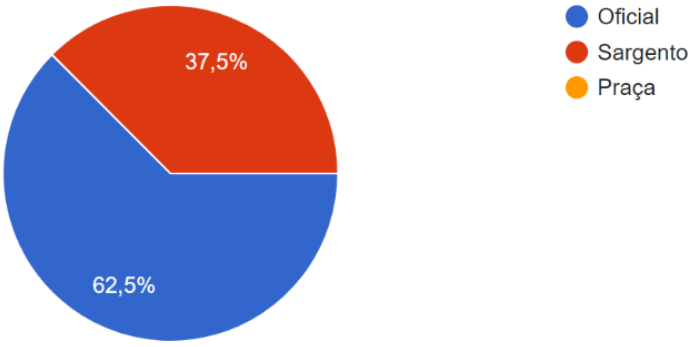
[49] websocket.org, “websocket.org,” 2017. [Online]. Available: http://websocket.org/aboutwebsocket.html. [Acedido em 2 Dezembro 2017].

7. Anexos

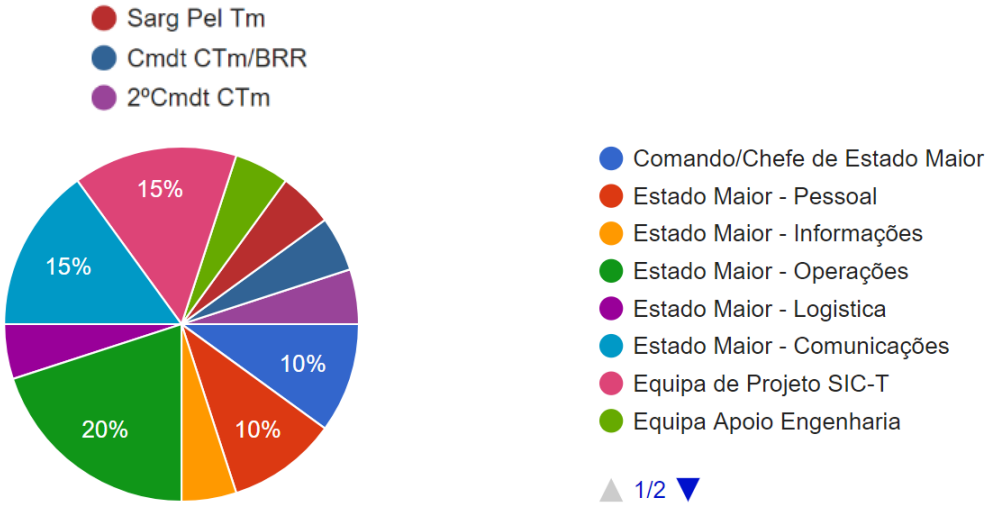
7.1 Anexo A – Inquéritos Iniciais

Foi apresentado um inquérito a diversos camaradas do Exército em que se colocaram as seguintes questões, e obtiveram-se as seguintes respostas num universo de vinte respostas:

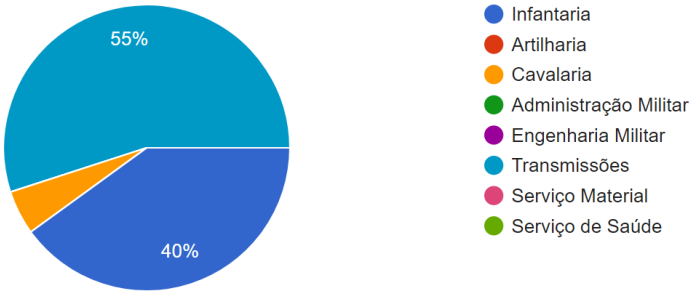
Categoria:



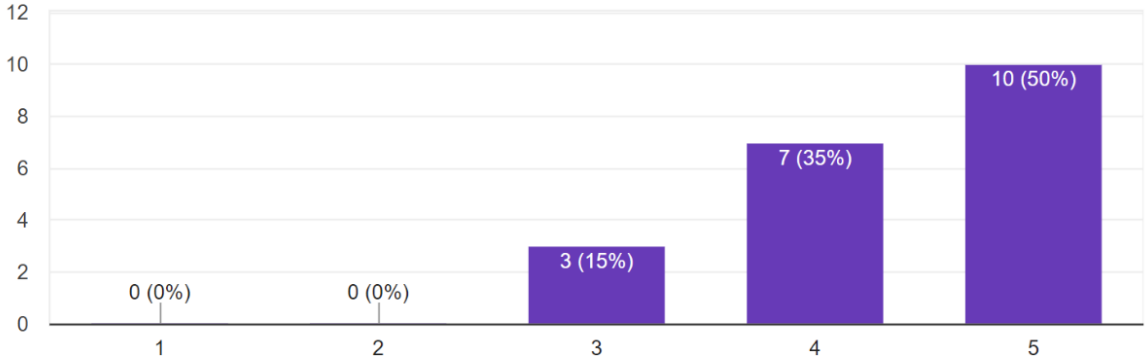
Funções que desempenha:



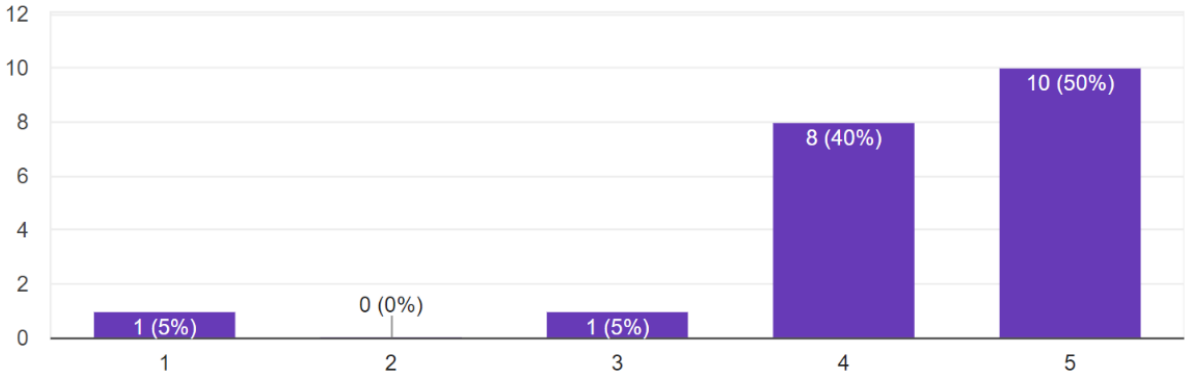
Arma/Serviço:



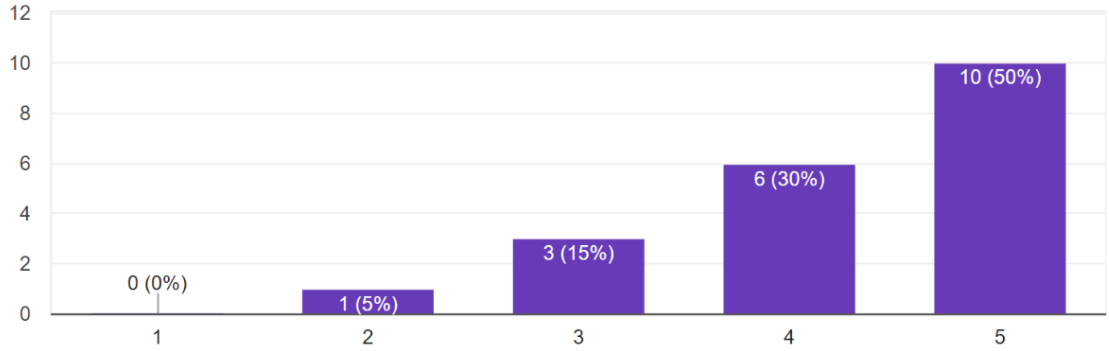
Acha útil que uma aplicação possa permitir o acesso remoto (ouvir/transmitir) a um Rádio, como o P/PRC 525? Como por exemplo, a utilização de um rádio através do seu tablet e/ou Computador?



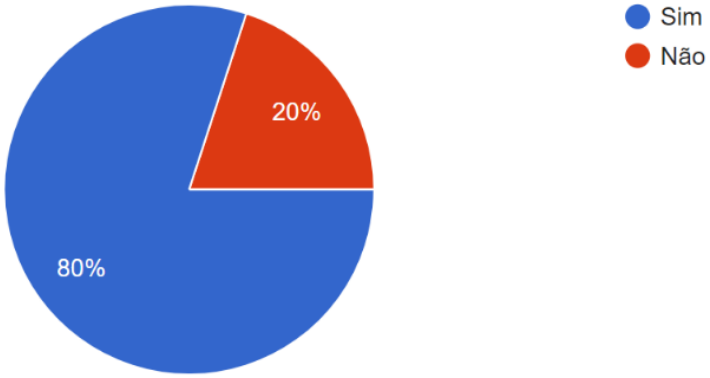
É útil uma funcionalidade que permita ouvir todas as redes rádio a que tenha permissão? Podendo-se selecionar quais as redes rádio que quer ouvir ao mesmo tempo.



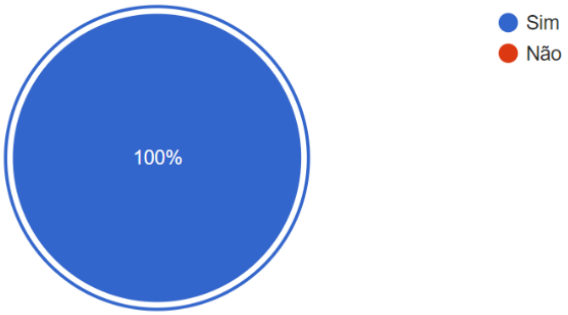
É útil a um operador dos rádios ter acesso às informações destes remotamente? Por exemplo, estado da bateria, se estão a transmitir ou não, se estão a comunicar em Segurança...



É pertinente que um utilizador consiga fazer PTT (remoto através da aplicação) para as redes rádio a que tem acesso?



Quando um utilizador usa um telefone IP para realizar uma chamada numa rede rádio (P/PRC 525esta rede fica limitada, ou seja, qualquer rádio que esteja nessa rede não consegue utilizar o rádio para dados por exemplo, porque a rede fica ocupada. Acha necessária uma solução para este problema?



Existe alguma funcionalidade que deva ser implementada, que não se encontre referenciada?

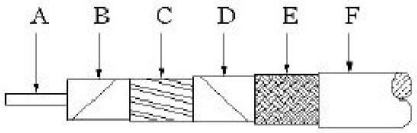
Para já não.
A disponibilidade de incorporar de forma facilitada o GPS do Rádio 525 para um sistema de "tracking" com software em computador posto comando, exemplo; - monotorização da movimentação ou posição das unidades/rádio quer em operações ou em apoio a MADBE.
A questão dos telefones VoIP é bastante útil. Já realizei várias experiências utilizando a waveform SECOM-V (VHF), e funciona corretamente. No entanto em ALE3G (HF) não sucede o mesmo, ocorrem vários erros. Uma boa oportunidade para estudar uma possível solução para este problema.
Nada
NTR
Se possível: Permitir configurações básicas tais como: alteração de potência, frequência...
- Assegurar os requisitos de COMSEC e TRANSEC do radio. - Poder reprogramar o rádio remotamente.

7.2 Anexo B – Especificações do cabo RG400

RG400 Cable Specifications M17/128-RG400

DOCUMENT No: CABLE-RG400 SHEET 1 OF 2 REV -

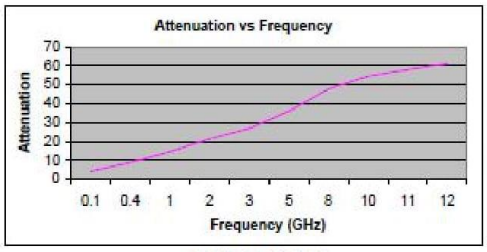
This group of cable includes familiar RG cable part numbers that have been superseded by MIL-C-17 numbers and alternative custom cable with improved electrical performance over standard M17 cables. The cables have been grouped by outside diameter. All standard cables supplied by Florida Rf Labs are purchased to the MIL-C-17 specification and no longer carry the RG designation.



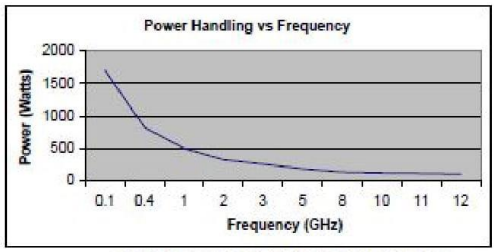
Electrical Data			
Frequency, Max (GHz)	12.4		
Impedance, nominal (Ω)	50		
Velocity of Propagation (%)	69.5		
Shielding Effectiveness, 1 GHz (dB/ft)	>60		
Capacitance (pF/ft)	29.4		
Delay (ns/ft), (ns/meter)	1.463	4.80	
Attenuation k1 (db/100ft) @ 23 deg C Attenuation k2 (db/100ft) @ 23 deg C	0.426 0.0012		Attenuation (typical) at any Frequency =k1 x SqRt (FMHz) + k2 x (FMHz)

Mechanical Data			
Weight (lbs/100ft), (Kg/100m)	5.00	7.52	
Temperature Range (°C)	-55 to 200		
Minimum Bend Radius (inch), (mm)	1.00	25.40	

Construction Data				
Inner Conductor (inch)	A	Stranded	19/.0080	Silver Covered Copper
Dielectric (inch)	B	Solid	0.116	Polyetrafluoroethylene
First Outer Shield (inch)	C		0.162	36SC
Second Outer Shield (inch)	D			
Third Outer Shield (inch)	E			
Jacket (inch O.D.)	F		0.195	Fluorinated Ethylene Propylene - IX



(dB per 100 feet)



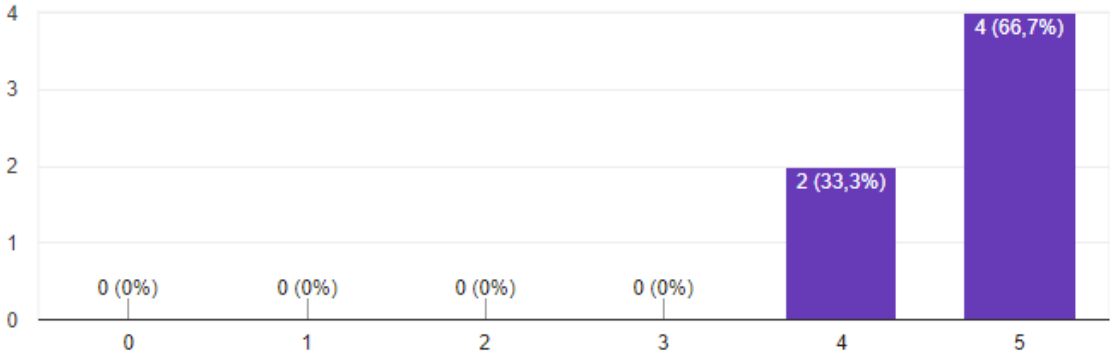
*CW Power in watts at sea level and 23°C

QUICK SPEC

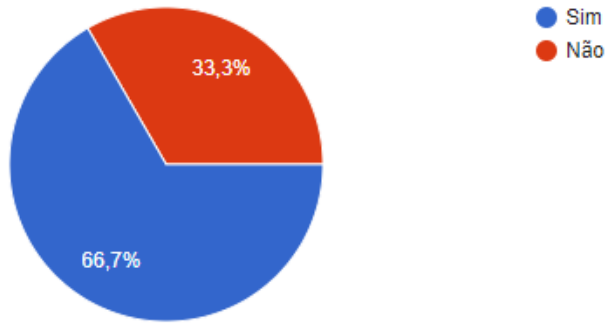
Max Frequency	Loss @ 5 GHz	Cable Diameter	Shielding Effect.
12.4 GHz	32 dB	0.195"	>60

7.3 Anexo C – Inquéritos finais

O botão PTT pode ser ativado de duas maneiras. Pressionando uma tecla do teclado, sendo assim o funcionamento idêntico ao do PTT do rádio, ou premindo um botão virtual para ativar/desativar. Quanto à sua usabilidade (facilidade de uso), avalie de 1 a 5.



Com este sistema é possível alterar as frequências (modo frequência fixa) e as *Preset Pages*. Estas configurações são suficientes? Senão, quais acha serem fundamentais?



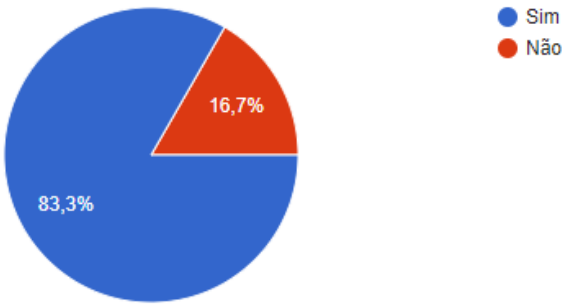
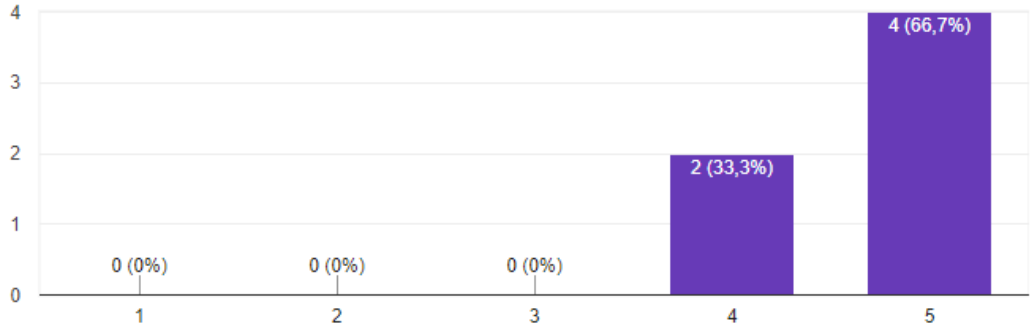
Quais acha serem fundamentais?

2 respostas

Poderia dar opção de alterar os Hopsets nas waveforms de SeCom.

Alteração dos próprios modos das Preset Pages

Acha importante a comunicação dita normal ser possível, em conjunto com este sistema desenvolvido, para o caso deste falhar?



As informações do rádio que a aplicação permite aceder são suficientes para este tipo de sistema? Bateria, potência, tipo de onda, frequência, estado da chamada (ALE3G).