UTILIZAÇÃO DA REDE TELEFÔNICA DO COMANDO DA AERONÁUTICA COM EMPREGO DA TECNOLOGIA DE VOZ SOBRE IP

Marco Aurélio Sernagiotto Al CFOE COM
Evanildo Feitosa Santos Al CFOE COM
Jurandyr Tavares de Sant'Anna Al CFOE COM
Marco Antônio Sabbá Marinho Al CFOE COM

Marcelo de Souza Freitas Maj QOECOM[A]

RESUMO

A Rede Telefônica do Comando da Aeronáutica (RTCAER) é um recurso muito importante para o Comando da Aeronáutica (COMAER), pois interliga estrategicamente os comandos das diversas organizações militares. A proposta desse trabalho é utilizar a tecnologia VoIP associada a métodos de criptografia que ofereçam tais características. Este trabalho propõe a estruturação de uma RTCAER em que a falha de alguns elos não a torne indisponível, distribuindo o roteamento numa grande nuvem de comunicação que envolva todas as unidades da Aeronáutica.

Palavras-chave: Rede RTCAER. VoIP. Criptografia.

[A] Comandante do Destacamento de Controle do Espaço Aéreo e Telemática do Rio de Janeiro (DTCEATM-RJ)

1 INTRODUÇÃO

O uso das telecomunicações nos dias atuais é imprescindível. Nas ruas, no comércio ou dentro de casa, enfim, em todo lugar, utilizam-se telecomunicações para que as pessoas possam trocar informações dos mais diversos tipos, desde informações pessoais até informações secretas entre países. E uma tecnologia que se destaca nesse universo é a Voz sobre IP (VoIP).

Pelos projetos atuais em empresas que já trabalham com VoIP e segundo analistas de mercado, ocorrerá a extinção por completo do modelo atual de ligações de longa distância (DDD/DDI) pela rede de linhas comutadas e, mais adiante, a erradicação dos sistemas convencionais de telefonia. Parte dessa evolução ocorrerá à medida que o telefone IP, utilizado no VoIP, e os acessos à Internet em banda larga forem se popularizando nos lares.

As Forças Armadas têm a necessidade de utilizar meios de comunicação para que as informações possam ser transmitidas entre seus militares. Um desses meios de comunicação no Comando da Aeronáutica é a RTCAER que, atualmente, utiliza linhas privadas para interconectar os comandantes da Força e lhes garantir sigilo na troca de informações.

Este trabalho tem como objetivo propor a utilização da RTCAER com a tecnologia (VoIP) em redes de comunicação já existentes no COMAER, a fim de prover um meio de comunicação eficiente e seguro, sem a necessidade do aluguel de novas linhas dedicadas, proporcionando uma economia mensal para os cofres públicos. O estudo está baseado na teoria de segurança em redes VoIP.

2 TECNOLOGIA VOIP

Nos últimos anos, diversas formas de comunicação têm sido convertidas da tecnologia analógica para a digital. Um desses exemplos é a tecnologia de comunicação por voz em redes IP.

Os termos VoIP e Telefonia IP podem ser facilmente confundidos, já que os dois consistem basicamente em trafegar voz em pacotes IP numa rede, mas apresentam diferenças que permitem distingui-los.

2.1 VoIP

O termo VoIP é usualmente utilizado no mercado de telecomunicações como o serviço fornecido pela conexão entre uma central telefônica convencional (PABX) com um roteador ou Gateway que está ligado a uma INTRANET ou rede corporativa, trazendo grande economia aos usuários. Nesse caso, as chamadas entre centrais localizadas em cidades diferentes são roteadas pela INTRANET e não pela rede pública de telefonia. Essa solução é largamente utilizada, pois apresenta baixo custo de implementação, devido ao fato de manter a infraestrutura existente de telefonia.

A tecnologia VoIP já vem sendo adotada há vários anos no mundo empresarial, em redes de dados privadas, ou linhas dedicadas, para reduzir custos de ligações telefônicas entre filiais.[1] Nessa tecnologia, telefonia e dados se "misturam" e, dessa forma, pode-se enviar não só a voz, mas também a imagem do interlocutor. Com um *software* apropriado, é possível fazer ligações para telefones convencionais usando apenas um microfone e caixas de som ou fones do próprio computador com acesso à rede. O VoIP também tem sido aplicado em centrais telefônicas PABX, trazendo economia aos usuários ao facilitar tarefas difíceis em redes tradicionais: chamadas entrantes podem ser automaticamente roteadas para o telefone VoIP, independentemente da localização desse telefone na rede. Assim, é possível levar um telefone VoIP para uma viagem e, por meio de uma conexão adequada à Internet, receber e realizar ligações em qualquer lugar do planeta.

Já a Telefonia IP utiliza aparelhos de telefone especiais, que se conectam diretamente à rede IP, recebendo voz, dados e imagens simultaneamente. A figura 1 mostra o uso da tecnologia VoIP e da tecnologia IP: uma rede LAN com computadores e *softwares* VoIP e um telefone IP ligado diretamente ao roteador.

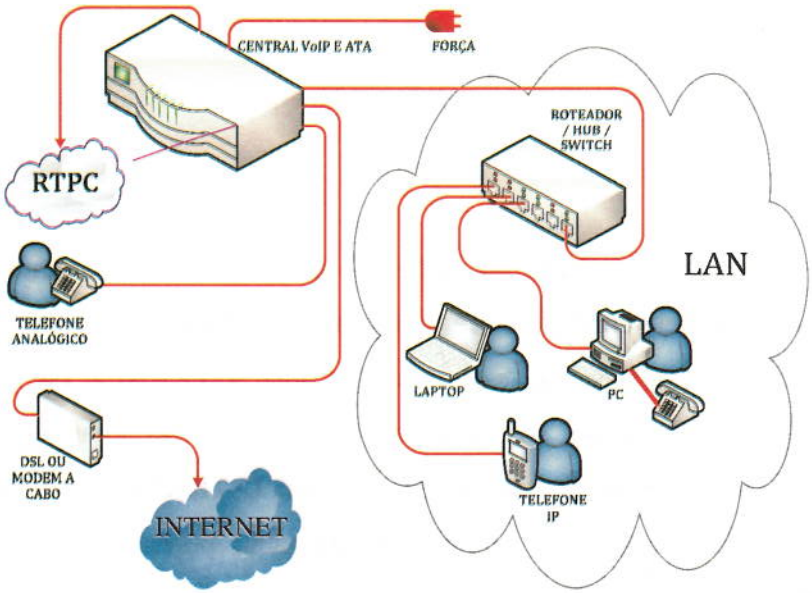

Figura 1: Uso da tecnologia VoIP e da IP.
Fonte: Elaborada pelos autores.

A tecnologia VoIP ainda inclui funções como videoconferência, redirecionamento e identificador de chamadas, conferência a três, mensagens instantâneas, compartilhamento de arquivos, gerenciamento de listas telefônicas, sem custos adicionais.[2]

O COMAER já utiliza alguns ramais VoIP na INTRAER[B], principalmente entre as organizações do Departamento de Controle do Espaço Aéreo (DECEA).

2.1.1 Funcionamento do VoIP

[B] Rede WAN (Intranet) do Comando da Aeronáutica

Para ser transmitida, a voz, que é um sinal analógico, deve ser transformada em pacotes de dados (figura 2). Esses pacotes são então enviados pela rede usando o protocolo IP (*Internet Protocol*).

Figura 2: Pacote de dados.
Fonte: Elaborada pelos autores.

Quando o destino recebe os pacotes, eles são retransformados em sinais analógicos e enviados a um transdutor, que nada mais é do que um alto-falante ou uma cápsula telefônica, para que possam ser ouvidos.

Além de ser utilizado em computadores, via *software*, o VoIP também pode ser utilizado através de adaptadores para telefones analógicos (ATA) ou em *Gateways* VoIP, ou seja, aparelhos conectados entre uma rede de banda larga e um aparelho telefônico comum ou PABX (figura 1). Os *Gateways* interligam as redes IP e a Rede de Telefonia Pública Comutada (RTPC): são os responsáveis por fazer a conversão da sinalização de chamadas e a conversão do sinal analógico em digital, e vice-versa (figura 2). Existe um tipo específico de *Gateway*: o *Gateway Controller*, também conhecido como *Call Agent*, que controla as chamadas feitas pelos *Gateways*.

Nas ligações de longa distância, são utilizados os *Gatekeeper*, equipamentos que gerenciam outros equipamentos da rede VoIP, e podem autorizar chamadas, funções típicas de uma central telefônica, e fazer controle da largura de banda utilizada.

A qualidade de serviço (QoS) é um fator importante para o bom funcionamento do VoIP. Por meio deste recurso, pode-se, por exemplo, priorizar os pacotes de voz sobre os pacotes de dados. O aumento da largura de banda, ou velocidade de transmissão e recepção de dados, contribui para melhorar o VoIP e, como o acesso à Internet em banda larga é cada vez mais comum, ele passou a se beneficiar disso.

Além da largura de banda, várias empresas passaram a pesquisar outros fatores que garantissem o melhor QoS possível. Neste contexto, surgiram vários protocolos para VoIP: um deles, o *Real Time Protocol* (RTP), adotado por quase todas as empresas, faz os pacotes de dados, como voz e vídeo, serem recebidos conforme a ordem de envio: ele "ordena" os pacotes e, caso algum desses pacotes chegue atrasado, faz uma interpolação no "intervalo" deixado pelo pacote e descarta-o. Assim, torna-se possível a transmissão de dados em tempo real mesmo com possível atraso de pacotes, já que estes podem seguir caminhos diferentes para chegar ao destino e o tempo para percorrê-los não é o mesmo.

Na transmissão de dados, o atraso não é um problema tão sério, pois os pacotes podem ser reordenados no destinatário, antes de serem decodificados, mas, com voz e vídeo em tempo real, isso não pode acontecer, pois prejudicaria a inteligibilidade da comunicação. Por exemplo: ao transmitir a palavra "INTRAER", se o pacote da letra "T" atrasar, o destinatário deverá receber "INRAER" e não "INTRAER".

Atualmente, a tecnologia VoIP não se limita às empresas. A popularização do software Skype[C] mostra o sucesso dessa tecnologia nas comunicações pela Internet - um sinal evidente de que o VoIP pode se tornar um dos fenômenos da Internet, assim como as mensagens eletrônicas.

2.2 Telefonia IP

A Telefonia IP é uma espécie de "versão evoluída" do VoIP. Para um serviço ser caracterizado como Telefonia IP, é necessário que tenha, no mínimo, funcionalidades e qualidade equivalentes às da telefonia convencional.

A Telefonia IP faz uso de aparelhos telefônicos específicos ou *hardwares* em redes IP, como a INTRAER, que se conectam diretamente a ela, recebendo voz, dados e

[C] *Software* criado por Niklas Zennström cuja marca é de propriedade da *Skype Limited*. O *software* possui mais de meio bilhão de usuários no mundo.

imagens simultaneamente. Os dispositivos apresentam tecnologia suficiente para a transmissão de voz em tempo real com qualidade que muitas vezes supera a telefonia convencional. Um fato interessante é que a Telefonia IP consegue essa eficiência sem necessitar de centrais telefônicas e ainda pode apresentar integração com outros serviços de dados, como vídeo e mensagens eletrônicas.[3]

As principais características da Telefonia IP são:

a) integração: é a utilização de uma mesma infraestrutura para comunicação de voz e dados. A tendência é que o computador e o telefone se tornem um único equipamento, já existem aplicativos que permitem que o usuário opere um telefone IP a partir da tela de seu computador;

b) aplicações: por estarem interligados à rede de dados, os Telefones IP podem funcionar como computadores conectados à Internet, permitindo consultas a informações sobre o tempo, a bancos de dados de notícias, ao comércio eletrônico etc;

c) mobilidade: através da Telefonia IP, utilizando a internet como meio de comunicação e uma conexão em banda larga, é possível ativar um ramal em qualquer lugar do mundo;

d) convergência: é possível a convergência de aplicações em *links* de alta velocidade, como a videoconferência junto à voz. Assim, o computador com uma *webcam* passa a funcionar como uma estação de videoconferência, recebendo voz e imagem em tempo real; e

e) período de transição: os benefícios da Telefonia IP podem ser testados antes da opção pela conversão completa. É possível utilizar-se de centrais híbridas, ou seja, com aparelhos convencionais e IP, o que torna a transição mais suave.[4]

3 RTCAER

A RTCAER, ou Telefone Vermelho[D], está normatizada por uma Instrução do Comando da Aeronáutica (ICA)[E] e tem como finalidade prover uma comunicação telefônica rápida e eficaz entre os Comandos das diversas organizações da Força Aérea Brasileira, no Brasil e no exterior.

A RTCAER atual é constituída por sete principais centrais telefônicas: uma em cada Comando Aéreo Regional (COMAR). Devido à demanda, também foi adicionada uma central para atender exclusivamente ao Departamento de Ciência e Tecnologia Aeroespacial (DCTA). As centrais instaladas em Belém – PA (COMAR I), Recife – PE (COMAR II), São Paulo – SP (COMAR IV), Porto Alegre – RS (COMAR V) e Manaus – AM (COMAR VII) atendem aos comandos de todas as Organizações da Aeronáutica situadas em sua respectiva área de jurisdição; as instaladas no Rio de Janeiro – RJ (COMAR III) e em Brasília – DF (COMAR VI), além de atenderem às suas respectivas Organizações, também são utilizadas como centrais de trânsito para o tráfego das ligações telefônicas entre as demais centrais. A central instalada no DCTA, em São José dos Campos – SP, fornece serviços apenas para os ramais daquela localidade.

A figura 3 mostra a interligação entre as centrais da RTCAER atual.

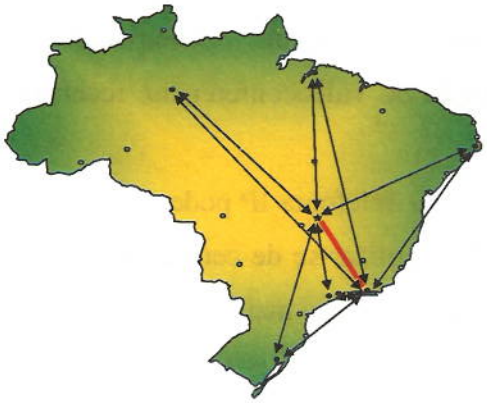

Figura 3: Centrais da RTCAER
Fonte: Elaborada pelos autores.

[D] A expressão "telefone vermelho" surgiu em 1963, quando os Estados Unidos e a antiga União Soviética criaram uma linha de telex direta entre os governantes dos dois países, com a finalidade de aplacar possíveis divergências entre os dois países, evitando um possível conflito, durante a Guerra Fria.

[E] ICA 102-3 – Rede de Telecomunicações do Comando da Aeronáutica.

Com a finalidade de se manter um alto grau de operacionalidade na rede, o número máximo de ramais ativos em cada central é limitado a cinco vezes o número máximo de ligações telefônicas simultâneas externas, até o limite de noventa por cento da capacidade de ramais da central. Essa reserva de dez por cento é estratégica e visa a atender à demanda de instalação de novos ramais em situações especiais, como em operações reais, manobras ou exercícios, a critério do DECEA.

3.1 Escuta clandestina na RTCAER[5]

Numa escuta telefônica, o atacante é capaz de monitorar a sinalização e a voz (dados) entre dois ou mais usuários (*endpoints*), mas sem ter a possibilidade de alterá-los.

Para que a comunicação de voz e dados seja segura, são realizados processos criptográficos desenvolvidos pelo CEPESC[F] e implementados por um algoritmo instalado no telefone seguro (TSG). Com um telefone convencional, a comunicação pode ser grampeada por um par de fios conectados em paralelo com os fios do telefone da "vítima" como, por exemplo, no quadro do distribuidor geral (DG).

Quando um telefone TSG apresenta defeito, a reposição não é imediata, sendo muitas vezes substituído por um telefone convencional - o que expõe a comunicação ao risco de interceptação e escuta clandestina. Assim, existe a necessidade de uma estrutura de rede de comunicações que permita o funcionamento sigiloso contínuo da RTCAER, independentemente do período de manutenção de equipamentos. Uma das soluções é o uso da tecnologia VoIP associada a métodos de criptografia.

3.2 Escuta clandestina na RTCAER via VoIP

[F] CEPESC – O Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações é parte integrante da estrutura da ABIN, Agência Brasileira de Inteligência, criada para sanar a flagrante deficiência do Brasil em salvaguardar o sigilo das transmissões oficiais.

Os seguintes aspectos podem ser comprometidos quando se fala em privacidade da comunicação por VOIP: para quem se faz e de quem se recebe a chamada, o que se fala e o que se digita no telefone em uma chamada.

É possível garantir a privacidade, porém, se o atacante possuir acesso a pontos chave da rede, como Dispositivo Cliente, *Switch* da Rede, *Proxy, Gateway* ou *Softphone*, ela estará ameaçada. Nesses pontos, é possível capturar os pacotes de sinalização e de mídia, e, empregando *softwares* específicos, converter o tráfego de rede em arquivos de áudio ou dados, para analisá-los posteriormente.

A aplicação VoIP será tão segura quanto mais seguras forem as camadas que lhe dão suporte. Por exemplo: se um servidor Asterisk usar um servidor Linux vulnerável, o atacante poderá assumir o controle do sistema operacional e capturar todo o tráfego de chamadas que passem por ele.

Outro tipo de ataque é realizado pela técnica *Man-in-the-Middle*, na qual o atacante envia vários pacotes ARP[G] para a rede alterando-a, ou seja, informando que ele é o *Gateway* ou servidor *Proxy*. Assim, todos os pacotes encaminhados para o *Gateway* ou *Proxy* na rede serão desviados para o atacante que, após sua análise, os encaminha para o *Gateway* ou *Proxy* correto, como se nada tivesse acontecido.

Existem, ainda, diversas formas de se comprometer o *switch* da rede. Alguns desses *switches* têm o recurso chamado Analisador de Porta Comutada Remoto (RSPAN), que permite o espelhamento do tráfego das portas ou redes virtuais de área local (VLANs) para uma determinada porta. Com isso, qualquer dispositivo que estiver ligado a essa porta poderá capturar o tráfego das outras portas, monitoradas pelo RSPAN.[6]

4 TÉCNICAS DE PROTEÇÃO AO USUÁRIO

[G] ***Address Resolution Protocol*** ou **ARP** é um protocolo usado para encontrar um endereço da camada de enlace (Ethernet, por exemplo) a partir do endereço da camada de rede, como um endereço IP.

4.1 Criptografia

Criptografia é o ato de codificar dados em informações aparentemente sem sentido, para que outras pessoas não consigam ter acesso a elas; é a arte de guardar ou transmitir mensagens de forma segura. Isso garante o sigilo da informação. Há vários usos para a criptografia no dia-a-dia: proteção de documentos secretos, transmissão de informações confidenciais pela Internet ou por uma rede local, etc.

Outros benefícios da criptografia são: a integridade, que consiste em verificar se a mensagem foi alterada durante o trânsito; a autenticação, que é a verificação correta da origem da mensagem para que um intruso não se passe por remetente da mensagem; e o não-repúdio ou irrevogabilidade, ou seja, a incapacidade de o remetente negar que enviou a mensagem.

A criptografia é, na maioria das vezes, utilizada indiretamente por ferramentas, protocolos e sistemas específicos: Protocolos de Segurança IP (IPSec), Assinaturas Digitais, Verificadores de Integridade (Funções de Hash[H]), PGP[I], Criptografia de Senhas, Interfaces Seguras (SSH)[J] e Protocolos de Camada de *Sockets* Segura (SSL)[K].

Os algoritmos de criptografia podem ser classificados em dois tipos, dependendo do tipo de chaves utilizada: simétrico, ou chave única, e assimétrico, ou chave pública e privada.

[H] Um **hash** é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando 1/2 byte cada. O conceito teórico diz que "hash é a transformação de uma grande quantidade de informações em uma pequena quantidade de informações".

[I] O **PGP**, do inglês *Pretty Good Privacy* (privacidade bastante boa), é um programa de computador desenvolvido por Phil Zimmermann em 1991 que utiliza criptografia para proteger a privacidade do e-mail e dos arquivos guardados no computador do usuário.

[J] Em informática o **Secure Shell** ou **SSH** é, simultaneamente, um programa de computador e um protocolo de rede que permite a conexão com outro computador na rede, de forma a executar comandos de uma unidade remota. Possui as mesmas funcionalidades do TELNET, com a vantagem da conexão entre o cliente e o servidor ser criptografada.

[K] **Secure Sockets Layer** - *Protocolo de Camada de Sockets Segura*, são protocolos criptográficos que conferem segurança de comunicação na Internet para serviços como *e-mail* (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados.

O algoritmo assimétrico utiliza duas chaves diferentes, uma para o processo de codificação e outra para o processo de decodificação. As duas chaves, pública e privada, são associadas através de um relacionamento matemático e geradas de tal maneira que, a partir de uma delas, não é possível calcular a outra a um custo computacional viável. Elas são geradas pelo responsável pela decodificação, ou seja, o destinatário, que manterá a chave privada consigo e a utilizará para decodificar as mensagens que os outros usuários codificarão com a chave pública divulgada. Somente o destinatário, de posse da chave privada, conseguirá decodificar as mensagens. Uma grande vantagem dos algoritmos assimétricos, particularmente o RSA[L], que é o mais conhecido e utilizado, é que o processo também funciona no outro sentido, a denominada assinatura digital, ou seja, usar a chave secreta para codificar os dados de forma que quem receba o arquivo, em posse da chave pública, consiga identificar o remetente do arquivo.

Especialistas estimam que, para alguém conseguir quebrar uma criptografia com chaves de 64 *bits* por ataques de força bruta (tentativa e erro), levaria cerca de 100.000 anos usando um PC comum. Atualmente, chaves de 128 *bits* já são comuns, dificultando ainda mais a descoberta da chave, comprovando a segurança dos sistemas de criptografia modernos.

4.2 Técnicas para proteger o usuário na RTCAER via VoIP

O sistema proposto para a RTCAER via VoIP não utiliza a RTPC para tráfego de voz. Ele apresenta somente Telefones IP, conectados aos *switches* da rede local e controlados por servidores com função de central telefônica IP, que são chamados PABX IP ou *Call Manager* (figura 4).

[L] Algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto MIT, seus inventores, Ronald Rivest, Adi Shamir e Leonard Adleman

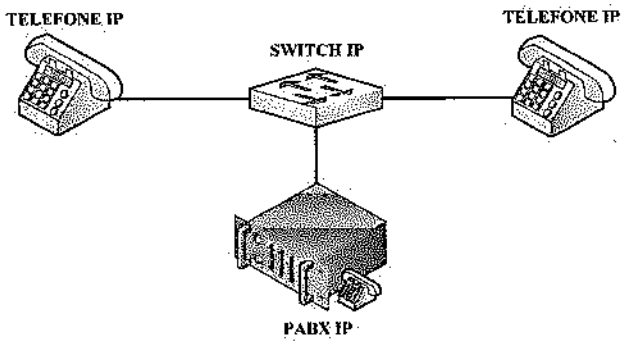

Figura 4: Central telefônica IP.
Fonte: Elaborada pelos autores.

O sigilo das comunicações será garantido pelas técnicas de segurança desenvolvidas no ambiente de redes de computadores, particularmente pela criptografia. Os componentes da rede podem sofrer qualquer tipo de ataque pelo simples fato de serem fisicamente acessíveis. Assim, os mesmos cuidados observados em servidores (*web*, *e-mail*, etc.) também devem ser observados nos servidores VoIP, com as seguintes ferramentas:

a) *Firewall*: protege os componentes da rede contra *crackers*, reforçando a segurança entre a rede interna segura e a rede externa não-confiável. O *firewall* pode ser um PC ou um roteador e determina quais informações ou serviços podem ser acessados e utilizados por quem não estiver conectado à rede local. Geralmente é instalado no ponto onde há o encontro da rede interna com a rede externa, chamado de ponto de "estrangulamento";

b) Sistema de Detecção de Intrusão (IDS): sistema integrado capaz de detectar tentativas de comprometimento ou de acesso indevido a uma rede ou aos seus recursos. Os IDS fornecem um aviso inicial de intrusão, para que a ação defensiva possa ser tomada - impedindo ou minimizando danos. Um elemento importante da prevenção à intrusão é o gerenciamento de senhas, impedindo que usuários não autorizados possuam senhas que possibilitem o acesso a áreas restritas. Atualmente, os IDS são uma das

soluções mais valorizadas no mercado porque suportam o conceito de integração de medidas de segurança e podem ser aplicados em praticamente todos os ambientes em que exista uma rede conectada a outras redes;

c) criptografia: utilizada nos pacotes de voz para assegurar que a conversa não seja decifrada, caso os pacotes sejam capturados na rede; e

d) VLAN/VPN: reservando uma VLAN específica para os telefones, outra para os dados e uma Rede Privada Virtual (VPN) ou *links* dedicados para interligar os *sites* distantes, isola logicamente as redes e dificulta o acesso aos pacotes de cada uma delas.

5 PROPOSTA DE UTILIZAÇÃO DA RTCAER VIA VOIP NO COMAER

O objetivo da estrutura da RTCAER é prover meios de comunicação necessários ao exercício da função de comando.[7] Porém, as atuais comunicações pela RTCAER, comutadas, apresentam algumas características que as tornam vulneráveis:

a) possibilidade de escuta inimiga, já que os dados trafegam nos canais de forma analógica[8]; e

b) dependência de linhas específicas dedicadas à comunicação, que podem ser alvo de sabotagem, facilitando a interrupção das comunicações ao interrompe-las física ou logicamente.

O VoIP é uma alternativa estratégica para contornar esses problemas e pode utilizar estruturas de comunicação já existentes no COMAER. Caso um inimigo interrompa uma linha de comunicação, roteadores conseguirão enviar o pacote ao destino por outros caminhos, pela INTRAER ou Internet, e a comunicação não será interrompida.

Atualmente, é utilizada uma rede HF de *backup* em caso de falha na RTCAER; mas, por ser irradiada, a Rede Alternativa de Comando da Aeronáutica (RACAER) é suscetível a interferências e interceptações eletromagnéticas.

5.1 Implementação da rede

A proposta inicial de estruturação da rede VoIP é instalar os "servidores" (*Call Managers*) nos Centros Integrados de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA), já que são as Unidades que administram a defesa aérea das regiões do espaço aéreo brasileiro e concentram *links* de comunicação com as outras unidades da Força Aérea Brasileira (FAB).

Faz-se necessário que, caso um dos servidores fique "fora do ar", os outros possam assumir o tráfego e continuar a comutar os pacotes na rede, evitando que as comunicações sofram solução de continuidade.

As duas formas de implementação sugeridas para a RTCAER em VoIP são: por Telefonia IP ou por softwares PABX VoIP.

Na Telefonia IP, o pacote de voz sai codificado do aparelho telefônico direto para a rede. Assim, a criptografia deve ser implementada no próprio equipamento (Telefone IP). Uma vantagem dessa implementação é que, mesmo que exista um ponto de captura de pacotes de dados próximo ao telefone, não haverá possibilidade de decodificar os dados capturados, devido à criptografia. A desvantagem é a necessidade de se desenvolver um hardware dedicado que implemente uma criptografia adequada ao nível de segurança militar, desenvolvido pelo COMAER ou pelo Ministério da Defesa, exigindo uma equipe de trabalho específica e especializada.

Para o uso de VoIP via *software* PABX, existe uma opção interessante, que implementa sozinho um PABX completo, chamado Asterisk[M 9]. Esse *software* pode funcionar na plataforma Linux, e oferece mais vantagens do que desvantagens em sua utilização.[10]

[M] O **Asterisk** é um Software Livre, portanto de código aberto, que implementa em software os recursos encontrados em um PABX convencional, utilizando tecnologia de VoIP.

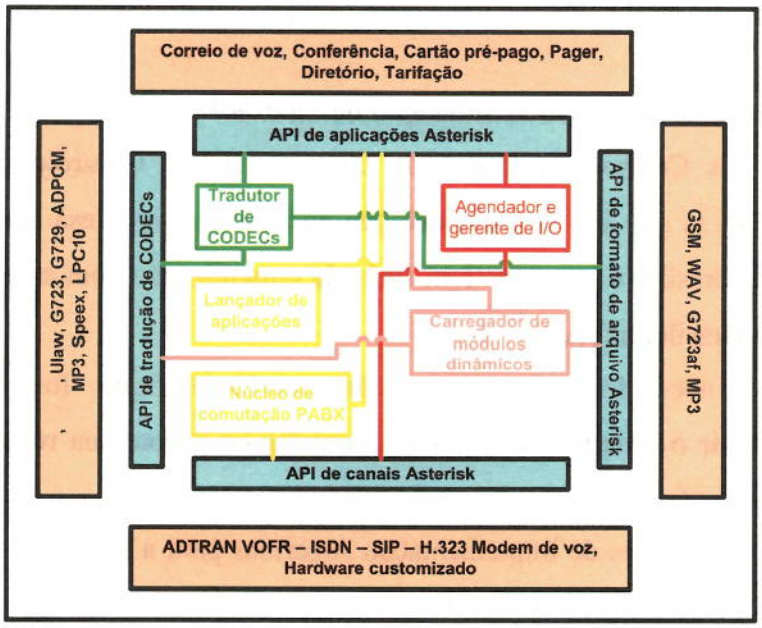

Figura 5: Asterisk
Fonte: Elaborada pelos autores.

O Asterisk foi desenvolvido com uma estrutura (figura 5) que permita o máximo de flexibilidade. As Interfaces de Programação de Aplicativo (API) desenvolvidas em torno do núcleo o tornam transparente a protocolos, codecs e *hardware*, sendo compatíveis com qualquer tecnologia existente ou que venha a ser lançada, sem a necessidade de mudanças no núcleo do programa para adequá-lo às novas tecnologias.[11]

A API de canais do Asterisk oferece a opção de trabalhar, além dos protocolos de sinalização, SIP e H.323, com o protocolo *Inter-Asterisk Exchange* 2 (IAX2) e oferece também a possibilidade de autenticação por chave RSA e criptografia AES de 128 *bits* para voz e para a sinalização, através de uma única porta TCP. O Asterisk pode ser utilizado em redes com NAT e, devido ao caminho dos dados e cabeçalhos dos pacotes não serem criptografados pelo IAX2[12], é possível utilizar VPN e *softwares* que atuem numa camada mais alta e apliquem uma outra criptografia (que pode ser desenvolvida pela FAB), conferindo níveis de segurança adequados ao sigilo militar.

5.2 Topologia e segurança na rede

A topologia de rede descreve como é o *layout* de uma rede de computadores por onde ocorre o tráfego de informações, e também como os dispositivos estão conectados a ela. Há várias formas de organizar a interligação entre cada um dos nós (computadores) da rede.

Topologias podem ser descritas fisicamente e logicamente. A topologia física é a verdadeira aparência ou *layout* da rede, enquanto que a lógica descreve o fluxo dos dados através da rede.

Uma vez estruturada a topologia da rede, deve-se buscar a implementação de critérios de segurança para proteger o tráfego de informações, principalmente no que diz respeito à defesa contra atividades não autorizadas.

Já existe uma estrutura de canalização prevista para a RTCAER (figura 6).

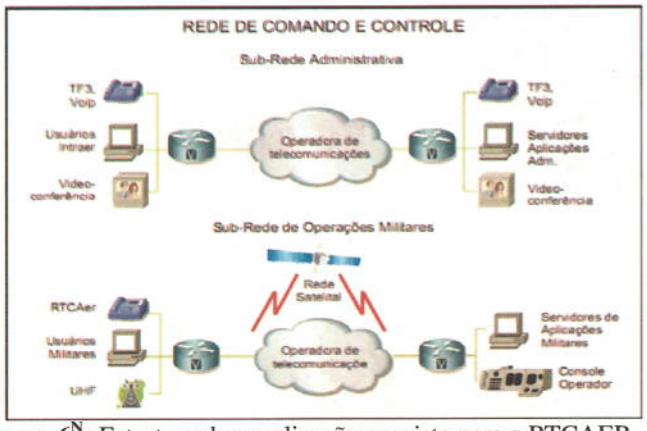

Figura 6[N]**:** Estrutura de canalização prevista para a RTCAER
Fonte: BRASIL, 2008.

De acordo com essa diretriz, estarão disponíveis dois canais de comunicação para a RTCAER: um via operadora de telecomunicações e outro através de uma rede

[N] Extraída da DCA 102-1 "Requisitos Básicos das Redes de Comunicações do COMAER"

satelital. Os pacotes VoIP que transitarem por elas já deverão estar criptografados, pois há possibilidade de interceptação.

A figura 7 mostra a ligação entre os elos principais da rede (CINDACTA I, II, III e IV). As setas indicam os links (duas redes): satelital e via operadora de telecomunicações.[13] Como os principais roteadores e *switches* da rede VoIP estarão nos CINDACTA, essa rede entre os centros deve ser do tipo *full-mesh*. Pela estrutura da INTRAER atual, as organizações militares (clientes) das localidades distantes dos CINDACTA têm que se comunicar via *link* de operadora de comunicações com um único CINDACTA e, a partir dele, conectar-se aos outros centros e atingir o destinatário da comunicação.

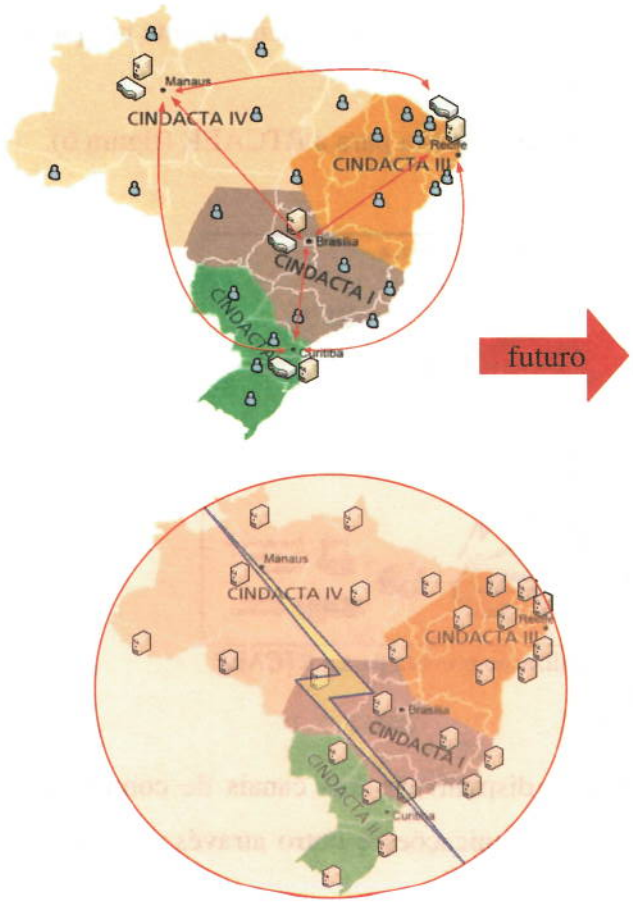

Figura 7: Ligação entre os elos principais da rede
Fonte: Elaborada pelos autores.

Porém, com a utilização do VoIP, caso um dos CINDACTA fique sem comunicação com os outros centros, as unidades conectadas a ele poderiam ainda continuar se comunicando com outros centros, bastando apenas uma conexão à Internet por uma VPN.

Outra possibilidade da tecnologia VOIP é a de que toda localidade com telefone VoIP RTCAER poderia funcionar, também, como centro comutador de mensagens, bastando um *software* capaz de gerenciar de forma adequada as sinalizações e uma base de dados atualizada de endereços de toda a rede, para roteamento dos pacotes. Nessa situação, mesmo que todos os CINDACTA ficassem inoperantes, as comunicações entre as outras unidades não seria interrompida – todas as unidades estariam logicamente conectadas numa rede *full-mesh*, como numa grande nuvem de comunicação (figura 6). Os links satelitais ficariam como opção em caso de falha das conexões terrestres à INTRAER e à Internet, já que os sinais do satélite são sensíveis à captura em qualquer local dentro de seu *Footprint* (área de cobertura).

Com relação à segurança, a fim de assegurar que os pacotes não sejam indevidamente desviados antes de entrarem na rede, os roteadores e *switch* deverão estar o mais próximo possível dos equipamentos VoIP da RTCAER (telefones IP ou servidores PABX VoIP), com *links* que preferencialmente não usem a tecnologia sem fio (*wireless*) – nesses *links*, o uso de fibra óptica tem, além da vantagem do alcance, o fato de oferecer maior dificuldade à interceptação do sinal, já que a fibra não permite a utilização de perturbações magnéticas para capturar sinais, como ocorre nos fios metálicos, e ainda o fato de que, para um intruso fazer alterações físicas na fibra óptica, ele terá que utilizar equipamentos caros e sofisticados.

Alguns *softwares* oferecem proteção contra as ameaças à rede: as VLAN, autenticação nas mensagens de sinalização (SIP, H.323 ou IAX), o IPSEC (na camada de rede), o TLS (na camada de aplicação), e a criptografia do RTP – nesse caso, preferencialmente com algoritmos e chaves desenvolvidos pela própria FAB, como os que são aplicados em alguns Destacamentos de Controle do Espaço Aéreo (DTCEA) para a canalização da INTRAER via Internet, por meio de uma VPN.

6 CONSIDERAÇÕES FINAIS

Sabe-se que o avanço tecnológico invade todas as áreas do conhecimento; obviamente nas comunicações não seria diferente. Sendo assim, a mudança da plataforma de funcionamento da RTCAER da Telefonia Comutada convencional para a Telefonia IP é uma necessidade premente. Esta mudança significará uma evolução nas comunicações aeronáuticas, uma vez que traz maiores possibilidades de proteção, flexibilidade, versatilidade e integração à informação. Nesse contexto, os comandantes de organizações militares terão a garantia de que suas comunicações serão processadas com qualidade, mobilidade, continuidade e sigilo.

Com o avanço da tecnologia de comunicação de dados, evoluem também as formas de ameaças e ataques às informações. Hoje é possível, por meio de filtragem dos pacotes de mídia (RTP), fazer a reconstrução do áudio das chamadas telefônicas VoIP: ferramentas como *Wireshark, Cain e Abel, vomit, voipong* e *oreka* são capazes de realizar essa tarefa. O aplicativo *voipong* é capaz de, em tempo real, filtrar dos pacotes e gerar um arquivo de áudio (em formato .WAV) automaticamente. A única forma de se evitar esse ataque é utilizando a criptografia do RTP e da sinalização.

Para comprovar a importância da segurança das comunicações, como exemplo, há no mercado uma empresa (*Gold Lock*) que oferece comercialmente, desde 2003, um *software* de criptografia em três níveis, com autenticação de 16384 bits, licenciado pelo Ministério da Defesa de Israel, com nível de segurança militar.

Nos dias atuais, o país que detém a informação pode até não ganhar uma guerra, mas aquele que não a possui será fatalmente derrotado.[14]

REFERÊNCIAS

ANDERSON, Mark. **VoIP security**: uncovered. 2005. 5p. Disponível em: <http://www.jimalexander.com/pdf/VoIPSecurityUncovered.pdf >. Acesso em: 07 out. 2010.

BASET, Salman A.; SCHULZRINNE, Henning. **An analysis of the Skype peer-to-peer Internet telephony protocol.** New York: Columbis, 2004. 12p. Disponível em: <http://arxiv.org/ftp/cs/papers/0412/0412017.pdf >. Acesso em: 07 out. 2010.

BRASIL. Comando da Aeronáutica. Centro de Instrução e Adaptação da Aeronáutica. **Sistemas operacionais 2**. Belo Horizonte: CIAAR, 2009. (Apostila).

BRASIL. Comando da Aeronáutica. Centro de Instrução e Adaptação da Aeronáutica. **VOIP**. Belo Horizonte: CIAAR, 2009. (Apostila).

BRASIL. Comando da Aeronáutica. **DCA 102-1**: requisitos básicos das redes de comunicações do COMAER. Rio de Janeiro: DECEA, 2008. 34p.

BRASIL. Comando da Aeronáutica. **ICA 102-3**: rede de telecomunicações aeronáuticas. Brasília: EMAER, 2002. 15p.

INFO WEBSTER: artigos técnicos ligados à tecnologia da informação. Disponível em: <www.infowester.com>. Acesso em: 07 out. 2010.

INTERNEXT: provimento de acesso à internet comercial no Brasil. Disponível em: <http://www.internext.com.br>. Acesso em: 25 set. 2010.

MADEIRA, Frederico Tiago Tavares. **Segurança em redes de voz sobre IP**. Olinda: [s.n.], 2007.

MEGGELEN, Jim Van; SMITH, Jared; MADSEN, Leif. **Asterisk**: the future of telephony. 2nd ed. USA: [s.n], 2007. 188p.

PINHEIRO, Bruno de Oliveira. **Voz sobre IP utilizando Asterisk**. Lavras: [s.n.]. 2005.

SOUZA, Rafael Moriggi; LIMA, Anderson Eduardo; SANTOS, Rafael Leandro. **Implementação de um PABX e Gateway VoIP com Asterisk**. Curitiba, 2006.

VOIP e telefonia IP paralelas e inevitáveis. Disponível em: <http://imasters.uol.com.br/artigo/2073/tecnologia/>. Acesso: 12 set. 2010.

VOIP: definição. Disponível em: <http://pt.wikipedia.org/wiki/Voz_sobre_IP>. Acesso em: 10 set. 2010.

[1] http://www.internext.com.br
[2] http://pt.wikipedia.org/wiki/Voz_sobre_IP
[3] InfoWester 2010 - www.infowester.com
[4] http://imasters.uol.com.br/artigo/2073/tecnologia/voip_e_telefonia_ip_paralelas_e_inevitaveis
[5] Apostila Sistemas Operacionais 2 CFOE2009 – CIAAR
[6] MADEIRA, Frederico Tiago Tavares. "Segurança em redes de voz sobre IP". Olinda-PE, 2007.
[7] ICA 102-3 – Rede de Telecomunicações Aeronáuticas
[8] PINHEIRO, Bruno de Oliveira. "Voz sobre IP utilizando Asterisk". Lavras-MG, 2005
[9] SOUZA, Rafael Moriggi; LIMA, Anderson Eduardo; SANTOS, Rafael Leandro. "Implementação de um PABX e Gateway VoIP com Asterisk". Curitiba-PR, 2006.
[10] PINHEIRO, Bruno de Oliveira. "Voz sobre IP utilizando Asterisk". Lavras-MG, 2005
[11] SOUZA, Rafael Moriggi; LIMA, Anderson Eduardo; SANTOS, Rafael Leandro. "Implementação de um PABX e Gateway VoIP com Asterisk". Curitiba-PR, 2006
[12] MEGGELEN, Jim Van; SMITH, Jared; MADSEN, Leif. "Asterisk – The Future of Telephony". 2nd edition. USA, 2007. pg 188
[13] DCA 102-1/2008 – Requisitos Básicos das Redes de Comunicações do COMAER
[14] Apostila VOIP CFOE2009 – CIAAR