SENADO FEDERAL

UNIVERSIDADE DO LEGISTATIVO BRASILEIRO

UNILEGIS

FILIPE ANDREI LIMA DE ANDRADE MOURA

APLICAÇÃO DE NOVAS TECNOLOGIAS DE TELECOMUNICAÇÕES NO SENADO FEDERAL VISANDO MAIOR SEGURANÇA NA COMUNICAÇÃO

Brasília, DF

2009

FILIPE ANDREI LIMA DE ANDRADE MOURA

APLICAÇÃO DE NOVAS TECNOLOGIAS DE TELECOMUNICAÇÕES NO SENADO FEDERAL VISANDO MAIOR SEGURANÇA NA COMUNICAÇÃO

Trabalho final apresentado para aprovação no curso de Pós-Graduação *Lato Sensu* em Administração Legislativa realizado pela Universidade do Legislativo Brasileiro e Universidade Federal do Mato Grosso do Sul - UFMS como requisito para a obtenção do título acadêmico de Especialista em Administração Legislativa.

Orientador: JOÃO ALBERTO DE OLIVEIRA LIMA

Brasília, DF

2009

APLICAÇÃO DE NOVAS TECNOLOGIAS DE TELECOMUNICAÇÕES NO SENADO FEDERAL VISANDO MAIOR SEGURANÇA NA COMUNICAÇÃO

Trabalho de Conclusão do Curso de Especialização em Administração Legislativa realizado pela Universidade do Legislativo Brasileiro no 2º semestre de 2009.

FILIPE ANDREI LIMA DE ANDRADE MOURA

Banca Examinadora:

_____

JOÃO ALBERTO DE OLIVEIRA LIMA

_____

ERNESTO WILHELMS NETO

Brasília, 20 de agosto de 2009.

AGRADECIMENTO

Ao Senado Federal e Universidade do Legislativo Brasileiro, pela oportunidade concedida para elaborar este trabalho, que representa o presente e futuro das telecomunicações. Espero que seja útil para embasar a geração de futuras tecnologias nessa área.

Ao Professor Doutor JOÃO ALBERTO DE OLIVEIRA LIMA, pelo espírito público, constante compreensão, orientação competente e o seu alto valor técnico e científico.

Aos estimados Especialistas da Pós Graduação da Universidade do Legislativo Brasileiro e aos distintos colegas, pela feliz convivência acadêmica, apoio e solidariedade.

Aos meus pais Josélio e Regina Moura e meu irmão Fabrício Moura que fazem parte de uma família muito unida e que sempre me incentivaram.

À Roberta Góes pelo carinho, apoio e compreensão em todos os momentos.

A todos que contribuíram de alguma forma para a realização desta dissertação.

RESUMO

Tendo em vista a constante demanda de segurança nos sistemas de telecomunicações e a facilidade de acesso de intrusos a todo tipo de informações e diálogos de parlamentares e servidores, surge assim a necessidade da implantação de uma rede de nova geração – NGN, que possibilita o uso de diversas técnicas de segurança e serviços inéditos nas telecomunicações do Senado Federal. A rede NGN provê serviços de videoconferência em alta definição, acesso a servidores *streaming* com canais de TV e rádio ao vivo, recebimento de mensagens de texto, alertas, e-mail, dentre outros serviços. Essa rede é integrada ao padrão Wi-Fi que dá mobilidade a todos esses serviços, que podem ser acessados em aparelhos celulares, com toda segurança de criptografia e VPN.

Com o avanço das tecnologias sem fio e da implantação dos padrões WiMAX ou LTE, todos esses recursos poderão ser acessados de fora do *campus* do Senado, com toda mobilidade e segurança, tendo uma comunicação toda IP, evita o encaminhamento das ligações dos parlamentares e servidores pelas operadoras e, consequentemente, gravações indesejadas.

Palavras-chave: VoIP, NGN, Criptografia

ABSTRACT

Considering the constant demand for security in telecommunication systems and the easy access of intruders to all types of information as well as conversations of politicians and staff, there is a need to set up a New Generation Network – NGN, which allows for the use of diverse up-to-date security techniques and services in the Federal Senate. The NGN provides services of high definition video conferencing, Access of staff streaming with live TV and radio, text messaging, alters and emails, among other services. This network is integrated with Wi-Fi which gives mobility to all these services, which may be accessed from a single cell phone and encrypted with total security and VPN.

With the advance of wireless technologies and implantation of WiMAX or LTE standards, all these resources could be accessed from outside the Senate campus, guaranteeing full mobility and security, with full IP communication, avoiding the need to use operators and thereby undesirable recordings for politicians and staff.

Key-Words: VoIP, NGN, encryption

SUMÁRIO

LISTA DE FIGURAS

NOMECLATURA E ABREVIAÇÕES

Sigla	Significado
3G	Terceira Geração
4G	Quarta Geração
AES	Advanced Encryption Standart
ATM	Asynchronous Transfer Mode
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transreceiver Station
CRC	Cyclic Redudance Check
DDD	Discagem direta a distância
DES	Data Encryption Standart
DHCP	Dynamic Host Configuration Protocol
DOS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
GSM	Global System for Mobile
HLR	Home Location Register
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IEEE	Institute of Eletrical and Electronocs Engineers
IP	Internet Protocol
IV	Initialization Vector
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
MAC	Media Access Control
MIC	Message Integrity Code
MIMO	Multiple-Input Multiple-Output
MPLS	Multi-Protocol Label Switching
MSC	Mobile Services Switching Center
NGN	Next Generation Network
OFDM	Orthogonal Frequency Division Multiple
PABX	Private Automatic Branch Exchange
PDA	Personal digital assistants
PMDB	Partido do Movimento Democrático Brasileiro
PSK	Pre-Shared Key
QoS	Qualidade de Serviço
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory

ROM	Read-Only Memory
RSA	Rivest Shamir Adleman
RSN	Robust Security Network
RTP	Real Time Protocol
SDH	Synchronous Digital Hierarchy
SEADTE	Serviço de Administração
SEARTE	Serviço de Administração da Rede Telefônica
SEAUS	Serviço de Atendimento ao Usuário
SECOTE	Serviço de Comutação Telefônica
SECT	Serviço de Controle Técnico
SEMT	Serviço de Material de Telecomunicações
SEPROJ	Serviço de Projetos
SEPVOZ	Serviço de Portal de Voz
SESTT	Serviço de Suporte de Telecomunicações e Teleinformática
SET	Serviço de Tarifação
SETM	Serviço de Telefonia Móvel
SNMP	Simple Network Management Protocol
SS7	Signaling System number 7
SSCTEC	Subsecretaria de Convergência Tecnológica
SSID	Service Set IDentifier
STELE	Secretaria de Telecomunicações
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TKIP	Temporal Key Integrity Protocol
TRAU	Transcoder and Rate Adapter Unit
UMTS	Universal Mobile Telecommunication System
VLR	Visitor Location Register
VoIP	Voz sobre IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privancy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WPA	Wi-Fi Protected Access Equivalent Privacy
WWiSE	World Wide Spectruan Efficiency

1. INTRODUÇÃO

A comunicação corporativa é reconhecida como um fator integrante da gestão nas instituições. Atualmente, as informações circulam de forma instantânea e de fácil acesso, e toda essa comunicação exige segurança para que seja usada com veracidade.

Além de toda essa exigência, o crescimento do tráfego de vídeo, de voz e de dados através da Internet e a rápida penetração da telefonia celular têm gerado enormes expectativas quanto às aplicações multimídia móveis. Essa demanda tem motivado, nos últimos anos, o desenvolvimento de tecnologias que permitiram estender os serviços disponíveis às redes de comunicações fixas para usuários em mobilidade, e utilizando criptografia o que dá maior segurança nas comunicações (MOURA, 2009).

No campo das comunicações, podem ser identificadas as tendências de popularização das redes fixas de banda larga e o avanço da comunicação sem fio. O caminho natural é a convergência dessas duas linhas de desenvolvimento. Esse interesse gerou uma grande discussão sobre novas tecnologias sem fio e possíveis padrões que suportem taxas de transmissão em banda larga. Assim, a demanda presente no campo de comunicações sem fio é prover altas taxas de dados para usuário móvel, com o menor consumo de banda possível. Isto implica em alta eficiência espectral, a fim de garantir uma melhor utilização do espectro de frequências. O VoIP (Voz over IP) através do Wi-Fi (Wireless Fidelity) é um desses serviços, com a possibilidade do uso da criptografia o que proporciona segurança na comunicação e pode ser aplicado nas redes da próxima geração (NGN – Next Generation Network).

A NGN é a tendência ou o próximo passo nos sistemas de comunicações mundiais e permitirá a convergência das redes tradicionais de telefonia fixa, móvel, multimídia, wireless e internet, hoje providas separadamente, para uma única infra-estrutura de transmissão em pacotes. Da convergência para uma infra-estrutura inteligente e altamente eficiente derivarão acesso universal e uma gama de novas oportunidades para tecnologias, aplicações e serviços (NASSIF,2004).

A implantação de uma NGN geralmente é faseada, aproveitando os equipamentos existentes e com substituição gradativa, ou com troca total da sua planta. Com a NGN, elas poderão atender às exigências dos usuários existentes e oferecer serviços mais evoluídos por um menor custo, pois os aplicativos são unificados e providos a partir de uma única infra-estrutura de rede. Essa NGN, em sua plenitude, estabelece uma plataforma

tecnológica que possibilita uma variedade praticamente ilimitada de serviços, combinando transporte e tratamento da informação em suas mais diversas formas.

O acesso à banda larga em qualquer local do campus do Senado, com possibilidade de mobilidade entre as antenas (*handover*), como disponibilizado nos celulares, significa uma quebra de paradigma nas comunicações móveis. Os aparelhos podem ser usados com um terminal multimídia fixo, portátil ou móvel, para serviços de navegação *web*, *downloads*, *videostreaming*, acesso às câmeras de segurança, TV ao vivo, telefonia IP (VoIP), mensagens instantâneas, entre outros, com baixo custo na transmissão de dados. Com o uso da tecnologia Wi-Fi, é dado mobilidade a todos esses serviços, tornando alguns inéditos e necessários como o ramal móvel IP, que pode ser acessado pela maioria dos dispositivos Wi-Fi. E com o uso da criptografia entre terminais e protocolos de segurança na rede sem fio, todos esses meios de comunicações passam a ser protegidos, mantendo o sigilo e privacidade esperada por todos os usuários do Senado Federal. Nesse sentido, as redes NGN revolucionam as transmissões de voz e vídeo, para dispositivos portáteis.

1.1. Objetivos do trabalho

Diante do exposto, pode-se concluir que a rede Wi-Fi apresenta diversas características que a credenciam como uma possibilidade para o acesso em mobilidade, com banda larga, às redes de comunicações fixas, móveis e multimídia do Senado Federal. Neste sentido, o presente estudo tem como objetivo mostrar o ambiente de acessos à rede NGN em diferentes tipos de serviços de voz e multimídia, e fornecer principalmente uma comunicação segura e confiável.

Para isso, será feito um comparativo entre o parque tecnológico atual e uma possível implantação da rede NGN.

1.2. Justificativa

O Senado Federal é uma casa legislativa onde há 81 senadores com as mais variadas necessidades de comunicação. Contudo, há um fator que todos exigem: o sigilo destas comunicações, que pode ser quebrado por terceiros. Recentemente foram divulgadas, pelo jornal ESTADÃO, conversas do Senador José Sarney com seu filho e sua neta de caráter

extremamente sigiloso e delicado, consequência de vazamento de informações de dentro da Polícia Federal. Foi interceptado também um diálogo entre o presidente do Supremo Tribunal Federal, Gilmar Mendes e o Senador Demóstenes Torres, conforme reportagem publicada pelo jornal O Globo em 1 de setembro de 2008. A partir deste episódio, todo o sistema de telecomunicações do Senado Federal e das operadoras foi questionado sobre sua segurança. Foi descoberta uma quadrilha que envolvia funcionários das operadoras que vendiam escutas tornando esse processo ainda mais fácil para pessoas mal intencionadas. Com todo este cenário de insegurança nas comunicações, e diante de uma Casa Legislativa com necessidade de Segurança Nacional, faz-se necessária a mudança de paradigma na comunicação. Para que isso ocorra é preciso que haja a implantação de uma nova geração de rede, com o uso de criptografia, que possibilitará um aumento do sigilo nestas comunicações.

1.3. Estrutura do Trabalho

Para que todo esse estudo seja feito, o trabalho será dividido em cinco capítulos. No capítulo 2 é apresentada a comunicação institucional de uma forma geral, detalhando a comunicação interna do Senado e a importância da segurança nessa comunicação. A comunicação interna será desmembrada, delineando os serviços da Secretaria de Telecomunicações, analisando uma possível implantação e comparações entre a tecnologia implantada atualmente, que será mostrada no capítulo 3. Já no capítulo 4 serão analisadas as técnicas de segurança de uma rede sem fio e suas possibilidades de ataque. Serão analisadas também as formas de criptografia na rede fixa e a viabilidade de implantação desta nova rede do ponto de vista operacional. A conclusão final de todos os critérios apresentados será mostrada no capítulo 5, bem como sugestão para trabalhos futuros.

2. COMUNICAÇÃO INSTITUCIONAL

Responsabilidade social, transparência, sustentabilidade e reputação são termos que saíram da esfera acadêmica para uso na administração das empresas. E cada vez mais as entidades possuem órgãos para a prevenção e gerenciamento de crises e para a gestão da imagem e da reputação, normalmente ligados à instância decisória.

Essa iniciativa, até então mais comum nas empresas privadas, já tem lugar também na administração pública. Há expectativas de que o Governo Federal torne cada vez mais rápida a comunicação entre ministérios e secretarias, garantindo mais agilidade à troca de informação. Atualmente o Interlegis já possui essa interligação entre diversas casas legislativas onde disponibiliza inclusive a videoconferência em alta definição.

2.1. Comunicação interna do Senado

A tendência é de que o Legislativo, cuja característica é justamente a contínua interligação com a opinião pública, aperfeiçoe seus sistemas de comunicação corporativa. No Senado Federal, além da criação da TV, Rádio e Jornal, já foram adotadas algumas medidas na direção da comunicação corporativa, a exemplo da criação do DataSenado, que elabora e divulga pesquisas de opinião, visando o aperfeiçoamento do processo legislativo. (Periódico do Senado Federal EM PAUTA, 2009)

O serviço Alô Senado é outro canal que liga esta Casa à população, permitindo a apresentação de questionamentos, dúvidas e reclamações dos cidadãos, geralmente respondidas por parlamentares, o que reforça o mecanismo da representação política.

Para dar transparência aos gastos públicos federais, o Senado também oferece na sua página da Internet, o SIGA BRASIL, projeto premiado como melhor iniciativa pública em matéria de transparência. Trata-se de um instrumento de controle social da política orçamentária, de fácil consulta pela população.

No âmbito da interlocução institucional, em nível técnico, foi criada, em 2005, a Secretaria de Coordenação Técnica e Relações Institucionais, órgão de assessoramento especial da Presidência, que promove o intercâmbio da Casa com outros Poderes, nas três esferas de Governo, e com a sociedade organizada, como forma de identificar ações legislativas que possam aperfeiçoar o funcionamento dessas instituições. Como se vê, gerenciar o fluxo de informações legislativas é um grande desafio para as Casa Políticas, e

há um crescente aumento de demandas de espaços de discussão para os grandes temas nacionais, espaços estes que extrapolam os plenários e as comissões do Parlamento, pela via da comunicação da informação.

Essa comunicação entre a Casa Legislativa e a população é importante, mas a comunicação interna é essencial para o bom funcionamento da Casa. Essa comunicação é gerenciada pela Secretaria de Telecomunicações do Senado Federal – STELE no âmbito da telefonia e pelo PRODASEN – Secretaria Especial de Informática - na área de TI (Tecnologia da Informação).

A Comunicação entre os parlamentares e sua base nos estados atualmente é feita através do uso de celulares ou ramais fixo, o que gera alto gasto nas ligações de longa distância DDD e sem qualquer tipo de proteção podendo ter a conversa gravada pela operadora ou por outros meios. Este risco pode ser eliminado usando na comunicação terminais IP com criptografia tanto no Senado como na base política nos estados.

Outra forma de comunicação interna é entre membros do próprio gabinete e membros das secretarias. Quando um senador está no plenário e o chefe de gabinete necessita iniciar uma conversa, a ligação tem que ser feita para o celular do parlamentar, causando ônus para o Senado Federal. Isso pode ser evitado, com o uso da rede NGN, pois ao configurar o próprio aparelho celular do senador cria-se um ramal móvel com o uso da rede Wi-Fi e o PABX IP do Senado, com toda a segurança que a criptografia oferece.

Outro importante fator é o sigilo nas informações. No ambiente IP é possível criptografar não somente a voz como também o vídeo. Atualmente a segurança na informação é de extrema importância e justifica todo o investimento visando uma rede segura.

Todas essas facilidades de comunicação podem estar unidas em uma única rede e todos esses serviços sendo acessados em um mesmo aparelho móvel e em tempo real. Com isso a rede NGN aumenta os meios e a segurança na comunicação.

2.2. Importância na Segurança da Comunicação

Com a evolução do uso de VoIP em redes IP, fixas ou via WiFi, surgem cada vez mais usuários que necessitam de confidencialidade em suas comunicações. É comum em nosso cotidiano comunicações através da telefonia tradicional, serem violadas por curiosos, espiões e detetives. Com a crescente popularidade, a comunicação VoIP também está com sua segurança ameaçada.

O sistema criptográfico RSA é bastante usado para prover confidencialidade nas transmissões de voz e dados mas para se ter um nível de segurança adequado as chaves devem possuir um tamanho de pelo menos 2048 bits, pois o alto poder de processamento dos computadores atuais combinados com métodos de fatoração de inteiros como o *General Number Field Sieve* podem ameaçar a segurança de sistemas com chaves menores. Tamanhos grandes de chaves implicam em um custo computacional elevado durante o uso destes sistemas criptográficos

Em contraste ao alto poder de processamento de alguns computadores, existem dispositivos móveis, como celulares e PDAs, que possuem um poder de processamento limitado, mesmo assim podem se beneficiar da tecnologia VoIP. O uso do RSA nestes dispositivos pode introduzir atrasos inaceitáveis na comunicação. O uso de sistemas criptográficos baseados em curvas elípticas se populariza e talvez venha desafiar o RSA. O principal atrativo do ECC (*Elliptic Curve Cryptography*) em comparação ao RSA é que aparentemente oferece uma segurança equivalente com um tamanho de chave muito menor (STALLINGS, W. 1999).

3. TELEFONIA DO SENADO FEDERAL

A Secretaria de Telecomunicações – STELE é a responsável por grande parte do Sistema de Telecomunicações do Senado Federal, a qual cumpre sua missão institucional, se empenha por atingir o pleno atendimento em telecomunicações, primando pela alta qualidade, segurança e disponibilidade de seus serviços. Para isso, disponibiliza aos Senadores e demais usuários do sistema os mais eficientes meios de comunicação, contando com um parque tecnológico de última geração que provê a interligação do Senado Federal com o mundo através dos mais variados meios de comunicação, tais como ramais, celulares, fax, dados, caixas postais, *contact center*, telegrama, portal de voz, etc. Dessa forma, a STELE acaba por se firmar como um importante veículo facilitador no processo de integração do cidadão com os seus representantes no Senado Federal (INTRANET DO SENADO FEDERAL, 2009).

3.1. Secretaria de Telecomunicações – STELE

A STELE é um órgão criado pelo então presidente senador Antonio Carlos Magalhães e está dividida em diversos setores que exercem diferentes tipos de serviços integrando todo o campus tecnológico da telefonia do Senado Federal como mostrado no organograma da figura 1.1.

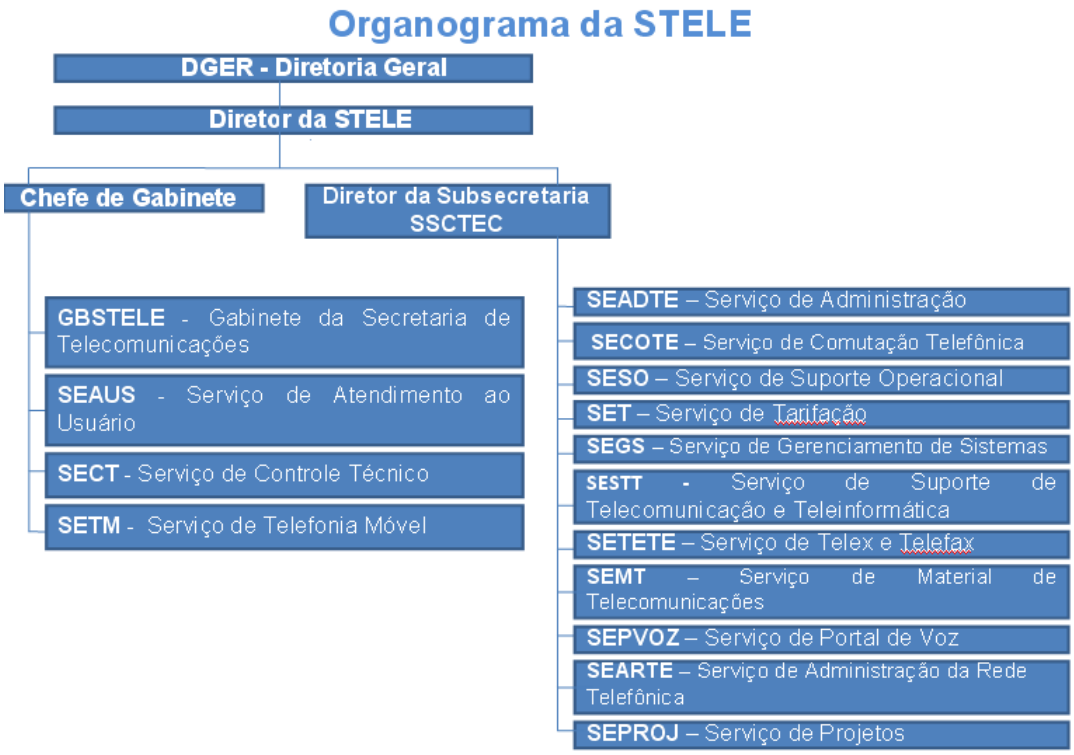

Figura 3.1: Organograma da STELE

3.2. Serviços prestados

A Secretaria de Telecomunicações presta serviço de telefonia móvel, telefonia fixa, fax corporativo, telegrama, dados, caixas postais, *contact center*, telegrama, portal de voz, e para atender todos esses serviços, o órgão é dividido nos serviços a seguir:

SEAUS - Serviço de Atendimento ao Usuário

Ao Serviço de Atendimento ao Usuário compete promover o controle da qualidade dos serviços executados; Realizar vistorias preventivas nos gabinetes parlamentares, residências oficiais e demais órgãos da Casa; Instruir os usuários sobre a operação dos diversos sistemas de telecomunicações disponíveis; Habilitar e programar as facilidades dos equipamentos telefônicos fornecidos aos usuários; Determinar prioridades de atendimento aos demais serviços técnicos da Secretaria; Coordenar os treinamentos dos servidores envolvidos no atendimento; Elaborar e fornecer relatórios com as informações solicitadas.

SECT - Serviço de Controle Técnico

Ao Serviço de Controle Técnico compete Coordenar e administrar o Help Desk da Secretaria; Expedir Ordens de Serviço, controlando e distribuindo os serviços de acordo com as solicitações dos usuários de telecomunicações; Controlar e supervisionar equipe de atendimento; Manter arquivo atualizado das Ordens de Serviço concluídas e em execução; Manter atualizado o Guia Telefônico on-line disponibilizado na intranet; Manter atualizado o Portal de Voz (3303-4141); Manter atualizado a Agenda Eletrônica; E controlar e manter atualizado o banco de dados com as informações dos usuários do Sistema Telefônico do Senado Federal.

SETM - Serviço de Telefonia Móvel

Ao Serviço de Telefonia Móvel compete Gerenciar e controlar as linhas celulares de uso do Senado Federal; Administrar e gerir os contratos e serviços prestados pelas concessionárias e autorizatárias de telefonia móvel; Manter cadastro atualizado de usuários; promover o controle das cotas dos telefones celulares; Controlar e supervisionar equipes de consultores residentes de telefonia móvel; Coordenar os treinamentos aos usuários; Controlar o estoque de terminais e acessórios; Promover pesquisas de tecnologias de telefonia móvel; Auxiliar na elaboração de editais de licitação.

SSCTEC - Subsecretaria de Convergência Tecnológica

À Subsecretaria de Convergência Tecnológica compete coordenar as atividades de desenvolvimento tecnológico na área de telecomunicações; implementar as políticas de telecomunicações determinadas pelo titular da Secretaria; prestar assessoria técnica e administrativa, controlando e coordenando as atividades dos serviços técnicos.

SECOTE - Serviço de Comutação Telefônica

Ao Serviço de Comutação Telefônica compete controlar, manter e operar o PABX do Senado Federal, bem como os periféricos a ele interligados; Programações em geral como, categorias e facilidades para ramais e periféricos do PABX MD 110; Programações de rotas de menor custo; Controlar e manter o Contact Center do Senado Federal; Administrar

os contratos e serviços prestados pelas empresas especializadas na manutenção de equipamentos de propriedade do Senado Federal; Promover, em consonância com o Serviço de Projetos, a atualização das tecnologias e equipamentos existentes; Controlar o acesso às instalações do PABX, bem como de outros locais onde se encontrem instalados equipamentos de telecomunicações, garantindo sua segurança e integridade; Promover pesquisas de atualização tecnológica e oferecer sugestões ao titular da diretoria; Emitir relatório de atividades.

SET - Serviço de Tarifação

Ao Serviço de Tarifação compete controlar e processar as contas telefônicas das linhas e ramais, através de sistema de tarifação; suporte na administração e gerência dos contratos e serviços prestados pelas concessionárias e autorizatárias de telefonia fixa; Suporte à promoção de glosas nas faturas; Suporte ao atesto, para pagamento, das faturas corretas; Expedir e enviar detalhamento de contas de ramais e linhas para todos os usuários via Intranet; Suporte na elaboração de editais de licitação de telefonia fixa e móvel.

SESTT - Serviço de Suporte de Telecomunicações e Teleinformática

O Serviço é responsável pela Informática da Secretaria de Telecomunicações, com atribuições específicas relacionadas ao Sistema STELE, desenvolvido para atender às áreas técnicas, e atribuições amplas de participação em novos projetos e produtos que envolvem sistemas de informação e sistemas especializados de informática e telecomunicações.

O Sistema STELE permite cadastro, consulta, relatório e exportação das seguintes informações:

- Terminais Telefônicos
- Órgãos do Senado Federal e órgãos externos
- Central Telefônica
- Rede Telefônica
- Aparelhos Telefônicos e de fac-símile
- Ordens de Serviço
- Fichas de Atendimento
- Lista Telefônica
- Gestão de contratos de Conta Telefônica

O Sistema STELE também exporta informações para os seguintes sistemas:

- Portal de Voz
- Sistema de Atesto de Contas Telefônicas
- Lista telefônica da página web da STELE na intranet

SEMT - Serviço de Material de Telecomunicações

Ao Serviço de Material de Telecomunicações compete o controle de todos os equipamentos de telecomunicações, peças de reposição, bens de consumo de telecomunicações, mobiliário técnico e material de expediente; Guardar os equipamentos eletrônicos em conformidade com as normas técnicas de telecomunicações e as orientações de cada fabricante; Controlar o estoque e promover a requisição de compra de materiais e equipamentos; Manter arquivo atualizado da movimentação dos equipamentos de telecomunicações e seus respectivos tombamentos; Emitir relatório de atividades e executar outras tarefas correlatas.

SEPVOZ - Serviço de Portal de Voz

O serviço é responsável pela manutenção de todos os sistemas que incluem o portal de voz, 0800 (a voz do cidadão) e a Agenda eletrônica. Tem como principais competências controlar, manter e operar o Portal de Voz do Senado Federal, bem como os periféricos a ele interligados; Controlar e manter o Portal de Voz Corporativo e o Portal de Voz do 0800 da Secretaria de Pesquisa e Opinião Pública do Senado Federal; Administrar contratos e serviços prestados por empresas especializadas na manutenção de equipamentos de propriedade do Senado Federal; Administrar contratos e serviços prestados ao Senado Federal por empresas de Telecomunicações; Promover, em consonância com o Serviço de Projetos, a atualização das tecnologias e equipamentos existentes; Controlar o acesso às instalações do Portal de Voz, bem como de outros locais onde se encontrem instalados equipamentos de telecomunicações, garantindo sua segurança e integridade; Promover pesquisas de atualização tecnológica e oferecer sugestões ao titular da diretoria; Emitir relatórios de atividades e executar outras atribuições correlatas; Executar rotinas diárias de manutenção preventiva nos equipamentos do Portal de Voz e seus periféricos; E realizar a gestão de contratos com empresas terceirizadas, além de participar de especificações de

implantação de novos sistemas solicitados pela STELE o por qualquer outro órgão da Casa.

SEARTE - Serviço de Administração da Rede Telefônica

Ao Serviço de Administração da Rede Telefônica compete acompanhar todas as manutenções ou ampliações que envolvam infra-estrutura de telecomunicações no âmbito do Senado Federal, das Residências Oficiais e da Residência do Presidente do Senado Federal.

É executado por este Serviço manutenções corretivas em todas as instalações telefônicas a partir de nossos distribuidores gerais, passando por distribuidores secundários, até os pontos telefônicos que se encontram por toda a planta arquitetônica do Senado Federal, das Residências Oficiais e da Residência do Presidente do Senado Federal.

O SEARTE realiza também os seguintes serviços:

- Instalação de ramais, linhas diretas e linhas privadas.
- Instalação de aparelhos telefônicos analógicos, aparelhos telefônicos digitais, fones de ouvido e expansores de teclas para aparelhos telefônicos digitais.
- Instalação de linhas diretas ou ramais para eventos temporários.
- Acompanha instalações e manutenções realizadas pelas operadoras de telefonia sobre linhas diretas e linhas privadas.
- Realiza manutenções corretivas para restabelecer as condições ideais para o uso do sistema telefônico, detectando e eliminando defeitos que venham a impedir o seu correto funcionamento.
- Troca de aparelhos telefônicos, fones de ouvido e expansores se detectado defeito que não possa ser corrigido no local.
- Remanejamento de ramais, linhas diretas e linhas privadas
- Desinstalação de ramais, linhas diretas e linhas privadas,
- Reposição de aparelhos telefônicos em caso de extravio devidamente comunicado para a SPATR e SESEG.

Vistorias para auxilio ao serviço de projetos no levantamento de informações e acompanhamento de obras no sistema telefônico do Senado Federal, das Residências Oficiais e da Residência do Presidente do Senado Federal. Cabe também ao Serviço de

Administração da Rede Telefônica realizar buscas em possíveis interceptações no sistema telefônico.

SEPROJ - Serviço de Projetos

O SEPROJ é responsável pela elaboração de projetos diversos, acompanhamento e vistoria de obras na área de telefonia do Senado Federal e tem como competências a administração, desenvolvimento, manutenção e controle de todos os projetos de telecomunicações da Subsecretaria; Implementar os projetos de rede telefônica interna e a atualização das tecnologias e equipamentos existentes; Promover a conservação das instalações físicas da Secretaria; Elaborar o planejamento e o orçamento do órgão; Adequar a estrutura física às normas técnicas de telefonia; Promover o mapeamento de toda a rede telefônica existente, através de meio eletrônico, inclusive de áreas onde inexistem plantas de rede; Controlar as redes internas de celulares das operadoras, promovendo ou determinando medições periódicas das freqüências nos diversos ambientes do Senado Federal; Pesquisar e especificar os softwares e hardwares necessários ao permanente desenvolvimento do Sistema.

3.3. Tecnologias existentes

Dentre todos os serviços mostrados anteriormente, a telefonia fixa e móvel são as tecnologias mais usadas pelos servidores e parlamentares do Senado e serão mostrados detalhadamente a seguir.

3.3.1. Telefonia Fixa

A telefonia fixa abrange mais de 5000 ramais e cobre todo a campus do Senado. A Central de telefonia existente é da marca Ericsson e tem vários recursos importantes. Siga-me, conferência, chamada em espera, são alguns serviços que podem ser feitos pelos aparelhos apresentados na Figura 3.2.

Figura 3.2: Telefones digitais do PABX do Senado

Apesar de todas essas facilidades, segundo estudos recentes do fabricante do PABX do Senado Federal, 70% das ligações entre ramais não são completadas, por diversos motivos. Geralmente destinatário está em reunião, em deslocamento ou pausa para o lanche e para localizar é necessário fazer uma ligação para o celular, que é uma ligação tarifada e externa ao PABX, gerando custos para o Senado.

3.3.2. Telefonia Celular

Atualmente existem duas operadoras de telefonia móvel. O contrato inicial foi feito com a operadora VIVO, mas em 2006 devido a problemas com clonagem de celulares, foi aberta uma licitação para cobrir as áreas onde a VIVO não tinham licenças com a Anatel e operava com a tecnologia Analógica. A licitação foi vencida pela operadora TIM e como atualmente todas as operadoras de Serviço Móvel Pessoal (SMP) já possuem a tecnologia GSM, será refeita a licitação unindo o contrato em uma só operadora.

Recentemente todas as prestadoras operam na tecnologia GSM, a qual nunca foi clonada, e apresentam uma estrutura de rede mostrada na figura 3.3.

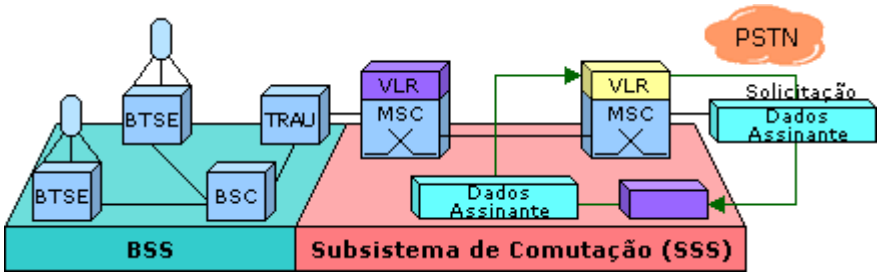

Figura 3.3: Rede GSM

3.3.2.1 Estação Móvel

Corresponde ao equipamento móvel (terminal) e um cartão inteligente designado de SIM que conecta-se à rede GSM através da BTS. O cartão providencia mobilidade pessoal,

de tal forma que o assinante consegue ter acesso aos serviços subscritos independentemente do terminal utilizado, isto é, ao inserir o cartão SIM num terminal diferente, o assinante pode usufruir dos serviços a partir desse terminal.

O cartão SIM tem uma identificação única mundial (IMSI), assim como o terminal (IMEI). Estes códigos são independentes permitindo uma maior mobilidade e uma segurança pessoal contra o uso não autorizado.

3.3.2.2 BSS – Base Station Subsystem

A BSS é composta por uma BSC e várias Base Transceiver Station (BTS). A BSS é responsável por 70% do hardware da rede, sendo o seu valor um fator importante na escolha pela operadora na introdução do GPRS ou nas atualizações das suas redes.

3.3.2.3 BTS – Base Transceiver Station

A BTS é composta pelos equipamentos de recepção e transmissão, incluindo antenas e todas as sinalizações relacionadas com a interface de radio. Cada Operadora tem uma BTS no Senado e mais de 100 antenas *indoor* para cobrir toda área dos gabinetes e plenário.

3.3.2.4 BSC – Base Station Controller

Em termos de *hardware*, a BSC requer o *Packet Control Unit* (PCU) para gerir o tráfego dos pacotes do voz. O PCU é responsável pelas camadas *Radio Link Control* (RLC) e *Medium Acces Control* (MAC) sobre a interface aérea, e em particular, controla a transferência dos pacotes do *Mobile Station* (MS) para o MSC. Geralmente a BSC tem a função de estabelecer, supervisionar e interromper as ligações durante a transição entre as BTS (*handover*).

3.3.2.5 TRAU - Transcoder and Rate Adapter Unit

TRAU é o equipamento que realiza as tarefas de codificação e decodificação, bem como a adaptação da taxa de dados.

3.3.2.6 MSC – Mobile Services Switching Center

O MSC realiza funções de comutação de circuitos do sistema GSM com outras redes de voz (PSTN, PLMN) e redes de comutação de circuitos de dados (ISDN). Através dela que a ligação feita para outras operadoras são completadas.

3.3.2.7 HLR – Home Location Register

A base de dados HLR contém a informação sobre todos os usuários pertencentes à operadora.

3.3.2.8 VLR - Visitor Location Register

A base de dados VLR contém a informação sobre todos os assinantes móveis de outras operadoras de outros estados localizados na área de serviço da MSC visitante. Os dados existentes são os mesmos que os encontrados no HLR da rede de origem do assinante.

Durante um "*location update*" - atualização de localização (quando o assinante se move para a área de serviço de outro VLR), o novo VLR requisita os dados do assinante ao HLR.

Nota-se que para efetuar qualquer ligação extra rede, fora o custo da operadora de origem e de destino, tem o tributo da Anatel de interconexão, o que torna o custo da ligação ainda mais alta. Com a implantação da rede NGN, todo este caminho é desfeito e a ligação entre celulares ou entre a rede fixa e a rede móvel dentro do campus do Senado é feita diretamente do PABX, toda criptografada, como será mostrado em detalhes no capítulo seguinte.

3.3.3. Canais de TV e rádio ao vivo via streaming

O Prodasen, responsável por todo o ambiente IP do Senado Federal, disponibiliza canais de TV e rádio ao vivo através do portal http://intranet/vip via rede interna utilizando a tecnologia *streaming*. Essa tecnologia torna eficiente o download e a execução de áudio e vídeo na internet. Esta técnica possibilita a reprodução dos arquivos de áudio ou vídeo enquanto ainda se está realizando o download. Sem o uso do *streaming*, seria necessário realizar o download de todo o arquivo e posteriormente executa-lo

O termo *streaming* deriva da palavra *stream*, ou seja, fluxo contínuo, pois os pacotes são enviados na forma de uma corrente que ao chegar ao seu destino permite que estes sejam remontados. Este tipo de armazenamento é denominado *bufer*.

Assim, neste processo, o computador do cliente conecta-se ao servidor e este, começa a lhe mandar o arquivo. O cliente começa a receber o arquivo e constrói um buffer onde começa a salvar a informação. Quando se enche o buffer com uma pequena parte do arquivo, o cliente começa a executar o arquivo ao mesmo tempo em que o download continua a ser executado. O sistema é sincronizado de tal forma que o arquivo possa ser executado ao mesmo tempo em que o download é processado, assim, quando o download for concluído a execução do mesmo também o será.

Na conexão sem fio os fluxos são inconstantes, a velocidade de transferência do arquivo pode variar muito, e até ser momentaneamente interrompida. Para que não haja interrupção durante a reprodução do vídeo usa-se um recurso chamado *buffer*. O vídeo recebido é parcialmente arquivado em um buffer local, geralmente numa memória temporária, que armazena antecipadamente alguns segundos desse vídeo, o que garante que não haja interrupções momentâneas caso o fluxo se torne muito lento.

Quando o *buffer* é preenchido, o *player* começa a reproduzir o conteúdo. Paralelamente à exibição, o *download* prossegue, preenchendo continuamente o buffer, até que se encerre o conteúdo.

Foi analisada na prática uma diferença de 25 segundos em média entre a transmissão do canal na televisão e na Estação Móvel. Essa diferença é exatamente o buffer de armazenamento do vídeo. Quanto menor for à taxa de transmissão maior é a necessidade do armazenamento do buffer e quanto maior for a qualidade do vídeo, mantendo uma mesma taxa de transmissão, maior deve ser o buffer também. Caso a conexão seja totalmente perdida, o buffer se esvaziará e a execução do arquivo será perdida.

Esse armazenamento na memória temporária não requer muito hardware. Sendo uma vantagem, pois as Estações Móveis atualmente não possuem grandes capacidades de armazenamento.

3.4. Tecnologia a ser implantada

Tendo em vista a importância de uma rede segura, onde os usuários podem usufruir de todos os recursos que é proporcionada sem o receio de estarem sendo monitorados, justifica uma decisão pela implementação de uma rede NGN.

A onipresença da Internet é real, tanto no segmento corporativo, na qual o aumento da produtividade é resultante da transformação gerada pelo e-business, como no segmento residencial com a crescente demanda por serviços diferenciados, em particular os relacionados ao entretenimento. São serviços que requerem uma largura de banda cada vez maior e crescentes taxas de transporte que garantam a qualidade e o desempenho esperados pelo usuário.

Se por um lado é real que o tráfego gerado pela Internet cresce exponencialmente, e o tráfego de voz se mantém com crescimento mais lento, também é bastante clara a forte queda nas tarifas dos serviços de conectividade e, por conseguinte, das receitas médias geradas por usuário. Além disso, ao contrário do comportamento relativamente previsível do tráfego gerado por serviços de voz, o tráfego gerado pelo ambiente Internet tem enorme volatilidade. Por exemplo, o acesso de centenas de usuários em um determinado evento no plenário do Senado, gerando picos de utilização sem precedentes em uma rede, em um determinado momento, e em outros momentos pode estar totalmente ocioso. Portanto, torna-se essencial disponibilizar uma solução de rede que seja extremamente flexível para o provimento de serviços diferenciados e sob demanda, que associe o desempenho e a confiabilidade da atual infra-estrutura das redes de telefonia e de dados e que possa sustentar o crescimento de novas demandas.

Analistas e especialistas do mercado de telecomunicações observam que é um consenso a tendência de que a tecnologia IP passe a ser o ambiente dominante para o transporte de serviços por pacotes, possibilitando maior flexibilidade no provimento de novos serviços de voz, multimídia e de banda larga (SEM BRASIL, 2009).

Dessa forma, a migração de plataformas de telecomunicações para um ambiente que associe as vantagens tecnológicas do IP (flexibilidade e rapidez no provimento) às

vantagens das tecnologias TDM tradicionais (confiabilidade, desempenho e proteção de rede) é um fator crucial para o sucesso futuro de empreendimentos nos segmentos de operadoras de serviços de telecomunicações, corporativo e governo.

De acordo com pesquisas realizadas, quase 90% das maiores corporações européias planejam a implementação de redes convergentes nos próximos dois anos. Em 2006, 50% do mercado de comutação privada para o atendimento de pequenas, médias e grandes empresas serão relacionadas a redes convergentes. Em 2005, 45% das linhas instaladas na Europa serão baseadas em tecnologia IP (SIEMENS, 2006).

Outro estudo semelhante realizado pela Siemens no Brasil, com um universo de 3.200 pequenas, médias e grandes empresas, revela que cerca de 30% planeja migrar suas redes corporativas para um ambiente convergente nos próximos anos, enquanto 15% já optou pela migração. Isso demonstra existir uma enorme massa crítica de usuários que viabiliza a construção de redes NGN pelas operadoras de serviços de telecomunicações.

O ambiente IP permitirá ao Senado oferecer novos serviços, aplicações, comodidade e segurança aos Parlamentares e usuários de uma maneira mais eficiente e a custos reduzidos, quando comparados a uma rede de serviços baseadas em circuitos.

A implementação de uma infra-estrutura de rede convergente para o provimento de serviços de voz e dados integrados, em contraste com as atuais plataformas independentes, representa um enorme potencial de redução de custos de operação e manutenção de rede. Verifica-se que, na atual topologia de rede, quanto maior a diversidade de serviços associados, maior será a quantidade de elementos e a complexidade da rede. Mas as NGN, ao contrário, possibilitam uma redução de até 80% dos elementos de comutação, resultando em até 40% de redução nos custos operacionais e de manutenção da rede. Em mercados competitivos, como o brasileiro, algumas importantes oportunidades de negócio favorecem a introdução gradual de soluções NGN. Um exemplo é a redução de custos operacionais com VoIP *trunking*. Atualmente, os serviços de voz e dados são providos por redes independentes e algumas operadoras planejam estender a prestação de serviços de telecomunicações para outras áreas de atuação, podendo conectar-se o PABX IP do Senado diretamente nas operadoras de Telecomunicações, não precisando assim pagar interconexão entre operadoras.

Uma alternativa para essa mudança, é a introdução de componentes de comutação que viabilizem a implementação de redes convergentes e eliminem a necessidade da camada de trânsito de redes. Na etapa inicial, seriam implementados *softswitches* para a realização do controle da rede e dispositivos media gateways para a interligação das redes

de voz e dados existentes, possibilitando, assim, a eliminação da camada de trânsito nas redes de telefonia.

Desse modo, a migração dos serviços de voz de uma complexa rede por circuitos para uma rede flexível por pacotes ocasiona uma redução significativa da quantidade de elementos de rede, e, conseqüentemente, uma redução substancial nos custos de operação e manutenção e também nas ligações de longa distância.

Em seguida, as diversas aplicações multimídia poderiam ser implementadas por meio da infra-estrutura já existentes, disponibilizando canais como TV Senado ou TV Câmara, nos celulares dos Senadores através da rede WiFi.

O impacto das inovações tecnológicas no cotidiano tem ocasionado contínuas e significativas mudanças na relação de comodidade e qualidade de vida das pessoas. A crescente demanda por serviços multimídia, tanto no ambiente residencial como no corporativo, viabiliza uma extensa gama de novas aplicações e oportunidades de crescimento. Vídeo sob demanda, TV interativa, jogos interativos online, e-learning, telemedicina, teletrabalho, Web conferencing e websurfing são alguns exemplos associados a novos conteúdos e aplicações multimídia que atendem uma nova demanda por elevada flexibilidade e mobilidade.

Para garantir o atendimento às necessidades do usuário e disponibilizar serviços e aplicações multimídia com as redes convergentes é imprescindível o provimento de uma infra-estrutura eficiente e flexível que possibilite a melhor utilização do meio de transporte óptico. Dessa forma, as atuais redes ópticas migram de um modelo de conexões estáticas para um modelo que passa a incorporar características de transporte inteligentes, viabilizando o transporte integrado e otimizado de serviços por pacotes (IP) e TDM (SDH, por exemplo), a ocupação de banda sob demanda e o roteamento automático do tráfego.

Incorporando novas funcionalidades e facilidades, as redes totalmente ópticas viabilizam dinamicamente serviços de VPN, largura de banda sob demanda, roteamento óptico e dinâmico, possibilitando, portanto, enorme flexibilidade e otimização de rede com custos reduzidos de implementação para o usuário.

Enfim, a implementação de NGN terá um impacto decisivo nos modelos de negócios de serviços de telecomunicações, gerando soluções com maior segurança de utilização de rede e eficiência em sua infra-estrutura orientada à demanda de tráfego, bem como a um pacote completo e amplo de novos serviços de multimídia e banda larga. Assim, a chave para o sucesso está no trabalho conjunto entre o Prodasen, que controla

toda essa demanda da rede IP, e a STELE na qual compete a incorporação de novas tecnologias de telefonia fixa e móvel.

A estratégia deverá ser a de congregar as soluções e as oportunidades para desenvolver inovadores modelos tecnológicos e proteger o patrimônio dos investimentos realizados, garantindo a maximização da satisfação e segurança da comunicação dos usuários.

3.4.1. Serviços da NGN

O maior estímulo para a mudança das redes é a segurança na comunicação e a redução de custos. A rede NGN proporciona o uso de criptografia o que aumenta o sigilo nas comunicações. Os custos dos equipamentos de telecomunicações têm caído na mesma proporção dos computadores residenciais e isso tem estimulado o crescimento e o uso das redes. Outra economia é o uso compartilhado da infra-estrutura, operação, manutenção e serviços. Por exemplo, uma NGN implementa soluções que usam um acesso IP para várias redes privadas, para acesso à Internet e para os tradicionais PABX, resultando em reduções significativas de custos.

A Internet e os acessos on-line trouxeram milhões de consumidores potenciais, entretanto, a convergência dos serviços será a grande oportunidade para novos negócios, não apenas a redução de custos. Os novos serviços serão orientados pelos seguintes itens:

- A criptografia ponto a ponto dos equipamentos IP, tornando o VoIP uma comunicação segura;
- Novas aplicações avançadas que organizam a forma de trabalho. *Streaming* de vídeo, *ecommerce* e os leilões on-line são exemplos da denominada “aplicações de conteúdo específico”, enquanto a vídeo conferência com o compartilhamento de documentos através da Web é um exemplo de “aplicação de rede”;
- A conectividade universal, os equipamentos multifuncionais, o aprovisionamento de serviços e facilidades e os serviços que ultrapassam os limites das redes de telecomunicações do Senado, podendo se conectar com segurança, via VPN, até mesmo de outros paises.
- A opção da indústria por sistemas abertos torna a integração das redes viável. A consolidação do mundo da voz (VoIP, voz através de rede sem fio e a telefonia tradicional) e o mundo dos dados em dois ambientes distintos (Internet, Intranet,

transmissão sem fio e transmissão através da rede de voz) é uma significativa mudança sem ter que usar gateways e configurar interfaces.

- Processamento digital de sinais: o processamento dos sinais digitais é a tecnologia chave para a integração do tráfego de voz e dados. A vantagem dessa área é a facilidade de compressão de voz e a sua conversão para pacotes de dados;
- Roteamento dos pacotes: os recentes protocolos de roteamento permitem priorizar as filas e pacotes das aplicações que exijam qualidade de serviço (QoS);
- Redes ópticas: as redes ópticas aumentam, dramaticamente, a banda de transmissão que está disponível pelos provedores de telecomunicações e dos usuários. As vantagens da multiplexação por comprimento de onda e o roteamento por comprimento de onda deverá consolidar o roteamento nas redes ópticas;
- Protocolos avançados: desde que o TCP/IP tornou-se um protocolo estratégico, muitos esforços estão sendo feitos para conceber novas funções e aumentar sua performance. As redes IP em breve deverão ser capazes de prover a mesma qualidade de serviço encontradas nas redes ATM atualmente. Recentes avanços incluem o protocolo RTP (Real time Transfer Procotocol), o MPLS, o SS7-to-IP e a classe de serviço diferenciada (DiffServ).
- Aparelhos de última geração, Figura 3.4, agregando aplicações de dados, voz e vídeo, e tudo isso criptografado e com segurança.

O tráfego convergente tem trazido considerável interesse aos órgãos públicos, pois tem oferecido vários tipos de serviços e unindo as filiais em uma rede (*Backbone*). O Serpro é um exemplo bem sucedido desta convergência usando o VoIP nas ligações entre filiais. Nem os tradicionais serviços de telefonia nem os novos provedores de NGN serão competitivos apenas reduzindo os custos, entretanto, o ponto chave é o QoS, características como performance, disponibilidade, flexibilidade e adaptabilidade, são essenciais para uma boa comunicação.

Figura 3.4: Aparelhos de telefonia IP

3.5. Rede Wi-Fi

O Institute of Electrical and Electronics Engineers (IEEE) formou um grupo de trabalho com o objetivo de definir padrões de uso em redes sem fio. O padrão IEEE 802.11 começou a ser criado com a formação de um grupo de trabalho em 1991 com o objetivo de acrescentar uma nova camada física e de Data Link ao modelo ISO, dessa forma provendo Ethernet sobre radiofreqüência. A primeira versão do IEEE 802.11 foi lançada em 1995, que define como deve ser a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes[17]. Ao longo do tempo foram criadas várias extensões destas especificações, onde foram incluídas novas características operacionais e técnicas. O padrão 802.11 original oferece até 2Mbps e opera na frequência não licenciada pela anatel de 2,4 GHz. A evolução do padrão 802.11 está nos tópicos subsequentes:

3.5.1.1 802.11a

O padrão IEEE 802.11a, lançado em 1999, utiliza uma técnica de modulação conhecida pela sigla OFDM (Orthogonal Frequency Division Multiplexing), que possibilita um uso mais eficiente e otimizado da largura de banda alocada através da distribuição dos dados por múltiplos portadores com espaçamento preciso. Desta forma, cada portadora é identificada de forma única, eliminando a necessidade de reservar parte da banda para isolamento.

O IEEE 802.11a utiliza freqüência de 5 GHz através de 12 canais e pode atingir taxas de transmissão de 54 Mbit/s. A grande vantagem do IEEE 802.11a é o uso dessa freqüência, já que não ocorrem tantas interferências como nos padrões que utilizam 2.4 GHz. Por utilizar a técnica OFDM e frequências diferentes, o IEEE 802.11a não possui compatibilidade com o padrão IEEE 802.11b que será apresentado a seguir.

3.5.1.2 802.11 b

Em julho de 1999 a IEEE ratificou o padrão IEEE 802.11 b, uma nova extensão do IEEE 802.11. Utilizando o Direct-Sequence Spread Spectrum (DSSS) e a técnica de

modulação Complementary Code Keying (CCK), o IEEE 802.11b opera na freqüência de 2.4 GHz, conhecida como Industrial Scientific and Medical (ISM) que não necessita de licença para utilização. A taxa de transmissão pode atingir 11 Mbit/s com fallback para 5.5, 2 e 1 Mbps, abaixo dos 54 Mbps do padrão anterior.

Permite um número máximo de 32 clientes conectados. Há limitação em termos de utilização de canais, sendo ainda hoje o padrão mais popular e com a maior base instalada, com mais produtos e ferramentas de administração e segurança disponíveis. Contudo, esse padrão chegou ao seu limite e já está sendo substituindo pelo padrão 802.11n, padrão adotado pelo Prodasen, e será detalhado posteriormente.

3.5.1.3 802.11g

Homologado em Junho de 2003, o padrão IEEE 802.11g vêm se tornando à solução *wireless* substituta do IEEE 802.11b, que opera na mesma freqüência e permite um mesmo equipamento com ambos os padrões (b e g) coexistam no mesmo ambiente, possibilitando assim evolução menos traumática na infraestrutura instalada.

Este padrão resgata várias características positivas dos padrões anteriores como da técnica de modulação OFDM do IEEE 802.11b, além de atingir taxas de transmissão de até 54 Mbps do IEEE 802.11a.

3.5.1.4 802.11i

O Task Group IEEE 802.11i foi criado para melhorar as funções de segurança do protocolo 802.11 MAC, que agora é conhecido como Enhanced Security Network (ESN). Lançado em junho de 2004, este padrão utiliza técnicas autenticação e privacidade e pode ser implementado, em vários de seus aspectos, nos protocolos já existentes. O principal protocolo de rede definido neste padrão é chamado RSN (Robust Security Network), que permite meios de comunicação mais seguros e insere protocolos como o WPA, que foi desenhado para prover soluções de segurança mais robustas, em relação ao padrão WEP, além do WPA2, que tem por principal característica o uso do algoritmo criptográfico AES (Advanced Encryption Standard). A missão do ESN é unificar todos os esforços para melhorar a segurança das WLANs. Sua visão é consiste em avaliar os seguintes protocolos:

- Wired Equivalent Protocol (WEP)
- Temporal Key Integrity Protocol (TKIP)
- Advanced Encryption Standard (AES)
- IEEE 802.1x para autenticação e criptografia.

Percebendo que o algoritmo RC4 não é robusto o suficiente para as futuras necessidades, o grupo de trabalho 802.11i está trabalhando na integração do AES dentro da subcamada MAC. O AES segue o padrão do DES – Data Encryption Standard. Como o DES o AES usa criptografia por blocos. Diferente do DES, o AES pode exceder as chaves de 1024 bits, reduzindo as possibilidades de ataques.

3.5.1.5 802.11n

Também conhecido como WWiSE (*World Wide Spectruan Efficiency*), este é uma padrão em desenvolvimento, cujo foco principal é o aumento de eficiência espectral e de velocidade (cerca de 100 a 500 Mbps) com o uso de antena MIMO e técnicas OFDMA . Este padrão assemelha com o WiMAX e LTE por usar essas duas técnicas técnica de múltiplo acesso com subcanalização escalável podendo compartilhar na mesma subportadora vários usuários. O objetivo do OFDMA é realizar uma transmissão paralela de dados a baixas velocidades e com multiplexação de frequências em subcanais sobrepostos, o que evita o uso de equalização e explora de maneira eficiente a largura de banda disponível (IEEE,2004). Outra técnica importante é o uso de múltiplas antenas MIMO (*Multiple Input, Multiple Output*) tanto na transmissão quanto na recepção o que melhora seu desempenho.

Quando dois transmissores e dois ou mais receptores são usados, dois canais de transmissão podem ser utilizados duplicando a taxa de transferência de dados, além de aumentar a distância entre os equipamentos (MOURA, 2009).

Várias são as vantagens de se utilizar múltiplas antenas ao invés de uma. Entretanto, os termos *input* e *output* são relativos às transmissões no ar e não aos equipamentos. Nessa notação particular, múltiplos *inputs* (MI) significa que múltiplos transmissores enviam múltiplos fluxos de dados no ar; múltiplos *outputs* (MO) significa que múltiplos receptores estão recebendo múltiplos fluxos de dados através do ar.

A Fig. 3.5 mostra as formas possíveis de transmissão e recepção utilizando a tecnologia de múltiplas transmissões e recepções.

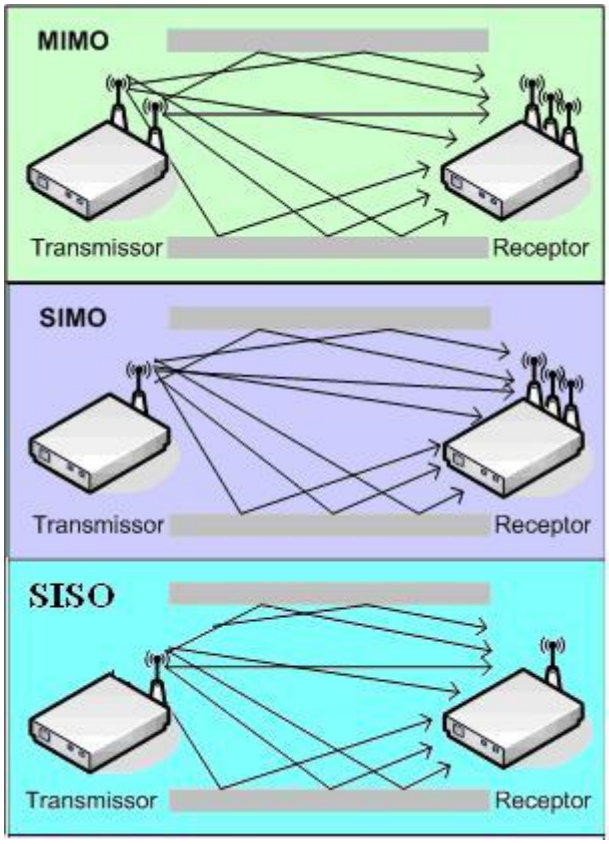

Figura 3.5: Tecnologias de múltiplas transmissões e recepções.

O 802.11n pode trabalhar com canais de 40 MHz e, também, manter compatibilidade com os de 20 MHz atuais, mas neste caso as velocidades máximas oscilam em torno de 135 Mbps.

O Prodasen está em fase de licitação deste padrão, o qual incorpora o uso de diversos serviços, inclusive o VoIP. Toda estrutura de rede fixa e sem fio é de responsabilidade do Prodasen, ficando a cargo da STELE o gerenciamento, qualidade e tarifação das ligações.

3.5.1.6 802.1x

Mesmo não sendo projetado para redes sem fio, o 802.1x possui características que são complementares a essas redes, pois permite autenticação baseada em métodos já consolidados, como o RADIUS (Remote Authentication Dial-In User Sevice), de forma

escalável e expansível. Desta maneira é possível promover um único padrão de autenticação, independentemente da tecnologia, e manter a base de usuários em um repositório único, quer seja em banco de dados convencional, LDAP ou qualquer outro reconhecido pelo servidor de autenticação.

IEEE 802.1x é um padrão IEEE para controle de acesso à rede com base em portas e faz parte do grupo IEEE 802.1 de protocolos de redes de computadores, evidenciando um mecanismo de autenticação para dispositivos que desejam juntar-se à uma porta na LAN, seja estabelecendo uma conexão ponto-a-ponto ou prevenindo acesso para esta porta se a autenticação falhar. É usado para a maioria dos Access points sem fio 802.11 e é baseado no Protocolo de Autenticação Extensiva (EAP). Utiliza-se também com a presença de um elemento autenticador, tipicamente um servidor RADIUS, e um requerente, ou seja, o elemento que requer autenticação, no caso o equipamento cliente. Essa autenticação é feita antes de qualquer outro serviço de rede estar disponível ao usuário requerente. Este, primeiramente, solicita autenticação ao autenticador, que verifica em sua base de dados as credenciais apresentadas pelo cliente, e conforme a validade ou não dessas credencias (normalmente o binômio usuário/senha), permite ou não o acesso a estas. Uma autenticação bem-sucedida irá deflagrar todos os outros processos para permitir ao usuário acesso aos recursos da rede, o que pode incluir receber um endereço via DHCP ou outro protocolo de atribuição de endereços IP, com informações de roteamento, servidores DNS, liberar roteamento na porta pelo switch, etc.

Para redes sem fio somente estará apto a fazer uso dos serviços da rede o cliente que estiver devidamente autenticado no servidor RADIUS. O 802.1x pode utilizar vários métodos de autenticação no modelo EAP (Extensible Authentication Protocol), que define formas de autenticação baseadas em usuário e senha, senhas descartáveis (One Time Password), algoritmos unidirecionais (hash) e outros que envolvam algoritmos criptográficos (SOUZA; MONTALVÃO; RAMOS, 2006).

3.6. Convergência Tecnologia e serviços agregados

Com o avanço cada vez maior na utilização de aparelhos portáteis, como os notebooks, os PDA’s (Personal Digital Assistance) e celulares, pode-se verificar a agregação de diversas facilidades a estes aparelhos. Com todas essas possibilidades, e com a convergência de diversas tecnologias, surge então serviços não existentes atualmente.

Serviços como videoconferência, informativos e alertas na tela do telefone fixo, VoIP em dispositivos móveis e a visualização do status de presença do destinatário são alguns exemplos desta convergência e estão mostradas na figura 3.6.

Figura 3.6: Exemplos de serviços da rede NGN.

A videoconferência é um recurso bastante útil para o parlamentar que necessita de uma constante comunicação com sua base eleitoral no estado. Essa solução permite uma comunicação áudio visual com a sensação de estar no mesmo ambiente. Quando se estabelece a comunicação entre a origem e o destinatário, é fechada uma VPN, a qual cria um túnel entre as partes dificultando a intrusão de terceiros. Além desta proteção pode-se incluir criptografia nos aparelhos o que dificulta ainda mais uma escuta ou intrusão na conversa.

Outro serviço interessante são mensagens enviadas ou acessadas de um servidor diretamente para o aparelho fixo ou móvel do usuário. Pode-se com isso acessar a ordem do dia ou a lista de ramais do Senado.

Todos os serviços existentes na rede do Senado podem ter mais praticidade com a mobilidade. Um desses serviços é a TV ao vivo disponibilizada pelo Prodasen pelo endereço http://intranet/vip. Com isso é possível visualizar todos os canais disponíveis através do celular com a utilização a rede Wi-Fi.

Um dos mais importantes serviços é a criptografia nas ligações entre aparelhos VoIP e sua mobilidade no campus do Senado. Com uma simples configuração no celular, este torna-se um ramal móvel do PABX do Senado dando mais sigilo das comunicações quando estão no ambiente IP. Todos estes serviços estão resumidos na figura 3.5.

Figura 3.7: Resumo dos serviços disponíveis em uma rede NGN

Com todas essas inovações, o Senado pode disponibilizar informações de multimídia, como TV e rádios ao vivo, documentários e diversos outros vídeos e áudios disponibilizados pela TV e Rádio Senado; disponibiliza também informações de dados como ordem do dia, agendas e diversas outras demandas além da comunicação de voz e vídeo conferência. Ao acoplar esses três principais serviços, a rede NGN torna-se TPS – *Triple Play Service*, como mostrado na Figura 3.8.

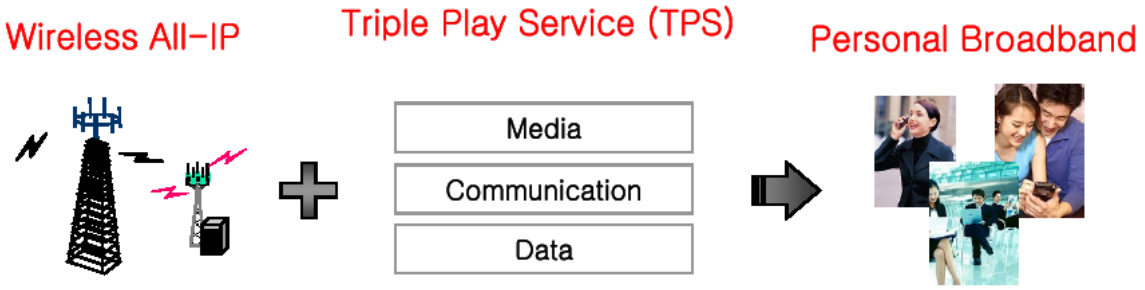

Figura 3.8: Rede NGN Triple Play

4. SEGURANÇA NA COMUNICAÇÃO

Todos os serviços mostrados anteriormente revolucionam o modo de se comunicar. Mas tudo isso será em vão se não houver disponibilidade e principalmente confiabilidade do sistema. O usuário não usará esses recursos se houver dúvida sobre sua segurança. Desde os tempos da Roma antiga, o homem deseja evitar que mensagens possam ser acessadas indevidamente. Confidencialidade, autenticação, integridade, controle de acesso e disponibilidade são serviços importantes na área de segurança. Essas propriedades são desejadas para que somente os envolvidos na comunicação tenham acesso ao conteúdo da mensagem. Isto pode ser obtido quando o transmissor cifra a mensagem e o receptor a decifra. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar a informação. A propriedade autenticação se faz necessária para que transmissor e receptor possam confirmar a identidade da outra parte envolvida.

Devido ao alto processamento usado por sistemas criptográficos assimétricos, estes são utilizados somente para a troca de uma chave usada pelos sistemas criptográficos simétricos. Nas estações móveis o tamanho das chaves deve ser reduzido devido a menor capacidade de processamento. Os sistemas criptográficos simétricos possuem a característica de serem simples de implementar e muito rápidos, porém com o problema que as partes devem compartilhar uma chave comum.

4.1. TÉCNICAS DE SEGURANÇA EM REDES SEM FIO

Informação engloba todo conteúdo capaz de ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo útil ao ser humano. Trata-se de todos os dados que se traduzem em conhecimento ou comunicação. A segurança da informação está relacionada com a proteção existente ou necessária sobre dados que possuem valor para alguém ou para uma organização. Tal segurança não está restrita a sistemas computacionais, nem a informações eletrônicas ou qualquer outra forma mecânica de armazenamento. Nesse sentido, a informação digital é um dos principais, senão o principal, produto da era atual; ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo

diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando que seja modificada ou até mesmo apagada (SOUZA; MONTALVÃO; RAMOS, 2006).

Na década de 40 o computador foi introduzido nas mais diversas esferas de administração como dispositivo auxiliar em diversos tipos de atividades, o que possibilitou uma grande evolução nos modelos computacionais e tecnologias usadas para manipular, armazenar e transmitir informações.

Verificou-se uma migração de grandes centros de processamento de dados para ambientes de computação distribuída, este fenômeno, também ocorre dentro do Senado Federal brasileiro, objeto de estudo desta monografia.

"Segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes integridade, disponibilidade, e confidencialidade" (SOUZA; MONTALVÃO; RAMOS, 2006). Tais elementos apresentam-se como os três pilares da segurança da informação e, portanto, são imprescindíveis à integridade e confiabilidade dos sistemas:

- Confidencialidade – as informações só podem ser acessadas por pessoas autorizadas pelo seu proprietário;
- Integridade – as características originais da informação, estabelecidas pelo seu proprietário, devem ser mantidas; e
- Disponibilidade – a informação deve estar sempre disponível para os usuários autorizados pelo proprietário da informação.

Deve-se considerar que no caso do Senado Federal os aspectos relacionados com a segurança da informação são de extrema importância. Há uma grande quantidade de tentativas de ataques que diariamente são empreendidas contra a rede do Senado, administrada pelo Prodasen – Secretaria Especial de Informática. Os prejuízos causados por um ataque podem ser de várias dimensões. Por exemplo, quando uma rede é atacada pode-se perder apenas tempo, ou seja, o tempo de baixar um backup, re-organizar ou re-indexar alguns dados. No entanto, pode-se perder, ou serem vazadas, informações de extrema importância, como aquelas contidas em reuniões secretas das comissões parlamentares de inquérito; neste caso, os prejuízos serão incalculáveis, pois tratam-se de assuntos de segurança nacional.

A proteção de redes sem fios abrange muitos fatores. É necessário ter-se um conhecimento razoável de todos os padrões disponíveis e o que eles têm a oferecer e, de acordo com sua aplicação, objetivo e política de segurança, implementar o nível correto.

Possuir o último padrão desenvolvido e disponível não garante que a segurança será eficiente e que este padrão será o mais seguro, tudo vai depender da configuração completa do sistema. Os principais fatores envolvidos na segurança de redes sem fio serão apresentados a seguir.

4.1.1. WEP - Wired Equivalent Privacy

O WEP é um protocolo de criptografia bastante comum que pretende impedir que intrusos consigam ler os dados transmitidos, modificar estes dados e que tenham acesso à rede sem fio. Este protocolo provê três serviços básicos citados anteriormente: confidencialidade, integridade e autenticidade.

O WEP possui uma chave secreta que compartilhada apenas com o ponto de acesso e a única forma de distribuição possível é a manual. A base da criptografia desta chave é o algoritmo RC4 que é um algoritmo de fluxo, ou seja, criptografa os dados enquanto são transmitidos.

Segundo IEEE 802.11i WG, 2004, junto à chave secreta de 40 ou 104 bits é utilizado um vetor de inicialização (IV – Initialization Vector) de 24 bits para gerar a informação criptografada. Esse IV é enviado junto à mensagem cifrada formando uma chave de 64 ou 128 bits para que o receptor possa reverter o processo de criptografia. Ele afirma ainda que o WEP utiliza CRC-32 (*Cyclic Redundance Check 32*) para calcular o *checksum* da mensagem, que é incluso no quadro, para garantir a integridade dos dados. Dessa forma, o receptor recalcula o *checksum* para garantir que a mensagem não foi alterada.

Existem dois elementos básicos que compõem a segurança do WEP: uma chave estática (que deve ser a mesma em todos os equipamentos da rede) e um componente dinâmico. Juntos, estes dois elementos irão formar a chave usada para cifrar o tráfego. O protocolo não define de que forma essa chave deve ser distribuída, portanto, esta chave deve ser cadastrada manualmente em todos os equipamentos.

Posteriormente ao estabelecimento da conexão, a chave estática sofrerá uma operação matemática, originando quatro novas chaves. Uma destas será escolhida para cifrar as informações em trânsito; essa chave será fixa e será trocada apenas se a chave estática original mudar. “Portanto, essa nova chave gerada é fixa e susceptível a ataque de

dicionário e força bruta. Pode ter tamanho de 40 a 104 bits, e o padrão ainda é 104, mas já existem várias implementações com valores maiores" (SOUZA; MONTALVÃO; RAMOS, 2006).

A fim de evitar ataques é acrescentado um conjunto de 24 bits geridos por uma função pseudoaleatória que será concatenada às chaves fixas 128 bits. O padrão de 128 bits não tem suporte em todos os produtos, mas em compensação é mais seguro. Para habilitá-lo, seria necessário que todos os componentes usados na rede dêem suporte ao padrão. Normalmente, esse procedimento é realizado pelo concentrador que, então, distribui a informação para os elementos participantes da rede.

Uma das grandes fraquezas do WEP é a falta de gerenciamento de chaves, pois não especifica como deve ser a distribuição das chaves. Por isso foi criado o WPA (Wi-Fi Protected Access) para combater as vulnerabilidades do WEP.

4.1.2. WPA – Wi-Fi Protected Access Equivalent Privacy

De acordo com IEEE 802.11i WG, 2004, o WPA, também chamado de WEP2, surgiu da necessidade em se aumentar o nível de segurança das redes sem fios e de esforços conjuntos dos membros da Wi-Fi Aliança e dos membros do IEEE, que se uniram para combater algumas vulnerabilidades do WEP. O objetivo principal deste protocolo consiste na mudança constante da chave de encriptação dificultando a invasão ou descoberta da chave.

"O protocolo WPA é compatível com o padrão de redes sem fio 802.11i e realiza melhorias na encriptação de dados e na autenticação do usuário, porém requer um *upgrade* de *software* e pode ser implantado numa rede híbrida que tenha WEP instalado" (SOUZA; MONTALVÃO; RAMOS, 2006).

Ainda de acordo com SOUZA et al. 2006, a vantagem do WPA sobre o WEP é a melhoria na criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP – *Temporal Key Integrity Protocol*) que possibilita a criação de chaves por quadro, um mecanismo de distribuição de chaves e uma função detectora de erros em um vetor de inicialização de 48 bits, ao invés de 24 bits como era no protocolo WEP. Além disso, uma outra vantagem é a melhora na autenticação de usuários. Essa autenticação se utiliza do 802.1x e do EAP (*Extensible Authentication Protocol*), que faz a autenticação de cada usuário antes de entrar na rede.

Resumidamente o WPA utiliza-se de autenticação que através do EAP faz a validação do usuário; autorização, pois assegura acesso a serviços autorizados; confidencialidade, que se torna mais eficiente na criptografia dos dados com a utilização do TKIP e integridade, na utilização do MIC (*Message Integrity Code*) que valida os usuários.

Outra vantagem do protocolo WPA é a melhoria no processo de autenticação de usuários. “Essa autenticação se utiliza do 802.11x e do EAP (Extensible Authentication Protocol), que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso a rede. A autenticação com WPA é uma combinação de sistema aberto e autenticação 802.1x que utiliza duas fases: a primeira utiliza a autenticação de sistema aberto e indica ao usuário da rede sem fio que ele pode enviar quadros para o ponto de acesso sem fio e a segunda fase utiliza o 802.1x para realizar a autenticação do usuário” (SOUZA; MONTALVÃO; RAMOS, 2006).

Conforme salienta o estudo de SOUZA et al. 2006, em ambientes domésticos, onde não existe um servidor de autenticação (servidor RADIUS – *Remote Authentication Dial-In User Service*), o WPA provê um outro método de autenticação chamado PSK (*Pre-Shared Key*), que permite que o usuário digite chaves e senhas manualmente.

No WEP a integridade dos dados é garantida com um ICV (*Integrity Check Value*) de 32 bits, já no WPA existe um método conhecido como Michel que especifica um novo algoritmo, calculando um MIC (código de integridade da mensagem) e anexando-o ao ICV.

4.1.3. Endereço MAC (Media Access Control)

O MAC é o endereço físico atribuído pelo fabricante do hardware à sua placa de rede. Esse endereço é programado em um chip na placa com numeração única no mundo. Como o endereço MAC está localizado na placa de rede, se esta for substituída em um computador, o endereço físico acompanhará o MAC para o novo endereço. Este endereço MAC possui tamanho de 48 bits, expressos com doze dígitos hexadecimais. Os primeiros seis dígitos são administrados pelo consórcio IEEE e identificam o fabricante ou fornecedor da placa de rede e os seis últimos identificam a placa do equipamento. Os endereços MAC geralmente são gravados na memória ROM e copiados para a memória RAM quando a placa de rede é iniciada.

Uma das formas encontradas para restringir o acesso a uma determinada rede sem fio é mediante o cadastramento prévio dos dispositivos participantes. Nos casos dos celulares, existe o endereço MAC do Wi-Fi que é cadastrado da mesma forma. Como o endereço MAC identifica cada interface de rede, apenas os dispositivos cadastrados de antemão terão acesso permitido. Esse mecanismo exigirá sempre alguma manutenção, que será maior ou menor, de acordo com o fluxo de usuários e interfaces que entram e saem do cadastro, porém não deixa de ser uma boa solução para pequenas redes e ambientes com poucas mudanças. Mas é importante lembrar que esse tipo de autenticação pode, no melhor dos casos, identificar o equipamento e não o usuário. Particularmente, isso é importante em computadores compartilhados ou vulneráveis a acessos não autorizados, quer sejam acessos físicos, quer remotos (IEEE 802.11i WG, 2004).

4.1.4. VPN - Virtual Private Network

A VPN (Rede Privada Virtual) é uma rede com acesso privativo que utiliza uma técnica chamada de tunelamento, na qual pacotes são transmitidos na rede compartilhada em um túnel privado que simula uma conexão ponto-a-ponto, que por sua vez simula um enlace dedicado.

“Esta tecnologia possibilita que o tráfego de várias redes navegue via diferentes túneis sobre a mesma infra-estrutura. Permite que diferentes protocolos de rede se comuniquem através de uma infra-estrutura incompatível e também possibilita diferenciar o tráfego de várias fontes, permitindo distintas rotas de destino e qualidade de serviço. A característica mais importante para as redes sem fio é o fato de uma VPN criar canais privados de comunicação, onde os dados viajam criptografados, aumentando consideravelmente a segurança dos dados. Uma VPN provê uma conexão segura através de um conjunto de três serviços:

• Autenticação: implementada através de senhas e identificação dos usuários, estabelece a identificação do remetente e do receptor da informação;

• Encriptação: Implementada através de algoritmo de criptografia aplicado sobre a mensagem de texto aumentando a dificuldade para decriptografá-la;

• Encapsulamento: a mensagem criptografada é encapsulada pela VPN em pacotes com o seu próprio endereço como origem. Este processo é conhecido também como tunelamento” (SOUZA; MONTALVÃO; RAMOS, 2006).

Por fim, uma das grandes vantagens das Redes Privadas Virtuais é que elas tendem a apresentar custos muito menores de implementação do que aqueles obtidos com as Redes Privadas, conectando redes externas à rede do Senado. Um exemplo é a utilização da VPN entre um computador na rede regional do parlamentar e conectar-se diretamente ao Gabinete no Senado que pode transferir documentos sigilosos e ter conversas protegidas contra escutas indesejadas.

4.2. Vulnerabilidades em redes sem fio

Nos tópicos subsequentes serão abordadas as principais vulnerabilidades que as redes sem fio podem sofrer.

4.2.1. Vulnerabilidade no WEP

O WEP apresenta vulnerabilidades no vetor de inicialização (IV). Como as chaves de encriptação são utilizadas por longo período de tempo, recomenda-se que o vetor de inicialização seja alterado a cada quadro enviado. No geral, este vetor inicia em 0 e vai sendo acrescido em 1 a cada nova utilização.

“Dois problemas podem ser verificados nesse sistema: Um deles reside no fato de que em algum momento o vetor de inicialização (IV) se repetirá e sendo uma cadeia cíclica, o tráfego poderá ser facilmente monitorado. O outro problema está na freqüente remoção e reinserção dos dispositivos de rede sem fio, retornando a contagem do vetor de inicialização à 0, fazendo com que os quadros com valores baixos de IV sejam comuns.

Grande parte dos problemas do protocolo WEP vinculam-se ao fato de que o padrão foi definido em uma época em que havia restrições dos Estados Unidos referentes à exportação de criptografia com chaves maiores que 40 bits. Hoje, alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algum tempo. Outra grande vulnerabilidade do protocolo WEP é quanto ao método de criptografia que utiliza o RC4. O RC4 é simétrico, ou seja, a mesma chave utilizada para a criptografia também é utilizada para a decriptografia” (SOUZA; MONTALVÃO; RAMOS, 2006).

Teoricamente, conhecer o vetor sem conhecer a chave é inútil, porém existem situações que, na prática, contradizem essa afirmação. Em consonância com SOUZA, op.

cit., devido ao pequeno tamanho do vetor, este se repete várias vezes durante um dia de tráfego, pois com 24 bits são possíveis 16.777.216 valores diferentes. Como uma rede com tráfego intenso transmite em torno de 600 a 700 pacotes, mesmo que todos os valores sejam usados sem repetição, o mesmo valor será utilizado novamente ao final de 7 horas, assim um atacante poderá observar passivamente o tráfego e identificar quando o mesmo valor será usado novamente. Essa reutilização do vetor irá, em algum momento, revelar a chave (os outros 104 bits), pois alguns pacotes têm conteúdo previsível, como "username", "login", "password", vários espaços em branco em mensagens de e-mail, etc.

Ataques completamente passivos podem não obter um padrão de pacote que permita descobrir a chave, então o atacante poderá atuar de forma mais ativa e forçar uma resposta conhecida enviando, por exemplo, um ping para algum equipamento da rede-alvo. Devido ao pacote ICMP de resposta ter seu conteúdo conhecido, nesse momento a chave será revelada. Essa descoberta é possível por meio de uma simples operação matemática, conhecida como XOR, que diz que de posse de três informações complementares é possível deduzir a quarta. Neste caso são conhecidos a mensagem cifrada, a chave cifrada e o pacote em claro, portanto por uma operação de regra de 3 pode se chegar à informação desejada: a chave em claro.

Para piorar este cenário, algumas implementações utilizam a mesma seqüência de vetores desde o momento em que o equipamento é ligado, facilitando ainda mais a descoberta do segredo. Outro problema com o WEP relaciona-se à forma de armazenamento das chaves no cliente. Como o protocolo não define nenhum método para cifragem na guarda da chave, esta é armazenada de forma legível, o que torna um ambiente com chaves de melhor qualidade mais difícil de ser quebrado, vulnerável caso um cliente que compõe a rede seja comprometido (SOUZA; MONTALVÃO; RAMOS, 2006).

4.2.2. Vulnerabilidade no WPA

Criado para sanar as vulnerabilidades do protocolo WEP, apresenta algumas falhas que devem ser conhecidas para evitar possíveis problemas. No entanto, não há muitas ferramentas disponíveis que promovam ataques ao WPA.

A maior vulnerabilidade é caracterizada pela atitude do usuário ao registrar senhas de pequena extensão e fáceis de serem identificadas, este comportamento inadequado pode deixar a rede sujeita a ataques.

No caso do WPA, senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque. Comumente fabricantes cadastram senhas pequenas (de 8 a 10 dígitos) imaginando que o administrador irá modificá-las quando colocar o equipamento em atividade, porém isso não ocorre na prática, o que torna redes com WPA tão ou mais vulneráveis do que aquelas que utilizam WEP.

4.2.3. Vulnerabilidades Físicas

A segurança das redes Wi-Fi deve abordar também a parte física dos equipamentos. Diferentemente das redes cabeadas, nas redes sem fio esse aspecto é muito mais relevante, visto que a área de abrangência aumenta substancialmente, pois podem ser acessadas em ambientes externos do Campus do Senado. Muitos pontos, antes nas redes cabeadas, que eram irrelevantes devem ser cuidadosamente tratados nas redes sem fios como, por exemplo, o posicionamento dos *hardwares* utilizados e principalmente dos *Access Points* localizados nos estacionamentos e áreas públicas.

O acesso aos equipamentos, que há algum tempo, era estabelecido e controlado exclusivamente via portaria e/ou recepção, ou mesmo a necessidade de obter um ponto de rede cabeada, ou acesso a um computador da rede, agora devem ser pensados em termos de dezenas ou centenas de metros ao redor do ambiente do Senado. Aspectos antes irrelevantes (sob o ponto de vista de performance e segurança), como posicionamento de determinados componentes de rede, agora devem ser cuidadosamente estudados, sob o risco de comprometer o bom funcionamento da rede e, principalmente, facilitar o acesso não autorizado e outros tipos de ataques. (SOUZA; MONTALVÃO; RAMOS, 2006). É importante lembrar que na avaliação da rede sem fio deve-se considerar o alcance atingido pelo padrão a ser adotado e a potência dos equipamentos que serão utilizados. Pois em geral, concentradores têm potência de 15 dbm - alguns equipamentos atualmente chegam a 42 dbm - e a maioria dos concentradores permite selecionar valores intermediários, caso o administrador ache conveniente, em função da área efetiva a ser coberta por um determinado equipamento;

As vulnerabilidades físicas incluem aquelas configurações onde o administrador mantém as mesmas configurações cadastradas pelo fabricante. Alguns equipamentos que são fornecidos para a implantação de uma rede, muitas vezes, possuem ferramentas de segurança, mas nem sempre estas ferramentas já vêm habilitadas de fábrica. E mesmo que

elas já venham habilitadas, podem ser alteradas por terceiros que possuam conhecimento dessas configurações originais. Este fato faz com que os administradores com pouca experiência em redes sem fio coloquem os equipamentos em produção sem qualquer alteração nas configurações de fábrica, pois praticamente todos os equipamentos saem de fabrica com senhas de administração e endereço IP padrão.

Mesmo gerentes de TI com grande experiência em redes cabeadas vêm encontrando dificuldades em configurar de forma segura seu ambiente Wi-Fi. Por mais semelhanças que existam entre proteção de serviços, sistemas, aplicações e atualizações, há vários outros pontos que são novidade absoluta e, portanto, necessitam de tempo e disposição para resolver as novas questões de segurança em ambientes de rede sem fio. Se os dispositivos da rede sem fio forem mal configurados, há uma grade possibilidade de se associar a outro dispositivo, sem consentimento ou mesmo conhecimento do usuário, fenômeno conhecido como *Associação Acidental*.

4.3. Técnicas de ataques a redes sem fio

Para garantir a segurança em uma rede, é preciso conhecer os tipos de ataque que ela pode sofrer. Para evitar intromissão existem os tipos de interrupção e intersecção. O primeiro é o tipo de ataque em que o intruso interrompe o fluxo dos dados para que os mesmos não cheguem ao seu destino. Já o segundo ocorre quando o intruso captura o tráfego da rede. Esse procedimento consiste em colocar um terceiro computador entre dois computadores que se comunicam via rede. Em seguida, o computador intermediário se faz passar por um dos computadores originais e obtenha uma conexão funcional com os computadores originais, o que torna possível ler ou modificar mensagens trocadas entre os computadores originais, enquanto os usuários desses computadores crêem estar comunicando entre si.

4.3.1. Negação de serviço (*DoS)*

Diferentemente da maioria dos ataques em redes IP, um ataque de negação de serviço não visa invadir um computador para extrair informações confidenciais, como números de cartões de crédito e senhas bancárias, e nem para modificar o conteúdo armazenado em

computadores. Tais ataques têm como objetivo tornar inacessíveis os serviços providos na rede.

"Para as redes Wi-Fi, que utilizam a freqüência *ISM*, na faixa de 2,4 GHz, existe um mecanismo relativamente simples de se prover um ataque do tipo *DoS*, trata-se de ligar um aparelho qualquer que trabalhe na mesma faixa de freqüência daquela da rede. Aparelhos domésticos como telefones celulares, forno de microondas, telefones sem-fio e aparelhos de monitoramento infantil trabalham nesta faixa de frequência e podem ser utilizados para provocar *DoS* em uma rede" (SOUZA; MONTALVÃO; RAMOS, 2006).

Há também outra possibilidade de ataque: quando o atacante se faz passar pelo ponto de acesso utilizando-se do mesmo ESSID e endereço MAC do ponto de acesso da rede e a inunda com solicitações de dissociação. Tais pedidos obrigam os *hosts* a se desassociarem e se re-associarem à rede. Se estas dissociações forem realizadas em intervalos curtos de tempo, teremos um DoS, pois os clientes não conseguirão permanecer conectados por muito tempo.

Outra maneira de causar uma negação de serviço é inundar a rede com tráfego aleatório. Os ataques de DoS podem ocorrer sem que haja intenção maliciosa com redes vizinhas, já que, geralmente, cada fabricante utiliza o mesmo canal *default* para os seus equipamentos. Assim, uma rede pode interferir na outra, mesmo de forma não intencional (SOUZA; MONTALVÃO; RAMOS, 2006).

4.3.2. Acesso não autorizado

O objetivo é criar um ponto de acesso com sinal mais forte que os demais pontos da rede, tendo prioridade na conexão e tornando-se uma rede de captura de senhas ou ESSDI.

4.3.3. Mac spoffing

O objetivo principal é a troca do endereço físico não autorizado por um cadastrado no sistema. Desta maneira, qualquer atacante mal intencionado pode capturar, através de técnicas de Eavesdrooping & Espionage, um endereço MAC válido de um cliente, efetuar a troca de seu próprio endereço pelo do cliente e utilizar a rede como um usuário autorizado.

Uma das formas de se gerenciar o acesso a uma rede sem fio é mantendo uma lista com todos os endereços MAC das máquinas que terão permissão de acesso.

"Os ataques que forjam um endereço MAC podem ter diversos objetivos, dentre eles o de ocultar a presença do atacante na rede. Em virtude de a maioria dos detectores de ataque (IDS) não examinarem as camadas mais baixas do protocolo TCP/IP (normalmente analisa-se até a camada 3), o atacante pode utilizar-se de um ataque de força bruta, mudando sucessivamente o endereço MAC, buscando encontrar um que esteja autorizado no controle de acesso do concentrador e que por conseqüência, permita o acesso. Desta maneira, o atacante pode construir uma lista de endereços MAC válidos para uma determinada rede, utiliza de acordo com a sua conveniência e disponibilidade, por exemplo, endereços pouco utilizados para evitar choque com usuários legítimos" (SOUZA; MONTALVÃO; RAMOS, 2006).

4.3.4. Associação maliciosa

A associação maliciosa configura-se quando o atacante se faz passar por um ponto de acesso, assim os membros da rede irão enganar-se acreditando estarem conectados à rede real. A falha no sistema que possibilita a associação maliciosa é a má identificação do ponto de acesso.

Uma das ferramentas mais utilizadas para a associação maliciosa é o FakeAp, que possui características que podem levar o cliente a crer que está conectado ao ponto de acesso correto. Dentre algumas características do FakeAp destacam-se a recepção de conexões em um canal específico, a utilização de um ESSID específico, a utilização de um endereço MAC específico ou o padrão de um determinado fabricante, a utilização de uma chave WEP determinada pelo usuário e o FakeAp permite ainda a configuração manual da potência de saída.

4.3.5. Wardriving

Difundida principalmente entre os hackers dos Estados Unidos e Europa, e mais recentemente no Brasil. Esta técnica consiste em se dirigir um veículo à procura de redes sem fio abertas, as quais estejam passíveis de serem invadidas.

Através do uso de um *laptop* ou outro equipamento Wi-Fi e alguma antena, geralmente caseira, que pode ser posicionada dentro ou fora do veículo o processo de captação da rede passa a ser mais simples. Esta técnica procura identificar vulnerabilidade nos protocolos, ou em redes de empresas que não utilizem nenhum tipo de criptografia. Quando são descobertas falhas na rede consegue-se estabelecer a conexão. Alguns ataques são realizados por vândalos que picham os muros próximos à localização da rede e descrevem seu status como mostrado na Figura 4.1.

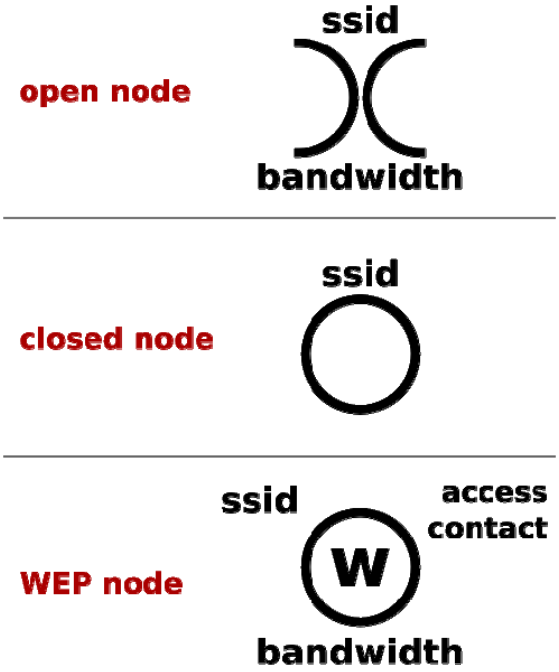

Figura 4.1 – Símbolos empregados no Warchalking**.**

“A propagação deste tipo de simbologia é conhecida como *Warchalking* , que é uma forma de comunicação inventado nos Estados Unidos, há aproximadamente 70 anos. O warchalking era uma forma de comunicação por andarilhos desempregados chamados de Hobos. Através de símbolos próprios os Hobos conseguiam se comunicar, informando, por exemplo, se em determinada residência havia um médico que não cobraria por uma consulta ou a existência de um lugar seguro para se fazer uma refeição.

Um par de semicírculos opostos em forma de "X", significa um "open node" ou, simplesmente, um link aberto. Um círculo fechado significa um "closed node". Um círculo com um "W" significa que a conexão está protegida por chave WEP ou WPA, geralmente indicada no canto superior direito. Abaixo do símbolo deve estar a velocidade do node. O SSID ou nome do hotspot deve ficar no topo da figura” (SOUZA; MONTALVÃO; RAMOS, 2006).

4.4. Técnicas de criptografia nos aparelhos IP

A criptografia ponto a ponto vem incrementar a proteção às redes sem fio, dificultando ainda mais a ação de intrusos na rede.

4.4.1. Criptografia Simétrica

Na criptografia simétrica a voz transmitida é cifrada através de um algoritmo criptográfico conhecido e público usando uma chave K secreta, e depois decifrada com um algoritmo de decifragem usando-se a mesma chave secreta K enviada anteriormente pelo equipamento que originou a ligação, como mostra a Figura 4.2. Exemplos deste tipo de algoritmo são o DES (Data Encryption Standart) e o AES (Advanced Encryption Standart). Apesar do grande sucesso do DES, sua chave de 56bits tornou-se pequena para o poder computacional dos dias de hoje. Para se ter uma idéia, em 1997, no DES Challenge a quebra do DES foi alcançada em um esforço coletivo em menos de 4 meses; em 1999, no DES Challenge III, o vencedor conseguiu descobrir a chave em pouco mais de 22 horas (ASHIDANI e BARBAR, 2008)[1].

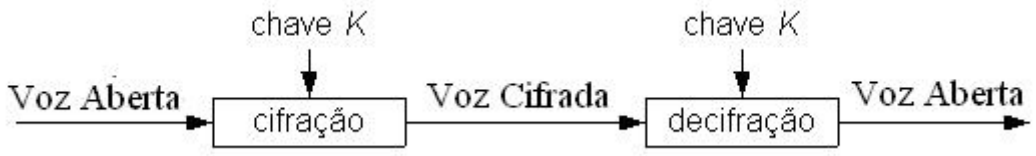

Figura 4.2: Criptografia simétrica

“Diante destes fatos o AES foi apresentado e ele pode trabalhar com chaves de 128, 192 e 256 bits e seu algoritmo processa os dados em blocos de 128bits. Para se ter uma idéia da força do AES, estima-se que uma máquina que pudesse através de força bruta quebrar o DES de 56 bits em 1ms , levaria 149 bilhões de anos para quebrar o AES com uma chave de 128 bits” (ASHIDANI e BARBAR, 2008)

“O AES baseia-se em uma rede de substituições e permutações sendo simples, consumindo pouca memória e apresentando desempenho rápido tanto em implementações de software e hardware. atualmente adotado pelo governo dos EUA para proteção das transmissões de dados normais (chave de 128 bits), classificados e altamente classificados (chaves de 192 e 256 bits)” (ASHIDANI e BARBAR, 2008).

Para que duas partes possam compartilhar a mesma chave, que pode ser capturada ao utilizar um canal inseguro ou o uso de chaves pequenas, utiliza-se a criptografia assimétrica para troca de chaves.

4.4.2. Criptografia Assimétrica

A criptografia assimétrica ou criptografia de chaves públicas, recebe esse nome porque o receptor dos dados possui uma chave pública (K_U) que é utilizada para cifrar dados usando um algoritmo predeterminado e somente o receptor possui a chave privada (K_R) capaz de decifrar a mensagem cifrada pelo transmissor dos dados. Como a chave de cifrar diferente da chave de decifrar dizemos que um sistema criptográfico assimétrico, mostrado na Figura 4.3.

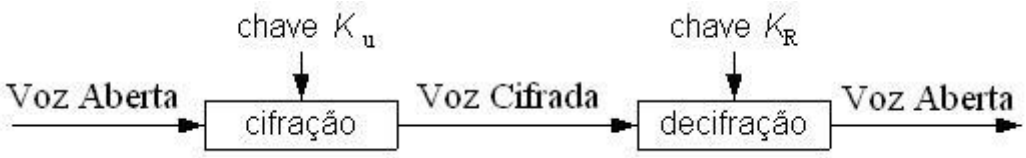

Figura 4.2: Criptografia assimétrica

A vantagem deste sistema é que uma das chaves pode ser divulgada livremente sem a necessidade de um canal seguro, diferentemente do sistema simétrico onde a chave secreta K deve ser compartilhada por ambos os lados participantes da comunicação.

4.4.3. Sistema Criptográfico RSA

O sistema criptográfico RSA, denominado com as iniciais dos inventores do sistema, Rivest, Shamir e Adleman funciona com base no fato de não se conhecer algoritmo capaz de fatorar rapidamente um número muito grande que faça parte da chave pública $K_U(n; e)$ em números primos p; q tal que $n = p \times q$ (RIVEST, SHAMIR E ADLEMAN,1978).

4.4.4. Criptografia de VoIP com Curvas Elípticas

A Criptografía de Curvas Elípticas - ECC é uma variante da criptografia assimétrica, baseada na matemática das curvas elípticas. A utilização de curvas elípticas em criptografia foi proposta de modo independente por Neal Koblitz e Victor Miller em 1985. Seus criadores argumentam que a ECC pode ser mais rápida e usar chaves mais curtas do que os métodos antigos, como RSA, e proporcionar ao mesmo tempo um nível de segurança equivalente. Este método é ideal para o tráfego de dados VoIP, por ser uma transmissão multimídia interativa, geralmente utiliza dispositivos de baixo processamento como os telefones, possuem características como a tolerância à perda de informação e baixa tolerância a atrasos.

"A voz possui muita informação redundante e intervalos vazios, portanto a perda de pequenos pedaços da conversa, não afeta o recebimento do conteúdo da mensagem, porém em uma conversa com interatividade entre as partes, atrasos excessivos podem tornar a experiência extremamente desagradável aos participantes. Para garantir a confidencialidade dos dados multimídias, deve-se criptografá-los, porém este processo não pode introduzir uma latência acima de 100ms, para que atraso total fique em um patamar tolerável abaixo dos 400ms" (ASHIDANI e BARBAR, 2008).

De acordo com os autores supracitados, o uso de um sistema criptográfico de chaves públicas para a cifragem dos dados, introduz um custo computacional elevado, devido aos cálculos matemáticos envolvidos no processo de cifragem e decifragem. A opção do uso de um sistema criptográfico simétrico torna-se a mais adequada. O tradicional DES, devido a sua chave pequena para os padrões computacionais atuais, não fornece segurança suficiente. O 3DES é mais lento que um sistema projetado para usar chaves criptográficas maiores que a do DES. Escolhe-se portanto, o AES como sistema de criptografia simétrica.

Conforme o estudo de ASHIDANI e BARBAR, os sistemas criptográficos simétricos transmitem uma grande quantidade de dados e estes dados são divididos em blocos, portanto existe a possibilidade de blocos repetidos, e uma análise de frequência dos blocos repetidos constitui uma ameaça à segurança dos dados. Para combater este problema, os sistemas criptográficos simétricos utilizam o encadeamento de blocos.

Devido às características de tolerância a perdas nas transmissões multimídia, as transmissões VoIP utilizam o protocolo UDP (User Datagram Protocol) que é um protocolo não confiável. Neste tipo de transmissão a perda de um bloco é aceitável pela aplicação, mas é inaceitável pelo sistema criptográfico. Uma vez que a decifragem de um

bloco depende dos dados do bloco recebido e decifrado anteriormente, a perda de um bloco causaria a impossibilidade de decifrar todos os blocos restantes da cadeia.

Entretanto há ainda o problema de compartilhar uma única chave entre os dois lados participantes da comunicação, que deve ser resolvido usando-se um sistema criptográfico de chaves públicas.

Em função da evolução do poder de processamento dos equipamentos e do avanço nos estudos sobre o RSA, o tamanho da chave aumentou significativamente ocasionando um alto processamento de aplicações que usam o RSA. Os sistemas criptográficos baseados em curvas elípticas têm chamado a atenção e parecem desafiar a supremacia do RSA. A figura 3 mostra uma comparação entre o tamanho da chave de um sistema criptográfico simétrico, curvas elípticas e o RSA (ASHIDANI e BARBAR, 2008). Observa-se que o ECC oferece um nível equivalente de segurança, porém com uma chave muito menor o que torna viável na utilização em celulares.

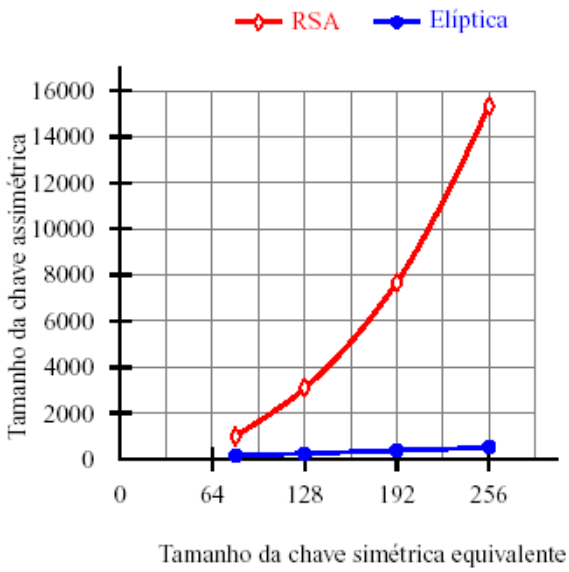

Figura 4.4: Comparação entre o tamanho das chaves simétricas, RSA e Elíptica

4.5. Segurança nas telecomunicações do Senado Federal

Os Órgãos Federais, inclusive o Senado Federal, podem tirar grande vantagem na utilização de aparelhos portáteis para fomentar seus membros com informações que, de outra forma, somente poderiam ser obtidas através de meios estáticos, o que demandaria tempo para tal aquisição. A mobilidade dentro de um ambiente como o Senado Federal é

imprescindível na medida em que os parlamentares poderão receber informação em tempo real e, desta forma, antecipar a tomada de decisões em situações urgentes. Como exemplo basta verificar o uso frequente de aparelhos celulares durante as reuniões. O mais importante é que toda essa agilidade virá acompanhada da segurança nas comunicações. Com a implantação da rede NGN toda essa comunicação passa a ser criptografada, sem que a operadora ou qualquer intruso tenha acesso às informações.

Recentemente foram divulgadas conversas do Senador José Sarney com seu filho e sua neta, de caráter extremamente sigiloso e delicado em que houve vazamento desta sequência de diálogos de dentro da Polícia Federal (Jornal ESTADÃO, 22 jul 2009).

Esse tipo de episódio já ocorreu envolvendo o Senador Demóstenes Torres e o Presidente do Supremo Tribunal Federal, Gilmar Mendes conforme reportagem publicada pelo jornal O Globo em 1 de setembro de 2008. Diante do ocorrido, todo o sistema de telecomunicações do Senado Federal e das operadoras foi questionado no que tange a sua segurança. A Polícia Federal fez uma investigação na Central Telefônica do Senado e concluiu que as escutas partiram das operadoras. Em paralelo foi questionado o critério dos juízes para a liberação de escutas de uma forma geral e se as escutas realmente foram feitas a partir de mandado judicial. Foi descoberta uma quadrilha que envolvia funcionários das operadoras que vendiam as escutas tornando a interceptação e o vazamento de informações ainda mais fácil para pessoas mal intencionadas.

Diante desse cenário de insegurança nas comunicações e devido aos assuntos de segurança nacional que a Casa Legislativa se ocupa necessária se faz, com urgência, a mudança de paradigma na comunicação. A segurança pode ser aumentada através do uso de criptografias, VPNs e através da implantação da rede NGN.

4.6. Comparação entre as tecnologias

A reformulação da política de segurança das comunicações móveis é imprescindível, pois a tecnologia atual encontra-se muito defasada se comparada às possibilidades de segurança e recursos da nova rede.

Apesar da tecnologia existente não ter nenhum registro de ataque dentro do campus do Senado Federal, é importante antecipar possíveis invasões criando protocolos de segurança mais rigorosos e atualizar o parque tecnológico. A tecnologia Digital existente dificulta os ataques em relação à Analógica, mas não possibilita a inserção de criptografia e VPN entre os usuários, o que aumenta a vulnerabilidade do sistema. Outro problema da

tecnologia existente é a obrigatoriedade do uso dos aparelhos da mesma marca do fornecedor do PABX, o que impossibilita a livre concorrência durante o processo de compra dos equipamentos. Já os equipamentos VoIP seguem a mesma padronização dos protocolos, o que favorece a participação de diversos fornecedores no processo licitatório.

A grande vantagem da rede NGN está na segurança da comunicação, onde toda conversa dentro do campus do Senado é criptografada. Além disso, ligações externas ao Senado, usando a tecnologia IP, também poderão ser criptografadas, dando maior abrangência na segurança.

Estão sendo implantadas no mundo duas tecnologias de maior alcance e mobilidade à rede IP, que são o WiMAX e o LTE. Essas técnicas são muito parecidas com o Wi-Fi, usando antenas MIMO e portadoras OFDMA, mas são padrões de ambientes externos. Com a implantação destas tecnologias no Brasil, a segurança, que se limitava ao campus do Senado e a alguns acessos via VPN, passa a abranger todos os locais que estas alcançarem. Com isso a operadora que controla as ligações de terminais móveis passará a ser a própria Secretaria de Telecomunicações do Senado Federal – STELE, impossibilitando interceptações e escutas por pessoas indesejadas.

5. CONCLUSÃO

A segurança é um requisito indispensável em qualquer rede de telecomunicações e torna-se mais importante dentro de uma Casa Legislativa onde há assuntos de segurança nacional. Atualmente a telefonia móvel celular e fixa não tem garantia de sigilo, pois existem muitas pessoas com acesso às informações nas operadoras. A rede IP do Senado já possui importantes e eficientes protocolos de segurança e podem ser usados na telefonia com a implantação de uma rede de próxima geração NGN. O uso do VoIP dentro da rede já existente torna possível a telefonia com criptografia e criam-se serviços até então não existentes. A tendência mundial é o uso destas redes de convergência tecnológica que proporcionam, além da segurança exigida, outros serviços como videoconferência e VoIP criptografado com mobilidade até então inéditos nas telefonias convencionais.

Em suma, a implantação da rede NGN no campus do Senado Federal, proporcionará aos parlamentares e usuários a segurança necessária de uma Casa Legislativa, evitando escutas indesejadas, como ocorre atualmente.

5.1. Proposta de Trabalhos futuros

Como proposta de estudo para trabalhos futuros, recomenda-se incluir uma especificação da rede NGN, com seus custos correspondentes e a economia gerada após sua implantação seguindo as resoluções da ANATEL que regularizam esse segmento de telecomunicação como especificado na resolução 272/2001. Outro importante aspecto a ser abordado é a interligação da rede NGN com tecnologias IP sem fio, WiMAX e LTE, que estão em fase de liberação das licenças pela ANATEL. Esse estudo comparativo pode auxiliar na redução de custo de projetos, principalmente em redes implantadas em nível nacional, desvinculando o PABX do Senado das operadoras de telefonia móveis já existentes.

Referência Bibliográfica

[1] ASHIDANI, P.J., BARBAR, J.S. (2008). *Criptografia para Voz sobre IP com Curvas Elípticas*. Dissertação de Mestrado, Departamento de Ciências da Computação, Universidade Federal de Uberlândia, Uberlândia-MG.

[2] ELIASSON, E. (2006). *Secure internet telephony: design, implementation and performance measurements. Licenciate of technology degree, Telecommunication Systems Laboratory Eletronic*. Royal Institute of Technology Stockholm.

[3] GUPTA, V., GUPTA, S., CHANG, S., and STEBILA, D. (2002). *Performance analysis of elliptic curve cryptography for SSL*. In: WiSE'02: Proceedings of the 1st ACM workshop on Wireless security, pages 87–94, New York, NY, USA. ACM.

[4] HANKERSON, D., MENEZES, A., and VANSTONE, S. (2004). *Guide to Elliptic Curve Cryptography*. Springer, 1st edition.

[5] IEEE (2004). *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*. IEEE Standard, 801.16.

[6] IEEE 802.11i WG, (2004). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements*. IEEE Computer Society.

[7] INTRANET DO SENADO FEDERAL, informações sobre a Secretaria de Telecomunicações. Disponível em <http://www.senado.gov.br>. Acesso em 10 de jun. de 2009.

[8] Jornal O GLOBO; *Diálogo grampeado entre Gilmar Mendes e Demóstenes Torres*. Disponível em: <http://oglobo.globo.com/pais/mat/2008/09/01>. Acesso em 07 jul. 2009.

[9] Jornal ESTADÃO; *Gravação liga Sarney a atos secretos*. Disponível em: <http://www.estadao.com.br>. Acesso em 22 jul. 2009.

[10] KUROSE, J. F. and ROSS, K. W. (2006). *Redes de Computadores e a Internet: uma abordagem Top-Down*. 3rd edition Pearson/Prentice-Hall. 2006.

[11] MOURA, F. A. L. de A. (2009). *Estimativa do número de estações rádio base para a implantação do wimax no Distrito Federal*. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM - 379/09, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 67 p.

[12] NASSIF, ANTÔNIO TEÓFILO (2004). *Redes da Próxima Geração: Aspectos Econômicos, Técnicos e Cenários de Migração*. Dissertação de Mestrado. Publicação 2004, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 164 p.

[13] Periódico do Senado Federal EM PAUTA; *O processo legislativo do Senado a serviço da cidadania*. N. 10, 21 a 25 mai. 2007. Biblioteca Digital do Senado Federal. Disponível em: < http://www2.senado.gov.br/bdsf/item/id/101976>. Acesso em 26 jun. 2009.

[14] RIVEST, R. L., SHAMIR, A., AND ADLEMAN, L. (1978). *A method for obtaining digital signatures and public-key cryptosystems*. Technical Report 2.

[15] SEM BRASIL, notícias sobre o mercado de telecomunicações. Disponível em: <http://www.sembrasil.com.br/noticias>. Acesso em 15 de jun. de 2009.

[16] SIEMENS LTDA COMUNICAÇÃO CORPORATIVA (2006). NGN: Em busca do retorno desejado. Disponível em: <http://www.siemens.com.br/coluna1.asp?canal =3822> . Acesso em 15 mai. 2009

[17] SOUZA, A.M., MONTALVÃO, L.G., RAMOS, K.M (2006). E*studo de um ambiente seguro para distribuição de áudio e vídeo, via rede sem fio, no Senado Federal*. Monografia de Especialização, Publicação UNB.LABREDES. MFE.014/2006, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília , DF, 69p.

[18] STALLINGS, W. (1999). *Cryptography and network security (2nd ed.): principles and practice*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2nd edition.