UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

LUIZ CESAR GAWLIK

COMUNICAÇÃO ENTRE EQUIPAMENTOS UTILIZANDO TECNOLOGIA 3G

MONOGRAFIA

CURITIBA
2011

LUIZ CESAR GAWLIK

COMUNICAÇÃO ENTRE EQUIPAMENTOS UTILIZANDO TECNOLOGIA 3G

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná
Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA
2011

AGRADECIMENTOS

A todos que direta ou indiretamente, contribuíram para a realização deste trabalho.

A Deus, agradeço pela iluminação em todos os momentos.

Meu especial agradecimento a minha família, que desde sempre é minha principal fonte de inspiração e apoio.

De forma indiscriminada, quero registrar também meus sinceros agradecimentos a todos os professores do I Curso de Especialização em Gerenciamento de Servidores, pois ensinar é um desafio, que faz tanto aluno quanto professor evoluir um pouco mais a cada dia. Seria imperdoável, também, esquecer de agradecer em especial o professor Prof. Dr. Kleber Kendy Horikawa Nabas, que leu e criticou, construtivamente, os capítulos que compõe essa pequena dissertação.

RESUMO

Gawlik, Luiz Cesar. **Estudo referente a comunicação entre equipamentos com tecnologia 3G**. 2011. 37 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

No momento atual define-se a tecnologia de terceira geração celular (3G) que possibilita acesso os dados com alta velocidade e permite a explosão comercial de telemetria celular. Algumas funcionalidades do celular já estão disponíveis nas tecnologias de transição, o projeto tem por finalidade comprovar a viabilidade técnica de desenvolvimento em um modo celular, para a comunicação de máquinas a partir de equipamentos com tecnologia e suporte 3G, utilizando-se de um pacote de dados que permite tráfego pesado de informações, o objetivo de implantar a tecnologia é reduzir radicalmente custos de implantação de infra-estrutura e ainda pode oferecer acesso com a rápida instalação até mesmo em locais de difícil acesso, com a disponibilidade de tecnologia de comunicação de dados, utiliza-se equipamentos que interpretam e desenvolvem um controle de gestão remota das máquinas, permitindo que todo o controle seja operado apenas pelos equipamentos, sem a intervenção humana, tudo de forma programada e automática.

Palavras-chaves: Comunicação M2M. Telemetria. Tecnologia de terceira geração.

ABSTRACT

At the moment defines the third generation cellular technology (3G) that allows access to data with high speed and allows the explosion of commercial cellular telemetry. Some features of mobile technologies are already available in the transition. The project aims to demonstrate the technical feasibility of development in a cellular mode, for communicating machines from equipment and support 3G technology, using a data package that allows heavy traffic information. With the evolution of technology (3G) facilitates the installation of equipment and even places of difficult access to infrastructure by cables or even other media of high cost. The goal of deploying the technology is radically reduce deployment costs, infrastructure and can still provide access to the quick installation even in hard to reach places. With the availability of data communication technology, it uses equipment that interpret and develop a management control of remote machines, allowing all the control is operated solely by the equipment without human intervention, all in a scheduled and automatic.

Keywords: M2M Communication. Telemetry. third generation technology.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A idéia de utilizar uma rede pública como a Internet em vez de linhas privativas para implantar redes corporativas é denominada de *Virtual Private Network* (VPN) ou Rede Privada Virtual. As VPNs são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos.

A referência Terceira Geração "(3G) a associada a M2M (Machine-to-Machine, Mobile-to-Machine, Machine-to-Mobile Communications), possibilita à transferência e utilização de dados via redes celulares provindos de equipamentos ou terminais remotos para a comunicação e transferência de alto tráfego de dados, controle de equipamentos sem a intervenção humana.

Combinando Tecnologia da Informação com os recursos das telecomunicações, o (M2M) é um recurso que agregado a tecnologia de telefonia celular e aos recursos (3G), que possibilita integrar e automatizar processos, entre ativos da companhia em seu sistema de TI e criar serviços de valor agregado. A plataforma M2M associada à tecnologia de terceira geração pode ser implantada em diversos ambientes de aplicações e soluções, como controle e tráfego de informações em qualquer ponto do mundo, controle e acesso remoto para manutenções sem precisar deslocamento, até mesmo a necessidade da presença física para manutenção, proporciona confiabilidade, gerenciamento de todo legado, beneficiando todo sistema de informação.

1.1 OBJETIVO

Estabelecer comunicação de equipamentos de controle de velocidade, que dispõe de tecnologia de Terceira Geração (3G), para estabelecer comunicação entre equipamento de medição de velocidade ao centro de controle, para que isso se tornar possível, também contamos com a tecnologia M2M, para estabelecer um controle sobre gerenciamento dos equipamentos, que estão conectados ao sistema, também para tornar totalmente automático toda forma de comunicação e transferência de dados em grande volume, eliminando toda e qualquer forma manual para se estabelecer comunicação entre equipamentos, construir uma transmissão, estabelecer comunicação e obter controle entre equipamentos, para então possibilitar a transferência de informações, que são coletadas nos equipamentos de medição de velocidade e avanço de sinal vermelho levando até o centro de processamento de dados, para então processar a informação coletada no equipamento de medição de velocidade.

1.2 JUSTIFICATIVA

As dificuldades de acessos à comunicação na década passada levaram algumas soluções a terem alto custo, e só eram viáveis para grandes projetos, que realmente eram implantadas através de grandes investimentos. Isso fez com que o uso da telemetria fosse muito específico.

Nos últimos anos, uma das mais importantes revoluções tecnológicas disponíveis no mercado, por meio do desenvolvimento da eletrônica e da informática, com o aumento da capacidade de processamento dos celulares, a tendência tem sido cada vez mais de integração desses dispositivos com a internet.

Esse cenário de popularização proporciona queda contínua dos preços da internet móvel, traz novas e promissoras expectativas de uso da telemetria, aumentando a gama de aplicações possíveis e tornando-a muito mais acessível. Nessa nova forma de telemetria, que está sendo chamada de comunicação máquina a máquina, utiliza-se a própria rede celular para conectar equipamentos, através da conexão destes com algum dispositivo de aquisição dos dados. A comunicação M2M abre um vasto campo de aplicações de telemetria e controle nas mais diversas áreas de interesse, antes eram impossíveis ou inviáveis de serem implantadas devido ao alto custo.

2 REVISÃO BIBLIOGRÁFICA

2.1 TECNOLOGIA GSM

2.1.1 Histórico

De acordo com Alencar (2004), chamamos de comunicação sem fio aquela em que, como o nome já diz, não é necessária a utilização de fios para estabelecer a comunicação entre dois pontos, como a transmissão através de canais de rádio. Já comunicação "Móvel Celular" é definida como a rede de comunicação, também por rádio, que permite aos elementos envolvidos a movimentação constante, porém sem interrupção da mesma, através da passagem da comunicação de uma "célula" para outra.

Foi o laboratório Bell, nos Estados Unidos, em 1947, que propuseram, inicialmente, a rede de comunicações celulares, embora os experimentos só tenham começado em 1978. Em 1973, a Motorola patenteou o telefone celular. Porém, apenas em 1984 é que o sistema de comunicação celular começou a ser instalado completamente na América. O primeiro país a oferecer o serviço celular foi a Suécia, em 1981.

O padrão GSM para telefonia celular começou a ser desenvolvido na Europa, no início da década de 80. O então criado grupo *Groupe Spéciale Móbile* teve o objetivo de desenvolver um novo padrão que substituísse os diversos padrões usados até então. Embora tendo sido pensado inicialmente apenas para a Europa, o padrão demonstrou condições de se tornar um padrão global (ALENCAR, 2004).

Lançado no mercado europeu em 1991, a sigla GSM foi alterada para *Global System for Mobile Communications*. Por razões econômicas, o processo de padronização para o GSM só poderia ocorrer com o lançamento de seus serviços e, portanto, foram criadas fases para o desenvolvimento, as *GSM Phase* 1 e *GSM Phase* 2. Atualmente utilizam-se as nomenclaturas de 2,5G e 3G, correspondentes as recentes implantações do padrão GSM. No Brasil, o padrão foi adotado no ano de 2002 (ALENCAR, 2004)

2.1.2 Tecnologias de acesso

As tecnologias de acesso múltiplo são responsáveis por prover acesso ao meio físico (canal de rádio) da rede a diversos dispositivos transmissores / receptores, possibilitando o compartilhamento do mesmo por mais de um elemento de rede, atuando assim na camada de enlace do modelo OSI. As três principais estratégias de acesso, múltiplos, compartilhados, utilizados na telefonia celular são: FDMA (*Frequency-Division Multiple Access*), TDMA (T*ime- Division Multiple Access*) e CDMA (*Code-Division Multiple Access*).

Conforme Sverzut, (2005), com o avanço dos sistemas de comunicações e da telefonia móvel, uma das formas de viabilizar o aumento do número de usuários foi a divisão de determinadas áreas geográficas em "células", que são agrupadas em *clusters*. Cada célula é servida pelo seu próprio conjunto de radiotransmissores e radio receptores. Assim, reduz-se a potência necessária nas interfaces de RF (radio freqüência) permitindo a reutilização das faixas de freqüência em *clusters* diferentes. Dessa forma, em locais com grande densidade de usuários, projeta-se um sistema celular com células menores e transmissores de menor potência, para que os canais de freqüência possam ser reutilizados mais vezes, aumentando a capacidade de usuários do sistema.

Cada célula possui um determinado número de canais designados de acordo com o espectro disponível, e as BTSs (*Base Transceiver Station*- Estações-Base Transceptoras) são projetadas para atingir apenas a área de cobertura da sua célula.

Uma rede de telefonia celular é composta por diversos elementos, interligados entre si através de canais de comunicação. Cada elemento possui uma função distinta, como enviar o sinal de RF até um telefone celular ou buscar numa base de dados se o usuário que solicitou uma chamada tem autorização para isto. Esses elementos são instalados de acordo com a região de cobertura e as necessidades da operadora de telefonia celular.

A arquitetura da Rede GSM pode ser subdivida em três subsistemas, os quais são chamados de BSS (*Base Station Subsystem*), NSS (*Network and Switching Subsystem*) e OMS (*Operations and Maintenance System*). O BSS é visto como o subsistema da estação radio base (BTS), o NSS é o subsistema de gerenciamento e comutação da rede, enquanto o OMS é o subsistema de suporte e operação. A figura 1 representa a arquitetura da rede GSM.

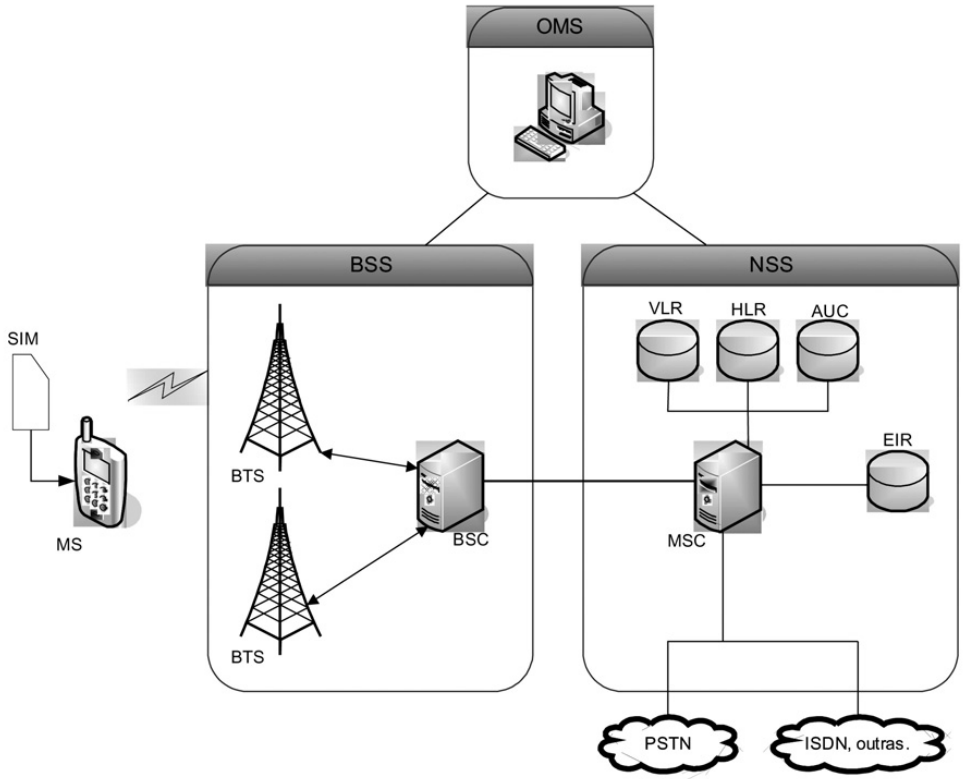

Figura 1 - Arquitetura rede GSM (Sverzut, José Umberto)

2.1.3 Identificação na Rede

Estação móvel (MS – *Mobile Station*): é o equipamento que se comunica na rede GSM, podendo ser, atualmente, um telefone celular ou também um equipamento qualquer que utilize a rede GSM para enviar ou receber informações. A MS ao movimentar-se ao longo de diferentes células, é capaz de medir a potência do sinal recebido por cada BTS e, caso o sinal esteja fraco, realizar uma troca de BTS. A opção sempre é pela BTS com melhor sinal e maior canal de freqüência, pois a potência necessária na transmissão é menor (SVERZUT, 2005; ALENCAR, 2004).

Identidade internacional do assinante móvel (IMSI – *International Mobile Subscriber Identity*): é o número que identifica o usuário na rede GSM, estando armazenado no *SIM* (SVERZUT, 2005; ALENCAR, 2004).

Identidade internacional do equipamento móvel (IMEI): assim como o IMSI, que é único por *SIM Card*, cada equipamento móvel apto a comunicar-se na rede GSM possui um número de identidade único, o IMEI. O IMEI é a forma de barrar acesso à rede de equipamentos não-aptos, como equipamentos roubados (SVERZUT, 2005; ALENCAR, 2004).

Módulo de identidade do assinante (SIM): o módulo de identidade do assinante, SIM (*Subscriber Identity Module*), fornece a identificação da MS para conexão na rede GSM. O número do assinante na rede não fica armazenado no *SIM Card* (cartão de identificação da MS), fica armazenado na operadora de telefonia celular da rede GSM.

2.2 AUTENTICAÇÃO

Centro de autenticação (AuC – *Authentication Center*): normalmente fica instalado junto ao HLR e é responsável pelas funções de autenticação e criptografia na rede. Ele fornece alguns parâmetros para autenticação, enviando estes dados ao HLR que, por sua vez, reenvia ao VLR.

Registro de identidade de equipamento (EIR – *Equipment Identity Register*): é uma base de dados contendo os números IMEI dos equipamentos. A base de dados do EIR é formada por três listas: lista branca, contendo todos os IMEI's de MS's habilitadas a utilizar o sistema, a lista negra, que contém os IMEI's de MS's que não estão habilitadas a utilizar o sistema, como exemplo MS roubada e a lista cinza, contendo os IMEI's de MS's com algum tipo de problema ou pendência, mas que não justifica a entrada das mesmas na lista negra.

Sistema de operação e manutenção (OMS): o sistema de operação e manutenção permite a supervisão e manutenção remota dos elementos da rede GSM (SVERZUT, 2005; ALENCAR, 2004).

Cada canal de rádio na interface aérea da rede GSM possui uma largura de faixa de 200 kHz. Utilizando a técnica de acesso múltiplo por divisão de tempo (TDMA), cada canal suporta ainda 8 canais, através da divisão de um período de tempo em intervalos de tempo de canal (ITC ou *time slots*).

Cada canal é numerado de 0 a 7, sendo a seqüência de divisão repetida a cada 4,615 ms, o que chamamos de quadro (portanto cada *slot* dura 576,92 µs). A informação que está sendo transmitida num ITC por uma MS é chamada de *burst* (SVERZUT, 2005; ALENCAR, 2004).

Assim, podemos concluir que há uma combinação da técnica FDMA com a TDMA no GSM. Existindo diversos canais de freqüência para transmissão, cada canal possui sua freqüência e largura de banda própria (técnica FDMA), porém o tempo de transmissão ainda é divido em oito partes, sendo cada parte designada a uma MS que transmite, teoricamente, por um quadro e ficam ociosos os sete quadros seguintes (técnica TDMA). Na prática, a

repetição garantida de um *slot* dispo- nível para a MS a cada quadro pode variar em função do tráfego da rede, nível de sinal da MS e outros fatores (SVERZUT, 2005; ALENCAR, 2004).

2.2.1 Serviço GPRS

Atualmente, são encontrados em operação os serviços 2,5G GPRS (*General Packe Radio Service*), 2,75G EDGE (*Enhanced Data rates for GSM Evolution*) e o sistema de terceira geração 3G UMTS (*Universal Mobile Tele communication System*).

O serviço GPRS utiliza os recursos já existentes na rede GSM, acrescentando alguns equipamentos na infra-estrutura da rede para suportar os novos serviços de dados. Além de permitir aos usuários a troca de dados e acesso à internet, a rede GPRS permitiu que as operadoras de telefonia utilizassem esta rede para testar e implantar novos serviços, que futuramente seriam aproveitados na implementação das redes 3G (SVERZUT, 2005).

Para a implementação do serviço de GPRS, utilizando a rede GSM, foram introduzidos novos elementos na arquitetura da rede, representada na figura 2 e descrita na seqüência.

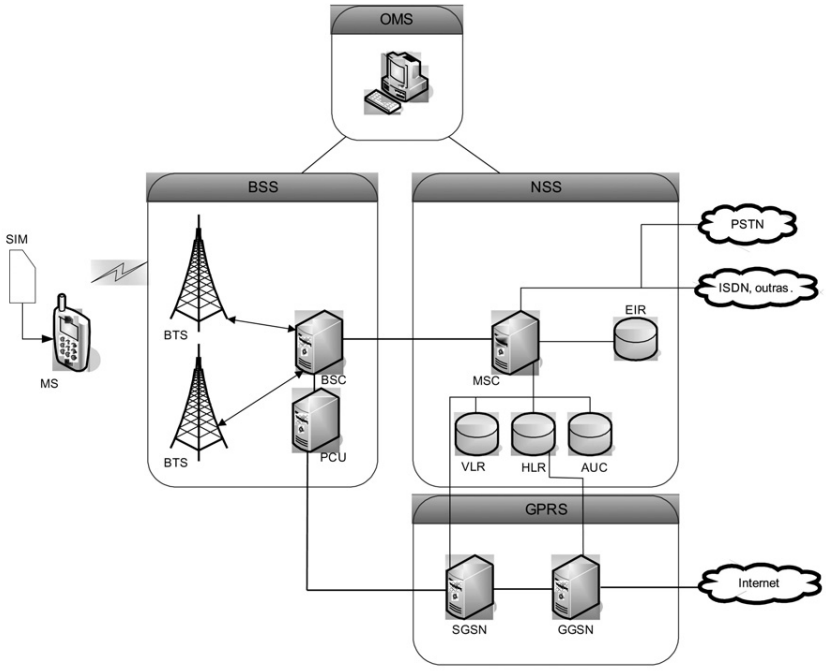

Figura 2 - Arquitetura rede GSM + GPRS (Sverzut, José Umberto)

As principais modificações realizadas na rede GSM para a implementação da rede GPRS estão indicadas no quadro 2.

Unidade de controle de pacote (PCU – *Packet Control Unit*): provê as interfaces

lógicas e físicas para o tráfego de dados na rede GPRS. Quando a rede GPRS está sendo usada, o tráfego dos dados é transferido através da PCU, que os envia para o SGSN. O tráfego de voz continua utilizando o mesmo caminho da rede GSM, passando do BSC para o MSC (SVERZUT, 2005).

Servidor do nó de suporte GPRS (SGSN– *Serving GPRS Support Node*): provê o acesso das MS's à rede GPRS. Quando uma MS realiza o *attach* na rede GPRS, o SGSN passa a gerenciar a mobilidade da MS. (SVERZUT, 2005; MISHRA, s.d.)

Tabela 1 – Modificações na rede GSM para suportar a rede GPRS

Elemento de rede	**Modificações**
MS	A MS precisa estar apta a acessar a rede GPRS.
BTS	Atualização de *software* nas BTS's existentes.
BSC	Atualização de *software* nos BSC's existentes e instalação de um novo *hardware* (PCU) para controle do tráfego de dados.
SGSN e GGSN	Dois novos elementos de rede para o serviço GPRS.
VLR, HLR, AuC, EIR	Atualização de *software* para suportar novas funções do GPRS.

2.2.2 Localização e Segurança

Quando a MS solicita uma ativação de contexto PDP (*Packet Data Protocol*), o SGSN estabelece um contexto PDP para os propósitos de roteamento necessários dentro da rede GPRS local do usuário e de acordo com o GGSN que o mesmo estiver usando, ou caso seja necessário acessar outra rede externa, como a internet. Os pacotes de dados recebidos no SGSN, após o devido processamento, são enviados ao GGSN destino. A conexão do SGSN com o GGSN é realizada através de redes IP (MISHRA, s.d.).

As principais funções do SGSN são gerenciamento de mobilidade (MM – *Mobile Management*), processamento de registro e autenticação da MS, compressão e criptografia dos dados, tarifação dos dados trafegados e interface com o HLR (para obter os dados dos usuários GPRS) (SVERZUT, 2005; MISHRA, s.d.).

Um SGSN pode direcionar os dados a mais de um GGSN de acordo com a APN utilizada pela MS.

3 METODOLOGIA

Para essa aplicação possível e viável para a instalação do medidor de velocidade, são desenvolvidos estudos técnicos nas rodovias visando identificar trechos de maiores índices de acidentes em pontos estratégicos, onde condutores costumam exceder o limite de velocidade, aumentando o risco de acidentes.

Para isso são executados estudos técnicos de campo, avaliando todo o local para a instalação do equipamento, para isso são utilizados equipamentos de medição, para verificar a se existe condições de implementação do sistema no exato local.

Todos estes estudos também seguem um rigoroso processo dentro das normativas de trânsito e segurança pública.

3.1 ANÁLISE TÉCNICA

Para consolidação do projeto, são avaliados pontos de maior índice de acidentes e excesso de velocidade nas rodovias federais. Efetivado local para a instalação do Medidor de Velocidade, são efetuados um conjunto de avaliações do local para a instalação física do medidor de Velocidade.

São utilizadas diversas ferramentas que auxiliam as pesquisas para determinar qual a operadora que poderá oferecer melhores resultados com sinais de celular no local. Medições são realizadas com equipamentos de precisão, utilizando “chip” de telefonia celular, com as operadoras disponíveis na local, com auxílio de demais ferramentas que fornecem medidas de sinal celular, potência de sinal, área de sombra, efetuando testes com todas as operadoras de telefonia celular existentes na região.

Importante para tornar possível o projeto de comunicação, é possuir em primeiro lugar recursos de infraestrutura elétrica, para fornecer energia para os equipamentos que serão instalados no local.

Contemplando estes requisitos que são obrigatórios, outras avaliações e estudos seguem para concluir a avaliação global do sistema e também para atender a normativa de segurança pública de trânsito.

3.2 ARQUITETURA DE COMUNICAÇÃO

Após conclusão do estudo técnico do local pode-se avaliar qual tipo de infraestrutura de comunicação são recomendáveis para a instalação, entre Fibra Ótica, Sinal de rádio, cabos metálicos de comunicação ou tecnologia GSM. O projeto como um todo contemplar a implementação da rede de comunicação sem fio, por meios de comunicação de telefonia celular.

Juntamente com o equipamento de medição de velocidade é instalado Um roteador que permite estabelecer a comunicação via celular dispensando qualquer outro tipo de infraestrutura de comunicação. O componente o qual vai estabelecer a comunicação entre medidor de velocidade e o centro de controle (CCO), tem como principal objetivo um modem de tecnologia 3G embarcado internamente no roteador, permitindo que o equipamento estabeleça a comunicação entre equipamentos pela rede de telefonia celular.

O medidor de Velocidade compõe de uma CPU compacta com sistema operacional Linux, com aplicativo dedicado ao tratamento das infrações, não podendo ser instalado qualquer software adicional, também não é possível conectar nenhum hardware em portas locais do equipamento, por este motivo utiliza-se o roteador para estabelecer a comunicação do equipamento.

O projeto conta com algumas opções de comunicação, as quais oferecem a mesma conectividade, mas com diferencias de infraestrutura e custos.

Dentre as diversas opções para estabelecer as comunicações entre equipamentos, três delas são as mais recomendadas, sendo elas Arquitetura com VPN pública, VPN pública, mas, com APN das operadoras e VPN privada que automaticamente contempla a APN com as operadoras.

Cada arquitetura possui formas diferentes de conectividade, administração de cada circuito e custos de implementação diferenciados para o projeto.

3.3 TIPOS DE REDES

Muita coisa mudou com o início do serviço GSM, que trouxeram o GPRS e EDGE e recentemente, com a implementação das redes 3G, também o HSDPA/HSUPA.

O GSM (Groupe Spécial Mobile, mais tarde renomeado para Global System for Mobile) surgiu da união de vários países europeus, com a idéia de criar um padrão global de

telefonia, para substituir os diversos padrões existentes e usados com a primeira geração de redes celulares. A primeira rede GSM entrou em operação em 1991, na Finlândia. A padronização em torno do GSM acabou sendo um dos principais fatores que possibilitaram a globalização dos celulares e já que o uso de um padrão comum levou a queda dos custos.

O GPRS (considerado uma tecnologia 2.5G) foi a primeira opção de acesso à web através da rede celular realmente utilizável. Ele é um sistema inteiramente digital, baseado na transmissão de pacotes, tarifado de acordo com o volume de dados transferido.

3.3.1 Rede EDGE

EDGE, foi uma evolução do GPRS, que mantém a mesma estrutura GSM, mas implementa um novo sistema de modulação, que multiplica por três a velocidade de conexão. Apesar do aumento da velocidade, o EDGE não é considerado uma tecnologia 3G, mas sim 2.75G.

Mesmo nas redes GSM já atualizadas para o EDGE, o GPRS continua disponível, não existe diferença no alcance do sinal entre o EDGE e o GPRS.

Em seguida temos o HSDPA, um protocolo mais recente, que reduz a latência e aumenta a taxa de download da rede de forma expressiva. Utilizando o HSDPA como protocolo de transporte, o UMTS suporta taxas de 1.8, 3.6, 7.2 e 14.4 megabits, de acordo com a implementação usada pela operadora (no Brasil a versão de 7.2 megabits é a mais comum). Naturalmente, a velocidade real varia de acordo com a qualidade do sinal e o número de usuários conectados à mesma estação de transmissão, mas ela é sempre bem mais alta que no WCDMA.

3.3.2 Rede HSDPA

O HSDPA é considerado um protocolo 3.5G, é possível verificar qual sistema está sendo usado simplesmente olhando o ícone da conexão. Um "3.5G" mostra que está sendo usado o HSDPA, um "3G" que está em uso o WCDMA, um "E" que está sendo usado o EDGE e um "G" que você está em uma área em que apenas o velho GPRS está disponível.

O sistema HSDPA funciona bem apenas a distâncias relativamente curtas, por isso os aparelhos chaveiam automaticamente para o WCDMA nas áreas de menor cobertura, fazendo com que a taxa de transmissão seja reduzida. Outra limitação é que o HSDPA aumenta apenas

a taxa de download, sem fazer nada com relação ao upload, que continua sendo de apenas 384 kbits, assim como no WCDMA.

3.3.3 Rede HSUPA

Temos também o HSUPA (também chamado de EUL), um padrão atualizado, que complementa as melhores taxas de download do HSDPA com melhoras também nas taxas de upload, atingindo a velocidade de 730 kbps (no HSUPA categoria 1) até 5.76 megabits (HSUPA categoria 6). Por ser apenas uma extensão do UMTS e não um novo padrão 3G, os investimentos necessários para migrar as redes são relativamente pequenos, já que é preciso apenas substituir alguns equipamentos nas torres e adequar a estrutura de roteamento.

No Brasil, a única operadora a já utilizar o HSUPA (no início de 2009) é a Vivo, o que pode resultar em um diferencial competitivo no futuro. Ainda não existem notícias sobre o HSUPA por parte da Claro, da TIM ou da Oi, já que elas optaram por inicialmente implantar apenas o HSDPA e precisarão trocar equipamentos para oferecerem o HSUPA. Como não existe tanta demanda por melhores taxas de upload quanto existe por downloads mais rápidos, pode ser que a atualização demore um pouco.

3.3.4 Funções básicas de VPN

A utilização de redes públicas tende a apresentar custos muito menores que os obtidos com a implantação de redes privadas, por isso nasce a necessidade de utilizar VPNs. Esta necessidade torne-se efetiva e deve prover um conjunto de funções que garanta Confidencialidade, Integridade e Autenticidade.

3.3.5 Integridade de VPN

Na eventualidade dos dados serem capturados, é necessário garantir que estes não sejam adulterados e re-encaminhados, de tal forma que quaisquer tentativas nesse sentido não tenham sucesso, permitindo que somente dados válidos sejam recebidos pelas aplicações suportadas pela VPN.

3.3.6 Autenticação VPN

A Autenticação é importante para garantir que o originador dos dados que trafeguem na VPN seja, realmente, quem diz ser. Um usuário deve ser identificado no seu ponto de acesso à VPN, de forma que, somente o tráfego de usuários autenticados transite pela rede. Tal ponto de acesso fica responsável por rejeitar as conexões que não sejam adequadamente identificadas. Para realizar o processo de autenticação, podem ser utilizados sistemas de identificação/senha, senhas geradas dinamicamente, autenticação por RADIUS (Remote Authentication Dial-In User Service) ou um código duplo.

A definição exata do grau de liberdade que cada usuário tem dentro do sistema, tendo como conseqüência o controle dos acessos permitidos, é mais uma necessidade que justifica a importância da autenticação, pois é a partir da garantia da identificação precisa do usuário que poderá ser selecionado o perfil de acesso permitido para ele.

3.3.7 Nível de Segurança

A especificação da VPN a ser implantada deve tomar por base o grau de segurança que se necessita, ou seja, avaliando o tipo de dado que deverá trafegar pela rede e se são dados sensíveis ou não. Dessa definição depende a escolha do protocolo de comunicação, dos algoritmos de criptografia e de Integridade, assim como as políticas e técnicas a serem adotadas para o controle de acesso. Tendo em vista que todos esses fatores terão um impacto direto sobre a complexidade e requisitos dos sistemas que serão utilizados, quanto mais seguro for o sistema, mais sofisticados e com capacidades de processamento terão de ser os equipamentos, principalmente, no que se refere a complexidade e requisitos exigidos pelos algoritmos de criptografia e integridade.

3.4 ARQUITETURA COM VPN PÚBLICA

A arquitetura com VPN pública oferece infraestrutura de baixo custo, administração dos circuitos de conexão muito simplificada, gerenciamento via HTTP de acesso interno ou externo, podendo ser acessada de qualquer local, software de gerenciamento de fácil operação e administração.

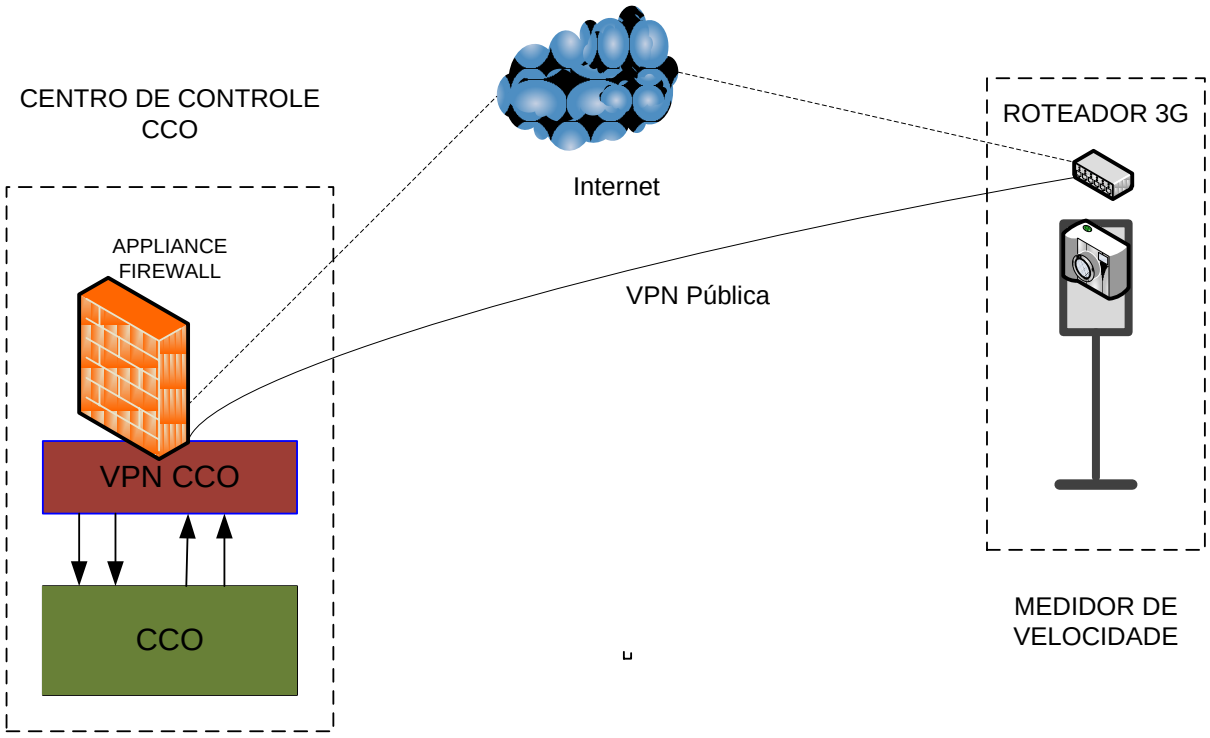

Figura 3 - Arquitetura com VPN Pública (Autoria própria)

3.5 VANTAGENS E DEVANTAGENS PARA UTILIZAÇÃO DE VPN PÚBLICA

3.5.1 Vantagens

- Baixo custo de manutenção e operação, envolve somente o custo sobre pacote de dados, multiplicados pela quantidade de radares sem custo adicional de operação ou infra-estrutura.
- Atente 100% dos pontos que possuem cobertura 3G, EDGE ou até mesmo GPRS, independente de qual operadora trabalhe e mesmo opcionalmente poderá ser efetuado por coleta manual na falha de qualquer equipamento.
- Não vincula as atividades em uma única operadora, pode agregar todas as operadoras de telefonia celular, não dependente da infra-estrutura interna da operadora para funcionamento.
- Após contrato de fidelidade permite a troca de operadora sem custos e transtornos, pois é só substituir a operadora e configurar os roteadores de cada ponto, não vinculando Link dedicado entre (CCO) e Operadora de telefonia.
- Com esta modalidade podemos atender a todos os tipos de conexão, Open VPN (sem fazer alterações de configurações no radar), podendo ainda utilizar protocolos de comunicação

L2TP, PPTP, IPsec, pois só dependerá dos serviços oferecidos pelos roteadores, pois os (Appliances) possuem e atendem todo tipo de comunicação disponível os quais são oferecidos pelos roteadores.

- Quando não houver mais disponibilidade de serviços contratados pela operadora poderá ser direcionado todo o tráfego dos radares para os (Appliances) sem custos ou investimentos com infra-estrutura.
- Administração local dos (Appliances) é mais intuitiva, fácil de operar e encontrar falhas, não dependendo de terceiros nas operadoras para detecção e resolução do problema.
- Manutenção simplificada e convergida para apenas uma administração e centralizada.
- Monitoramento simplificado e pró-ativo globalizada.
- Agrega apenas o custo do Link dedicado para comunicação com alta disponibilidade.
- Não envolve disponibilidade de outras operadoras para a comunicação funcionar.
- O link dedicado é de grande disponibilidade, sendo assim, se em algum momento a comunicação da Copel falhar o link alternativo de baixo custo assumirá o tráfego de dados.
- Apresenta o mesmo nível de segurança que outras opções, mas com baixo custo de manutenção e fácil gerenciamento.
- Possibilita a adesão a qualquer momento que necessário para o uso de VPN privada das operadoras, em caso de disponibilidade dos serviços.
- Fácil conversão para VPN Privada, sem fidelidade contratual.
- Fácil conversão de Rede privada para pública.

3.5.2 Desvantagens

- SLA alto de atendimento para pacote de dados é de 72 horas (Determinado pela Anatel), mas que são aplicadas a todas outras arquiteturas propostas.

3.6 ARQUITETURA COM VPN PÚBLICA COM APN DAS OPERADORAS

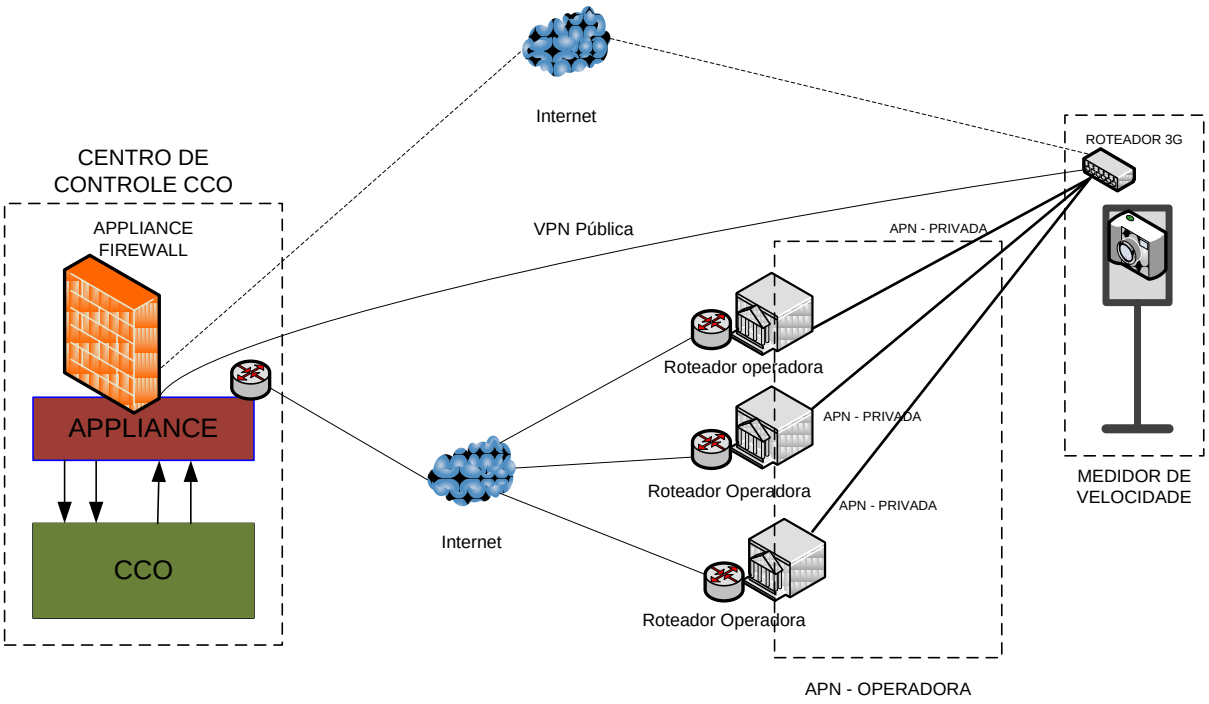

Figura 4 - Arquitetura de rede com VPN Pública e APN das Operadoras (Autoria própria)

3.7 VANTAGENS E DESVANTAGENS DA VPN PÚBLICA COM APN DAS OPERADORAS

3.7.1 Vantagens

- Baixo custo de manutenção e operação envolve somente o custo sobre pacote de dados multiplicados pela quantidade de radares sem custo adicional de operação ou infra-estrutura.
- A comunicação com a VPN privada é do ponto de radar até a infraestrutura da operadora, após esta etapa a operadora direciona a rota seu tráfego de dados para a internet pública através de roteadores internos.

3.7.2 Desvantagens

- Não atente 100% dos pontos que possuem cobertura 3G, EDGE ou até mesmo GPRS, pois depende que a operadora ofereça os serviços, que são em geral sem custo, mas nem todas as operadoras oferecem este serviço, apenas em projetos de grande porte e quando oferece.
- O tráfego dos radares passa pelo (Backbone) da operadora e é direcionada para a rede pública, incidindo na mesma opção da VPN Pública, direcionando o tráfego para internet, mesmo sendo criptografada.
- Administração de cada pacote de dados com respectivo tráfego de dados fica vinculada à operadora ficando mais difícil comprovar falhas, ou controle de dados sobre o mesmo, sempre que estiver conectado será "tunelado" na VPN privada, sendo assim sem exceder o volume oferecido, não poderá ser substituído por outro, pois, outro deverá passar por processo de registro para VPN privada, tendo que entrar em procedimento interno para inclusão no sistema.

3.8 ARQUITETURA COM VPN PRIVADA COM APN DAS OPERADORAS

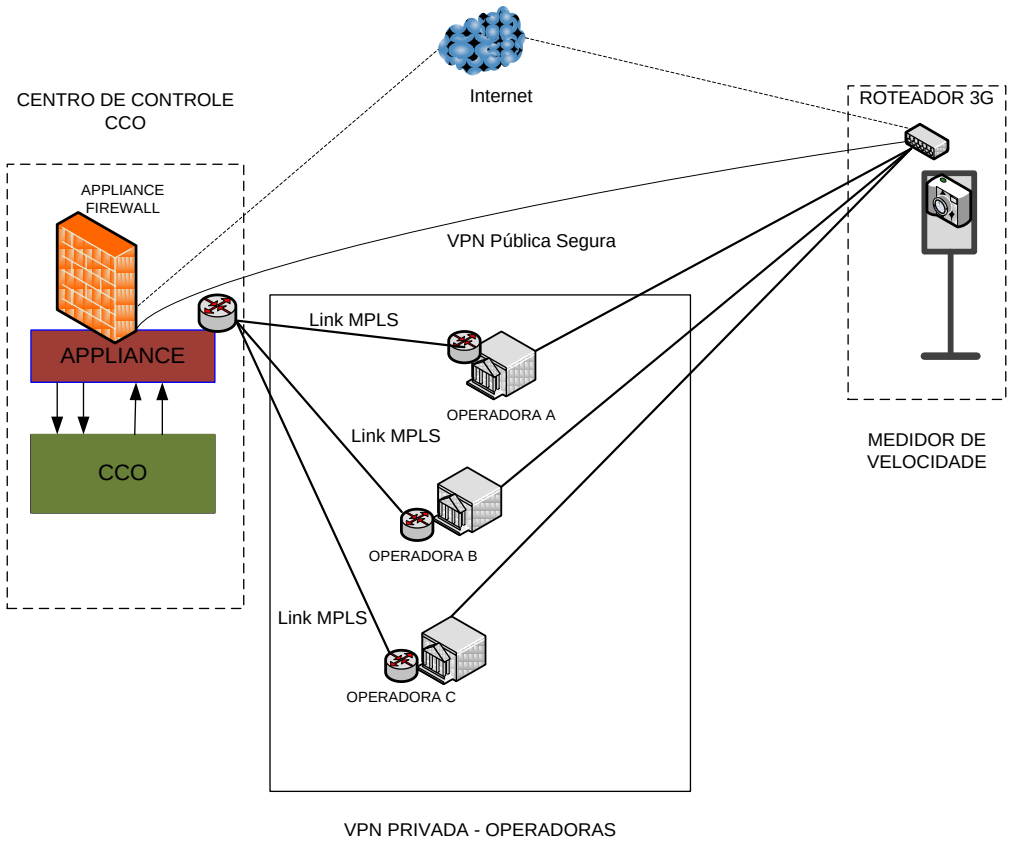

Figura 5 – Arquitetura de rede com VPN Privada com APN das Operadoras (Autoria própria)

3.9 VANTAGENS E DESVANTAGENS VPN PRIVADA COM APN DAS OPERADORAS

3.9.1 Vantagens

- Apresenta alto nível de segurança criptografia.
- É criada VPN privada desde o Roteador, passando pelo (BackBone) da operadora e sendo roteada para o CCO através de um link dedicado, contratado exclusivamente para ligar a operadora ao CCO, sem cair na rede pública de internet.
- Possui alta disponibilidade quando o tráfego sai da operadora e é roteada para o CCO.
- Tráfego possui redundância de Link pela operadora terceira contratada.

3.9.2 Desvantagens

- O link dedicado de cada operadora é estabelecido por uma terceira operadora. (Ex.: estabelecer VPN privada da vivo deverá contratar um link da Embratel, Copel, GVT, OI, entre operadora Vivo e CCO, que tecnicamente seria um Link dedicado “rede MPLS” o qual o tráfego de dados irá ser transferido.
- Os pacotes de dados sempre estariam vinculados a uma VPN privada sem condições em casos de falhas dos serviços na operadora de ser substituído por um alternativo para suprir necessidades.
- Alto custo mensal de link dedicado, para cada operadora deverá ter um Link Mpls estabelecido para trafegar dados em rede Privada.
- Deverá ter um investimento de um roteador no CCO para receber os pacotes roteador pela operadora.
- Descentralização de administração dos canais de comunicação entre operadoras.
- Difícil controle e detecção de falhas nas transmissões, pois o tráfego é gerenciado pela operadora terceira, usualmente usada para conectar empresas, em caso de centenas de conexões podem ser de alta complexibilidade.
- Difícil conversão para VPN pública. Existem contratos de fidelidade, com multas por finalização antecipada.
- SLA alto para atendimento e reparos, para pacote de dados é 72 horas (estabelecido pela Anatel) o mesmo para as outras VPNs, sendo pública ou privada.

3.10 DESEMPENHO DA REDE

Todas essas tecnologias permitem acesso de dados por meio da rede celular. A tecnologia GPRS permite acessos com taxa máxima de 40kbps, a tecnologia EDGE permite acessos de até 384kbps e a tecnologia 3G atual permite acessos de até 7,2Mbps.

4 ANÁLISE DOS RESULTADOS

4.1 MÉTODOS

Esta seção tem o intuito de descrever os métodos e critérios utilizados para compor a análise dos aspectos da tecnologia aplicada. A pesquisa tem como objetivo mensurar as vantagens que a tecnologia oferece com relação às outras tecnologias disponíveis no mercado, todas direcionadas para tráfego de dados paras sistemas de comunicações móveis e infraestrutura cabeada.

O referencial de pesquisa proporcionou uma análise mais detalhada dos tipos de serviços oferecidos por diversas operadoras de Telecom e as mais diversas opções de soluções disponíveis no mercado para atender a necessidade do projeto. Com a interpretação dos resultados obtidos, podemos obter uma avaliação dos prós e contras no uso dessa tecnologia.

4.2 COMPARATIVOS DE TECNOLOGIAS

4.2.1 Infraestrutura cabeada

Primeiramente foi analisado o custo para transmissão de dados na rede, através de instalação de uma infraestrutura composta em passagem de cabos par metálico ou até mesmo fibra óptica.

A infraestrutura depende muito da localização e recursos que as operadoras possuem para o local, mas na maioria dos serviços ofertados pelas operadoras, a infraestrutura cabeada envolve muito custo por depender de vários fatores como: mão de obra para instalação e aplicação do cabeamento possui custo excessivo, equipamentos de interface ainda possuem custo elevado, serviços e pacotes de transmissão somente são viáveis pra grandes projetos e para grandes corporações o que corresponde às despesas operacionais. A tabela 1 apresenta uma comparação dos custos (mensal) para transmissão de dados para cada ponto do projeto, contemplando que este projeto inicialmente possui 212 pontos para transmissão de dados.

4.2.2 Infraestrutura sem fio

Outra opção que está crescendo muito devido ao grande investimento e a comunicação sem fio via telefonia celular, a análise do desempenho evidenciou que é possível agregar a utilização dos recursos da telefonia celular para efetuar a comunicação de dados para o centro de controle, mesmo quando tiver um grande volume na transmissão e até mesmo oferecendo alta velocidade na transmissão.

4.3 COMPARATIVO ENTRE CUSTOS PARA CADA TECNOLOGIA

Tabela 2 Custo por ponto instalado (Autoria própria)

TECNOLOGIA	INSTALAÇÃO	MENSAL	FIDELIDADE	ANUAL	FINAL (5 ANOS)
ADSL	100,00	150,00	SIM	1.900,00	9.100,00
FIBRA ÓPTICA	580,00	1.614,16	SIM	19.949,92	97.429,60
RÁDIO	2.500,00	2.480,00	SIM	30.340,00	151.300,00
GSM (3G)	-	89,90	SIM	1.078,80	5.394,00

4.4 CUSTO PARA IMPLANTAÇÃO TOTAL DO PROJETO

Tabela 3 Custos VPN pública (Autoria própria)

SERVIÇO	QTDE	INSTALAÇÃO	UNITÁRIO	MENSAL	ANUAL	CUSTO (5 ANOS)	CUSTO TOTAL
APPLIANCE	2	15.000,00		800,00	30.183,00		
LINK DEDICADO INTERNET	1	580,00		1.316,14	15.793,68	78.968,40	
PACOTE DE DADOS 3G	212			21.178,80	254.145,60	1.270.728,00	
ROTEADORES (RADAR)	212		1.100,00			233.200,00	
TOTAL							1.630.894,40

Os custos relacionados contemplam toda a infraestrutura aplicada desde os equipamentos aplicados no centro de controle para recebimento dos dados até a tecnologia aplicada no ponto do medidor de velocidade, instalados a beira da rodovia que tem a função de coletar dados para o envio e processamento.

Esta planilha não contempla valores de softwares específicos e desenvolvidos exclusivamente para as atividades de operação, sendo assim, o projeto contempla apenas as instalações da infraestrutura e serviços de comunicação.

A tabela apresenta todos os custos aplicados para o desenvolvimento da infraestrutura baseada em Open VPN pública, projeto qual expressa uma redução de custos significativa e viável para a aplicação.

Ainda reduz o investimento em equipamentos em comparação a outras infraestruturas propostas e com vantagens e facilidades de administração e manutenção

4.5 CUSTO PROJETO PARA RADARES COM VPN PÚBLICA COM APN OPERADORA

Tabela 4 Custo VPN pública com APN das Operadoras (Autoria própria)

SERVIÇO	QTDE	INSTALAÇÃO	UNITÁRIO	MENSAL	ANUAL	CUSTO (5 ANOS)	CUSTO TOTAL
APPLIANCE	2	15.000,00		800,00	30.183,00	48.000,00	
LINK DEDICADO INTERNET	1	580,00		1.316,14	15.793,68	78.968,40	
PACOTE DE DADOS 3G	212			21.178,80	254.145,60	1.270.728,00	
ROTEADORES (RADAR)	212		1.100,00			233.200,00	
ROTEADOR (CCO)	1					6.000,00	
TOTAL							**1.636.894,40**

Os custos relacionados contemplam toda a infraestrutura aplicada desde os equipamentos aplicados no centro de controle para recebimento dos dados até a tecnologia aplicada, no ponto do medidor de velocidade, instalados a beira da rodovia que tem a função de coletar dados para o envio e processamento.

Esta planilha não contempla valores de softwares específicos e desenvolvidos exclusivamente para esta atividade, sendo isso apenas equipamentos e serviços de comunicação.

A implementação com VPN pública contém uma opção muito parecida com a estrutura de somente Open VPN pública, com a diferença que ao invés de ter o tráfego diretamente pela internet e sem passar diretamente pela operadora, a rota da VPN pública com APN da operadora faz uma conexão diretamente com o (Backbone) da operadora roteada o tráfego via roteadores distribuídos pelas cidades, chegando na infraestrura desejada em um Roteador específico, para isso são agregado custos e a administração do sistema passa a ser um pouco mais distribuído e descentralizado.

4.6 CUSTO PROJETO PARA RADARES COM VPN PRIVADA

Tabela 5 – Custo de VPN privada (Autoria própria)

SERVIÇO	QTDE	INSTALAÇÃO	UNITÁRIO	MENSAL	ANUAL	CUSTO (5 ANOS)	CUSTO TOTAL
APPLIANCE	2	15.000,00		800,00	30.183,00	48.000,00	
LINK DEDICADO INTERNET	1	580,00		1.316,14	15.793,68	78.968,40	
PACOTE DE DADOS 3G	212			21.178,80	254.145,60	1.270.728,00	
ROTEADORES	212		1.100,00			233.200,00	
ROTEADOR (CCO)	1					6.000,00	
LINK MPLS OPERADORA A (2 MBPS)	1	1.500,00		2.000,00	24.000,00	120.000,00	
LINK MPLS OPERADORA B (2 MBPS)	1	1.500,00		2.000,00	24.000,00	120.000,00	
LINK MPLS OPERADORA C (2 MBPS)	1	1.500,00		2.000,00	24.000,00	120.000,00	
TOTAL							**1.996.896,40**

Na opção de infraestrutura com VPN dedicada, todos os circuitos por onde trafegam as informações são de rede privada, pertencentes às operadoras, possuem a mesma segurança que outras oferecem mas por caminhos diferentes.

O custo para aplicação desta infraestrutura é bem elevada, onerando o orçamento, e em muitos casos pode tornar o projeto inviável.

Nesta opção, da mesma forma são contemplados apenas equipamentos e serviços de comunicação, softwares desenvolvidos e específicos para operação não foram orçados.

4.7 RESULTADOS

Levando-se em conta critérios de compatibilidade de tecnologias, embora ambos sejam padrões de tecnologia comumente aplicada, a tecnologia GSM (3G) 3G, são padrões desenvolvidos para solução em diferentes segmentos de tecnologia no mercado das telecomunicações, competem como solução para transmissões cabeada com altas taxas de transmissão de dados. Obviamente cada solução proporciona menor custo de implantação quando adotada em redes estabelecidas com suas respectivas tecnologias.

O custo para transmissão de dados em redes de telefonia GSM oferece a mesma disponibilidade, alta velocidade, com custos reduzidos, tornando viável muitos projetos que algum momento foram inviabilizados por terem alto custo para aplicação da comunicação de dados. Esse custo é em sua maior parte proveniente dos investimentos necessários para agregar à estação base a infra-estrutura necessária para que possa ocorrer uma transmissão de dados.

Adicionar uma tecnologia de 3G em sua rede significa à operadora agregar serviços diferenciados e explorar nichos de mercado, como por exemplo, mercados onde a oferta de acesso ADSL e infraestrutura cabeada é limitada e as operadoras podem oferecer a transmissão de dados pela rede celular como banda larga para conexão de seus assinantes à internet com custos significativamente mais baixos.

5 CONCLUSÕES E TRABALHOS FUTURO

5.1 CONCLUSÕES FINAIS

A presente pesquisa nos permite concluir que a modernidade da tecnologia exige, cada vez mais, dos usuários de tecnologia, conhecimento e capacidade de discernimento entre o grande número de opções e recursos oferecidos no mercado de tecnologia

A telefonia móvel encontra-se em constante evolução, graças às mudanças em adequação às necessidades e exigências do mercado, oferecendo basicamente serviço de dados para tráfego de voz e dados.

Conforme visto no decorrer deste trabalho, a transmissão de dados via terminais móveis está se difundindo rapidamente e se tornando uma nova fonte de renda entre operadoras e clientes, que utilizam cada vez mais este serviço que conta hoje com taxas de transmissão de dados que variam de 1 Mbps a 7.2 Mbps, valores semelhantes aos oferecidos por conexões de banda larga do tipo ADSL.

Dessa forma, a telefonia 3G surge como alternativa às crescentes exigências de rapidez e qualidade, possibilitando o acesso a serviços inovadores e com preços extremamente atrativos.

5.2 TRABALHOS FUTUROS

Com a expansão das tecnologias, em breve poderemos contar com mais opções e diversificar ainda mais a aplicação, facilitando e reduzindo custos de projeto, lançamentos de novos equipamentos de comunicação para oferecer mais opções. Equipamentos ofertados hoje no mercado ainda estão limitados aos serviços das operadoras, e muito em breve as operadoras oferecerão mais opções de serviços e com tecnologia mais avançada.

REFERÊNCIAS

ALENCAR, Marcelo Sampaio. **Telefonia celular digital**. São Paulo: Editora Érica, 2004.

ERONEN, Pasi. **TCP Wake-Up**: Reducing Keep-Alive Traffic in Mobile IPv4 and IPsec NAT Traversal. Nokia Research Center. 2008. Disponível em: http://research.nokia.com/files/NRCTR2008002.pdf. Acesso em 25/11/2011.

European Telecommunications Standards Institute (ETSI). **Digital cellular telecommunications system (Phase2+) - AT Command set for GSM Mobile system (Phase 2+) - General Packet Radio service (GPRS) - Mobile Station (MS) supporting GPRS**. 3GPP TS 07.60 version 7.2.0, 1998. Sophia Antipolis: ETSI TS 101356 V7.2.0. 2001.

Digital cellular telecommunications system. **(Phase 2+) General Packet Radio Service (GPRS) - Service description – Stage 2**. GSM 03.60 version 7.4.1, 1998. Sophia Antipolis: ETSI EN 301 344 V7.4.1. 2000.

Digital cellular telecommunications system (Phase 2+) - Radio transmission and reception. 3GPP TS 45.005 version 7.13.0 Release 7. Sophia Antipolis: ETSI TS145 005 V7.13.0. 2008.

HOLMA, H.; TOSCALLA, A., WCDMA for UMTS Radio Access for Third Generation mobile Communications, Wiley & Sons Ltd, 2004.

MISHRA, Amitabh. P**erformance and architecture of SGSN and GGSN of General Packet Radio Service (GPRS)**. Blacksburg, VA: Virginia Polytechnic Institute and State University, s.d.

QUALCOMM 3G Overview CDMA Technologies, Internet site address: http://www.umtschips.com/index.jsp. Acesso em 25/10/2011.

QUALCOMM. **HSDPA** Disponível em: http://www.umtschips.com/index.jsp. Acesso em 15/11/2011.

SVERZUT, José Umberto. **Redes GSM, GPRS, EDGE e UMTS**. São Paulo: Editora Afiliada, 2005

TELECO. **Tutorial GPRS**. Disponível em: http://www.teleco.com.br. Acesso em 25/10/2011.

TELECO. **Tutorial EDGE**. Disponível em: http://www.teleco.com.br. Acesso em 25/10/2011.

TELECO. **Tutorial UMTS**. Disponível em: http://www.teleco.com.br. Acesso em 25/10/2011.

TELECO. **Tutorial HSDPA**, Disponível em: http://www.teleco.com.br. Acesso em 25/10/2011

THEALANDER, M. **Evolução em 3G Levando o CDMA para a próxima década**. Documento escrito para o CDMA Development Group em 10/10/2011.

WACKER, J.; NOVOSAD, T. **Radio Network Planning and Optimisation for UMTS**, Wiley & Sons Ltd, 2006.