HOLOS
ISSN 1807 - 1600

SEGURANÇA E CONFIABILIDADE PARA AMBIENTE SOHO

M. A. G. T. Silva[1], R. B. Ferreira[1], O. S. Leite[1], S. H. Macedo[1], S. L. Santos[1]
[1]Coordenação de Telecomunicações – Instituto Federal Fluminense, campus Campos Centro
marcoagts@gmail.com – rbf-@hotmail.com – ozeas@iff.edu.br – shmacedo@iff.edu.br – suelsster@gmail.com

Artigo submetido em agosto/2012 e aceito em agosto/2013

RESUMO

Esta pesquisa propõe a utilização de tecnologia sem novos fios para ambientes de Pequenos Escritórios e/ou Escritórios Residenciais (SOHO), dentro de uma visão de segurança. É certo que as informações digitais são os produtos vitais da nova economia. No entanto, as pequenas empresas prestadoras de serviços para empresas de maior porte, acabam por ter acesso a esse patrimônio virtual sem nenhum requisito de segurança. Os estudos práticos deseja-se demonstrar que a infraestrutura da Tecnologia da Informação para SOHO pode ser atingida com equipamento sem novos fios, através da rede elétrica. Este sistema será demonstrado através de resultados práticos em diferentes ambientes do estudo da tecnologia *Power Line*.

PALAVRAS-CHAVE: SOHO, segurança, tecnologia, sem novos fios.

SAFE AND SECURE ENVIRONMENT FOR SOHO

ABSTRACT

This research proposes using a technology without new wires for environments of Small Office and/or Home Office (SOHO), with a security view. Indeed digital information products are vital to the new economy. However, the small businesses which provide services to large companies, end up having access to that virtual heritage without any security requirement. The practical studies want introduce that the infrastructure of Information Technology for SOHO equipment can be achieved without new wires, through the electrical grid. This system will be demonstrated through practical results in different environments of the Power Line Technology study.

KEYWORDS: SOHO, security, technology, no new wires.

HOLOS
ISSN 1807 - 1600

SEGURANÇA E CONFIABILIDADE PARA AMBIENTE SOHO

1 INTRODUÇÃO

A empresa tipo SOHO (*Small Office or Home Office* – Pequeno Escritório ou Escritório doméstico) surgiu no final da década de 90, inicialmente denominada de "*Home Office"* ou "*Go Home"* e tinha como objetivo reduzir custo com funcionários. Ficou claro que tal atividade foi possível no início para alguns profissionais, como: jornalistas, arquitetos, despachantes, técnicos em informática, *designers* gráficos e outros (Ed. GLOBO, 2007). Na mesma época, o acesso à rede mundial de computadores desponta com o advento da Ethernet e a evolução das redes locais, o que torna este tipo de investimento cada vez mais viável.

Segundo Bolzani (2004), os produtos virtuais da rede de dados, juntamente com os serviços agregados, são provavelmente os ativos que gerarão mais lucro, onde as "informações digitais, produtos virtuais da nova economia, representam diferentes formas de conteúdos". Para o autor (*op. cit.*), este é o nicho de mercado que provavelmente mais crescerá economicamente.

Schetina, Green, e Jacob (2002) afirmam também que apesar desta tendência do mercado, a "comunidade de redes SOHO, geralmente é negligenciada pelo mundo da segurança da informação", além de não terem suporte de uma equipe própria de TI. A segurança destas empresas é de suma importância para as grandes empresas, as quais diferem entre si com a existência de administradores de rede e uma equipe bem preparada (SCHETINA *et al.*, 2002).

2 SEGURANÇA DA INFORMAÇÃO

Uma rede local é de extrema importância podendo automatizar e simplificar tarefas, facilitando a vida do usuário através do compartilhamento de recursos. Porém, as redes locais ou LAN (*Local Area Network* – Área da Rede Local*)* sempre possuem um *link* para prover a conexão com a internet do cliente e do servidor sem nenhum tratamento adicional por parte dos provedores. Logo, qualquer dado que trafegue neste ambiente está normalmente desprotegido.

Bolzani (2004) afirma que a segurança das informações que circulam numa rede deve ser uma das principais preocupações de um integrador de sistemas desta natureza. No qual deve ser realizado um controle relacionando todos os tipos de acesso, seja de dados ou tráfego, tendo em vista o meio ser inseguro.

Para Peres e Welber (2003) os protocolos que formam a VPN (*Virtual Private Network* – Rede Privada Virtual) são possivelmente a solução para a comunicação em redes com baixa segurança. Os autores (*op. cit.*) corroboram também com a ideia que a solução mais natural é a utilização do IPSec (*Internet Protocol Security* – Protocolo de Segurança da Internet) ou outro algoritmo robusto de criptografia, em conjunto com redes VPN. O propósito do emprego desta tecnologia é aumentar a segurança das redes, sejam essas separadas fisicamente ou dentro de uma rede local. Também é possível a partir de uma VPN compartilhar os recursos disponíveis entre as LANs ou ao acesso remoto.

2.1 Redes virtuais

Uma VPN oferece, tanto ao cliente quanto ao servidor, a possibilidade do emprego de acesso de formas diferentes: por rádio; cabo; satélite; ou qualquer outra forma de conectividade com a rede.

Sarlo da Silva (2003, *passim*) define outra vantagem: a possibilidade de ser implementada uma VPN, como ferramenta de conexão entre redes, possibilitando uma grande escalabilidade, que permite adicionar filiais ou novos usuários remotos, ou seja, sempre é possível incluir um novo cliente através de acesso remoto na rede.

Dentre a possibilidade das conexões de uma VPN existem três topologias comuns possíveis: (i) *host a host,* que é a comunicação entre dois microcomputadores separados fisicamente, podendo estar ou não em uma mesma rede física; (ii) *host ao gateway,* que é a conexão de um equipamento remoto a uma rede fisicamente distante; e, (iii) *gateway* a *gateway,* cuja conexão é estabelecida entre duas redes distintas, onde os *gateways* de VPN estarão sempre conectados.

A Figura 1 ilustra a topologia das possibilidades de conexão VPN entre redes *(gateway* a *gateway),* um cliente remoto (*host* ao *gateway*) e considerando somente a LAN "A", observa-se a conexão entre equipamentos (*host* a *host*).

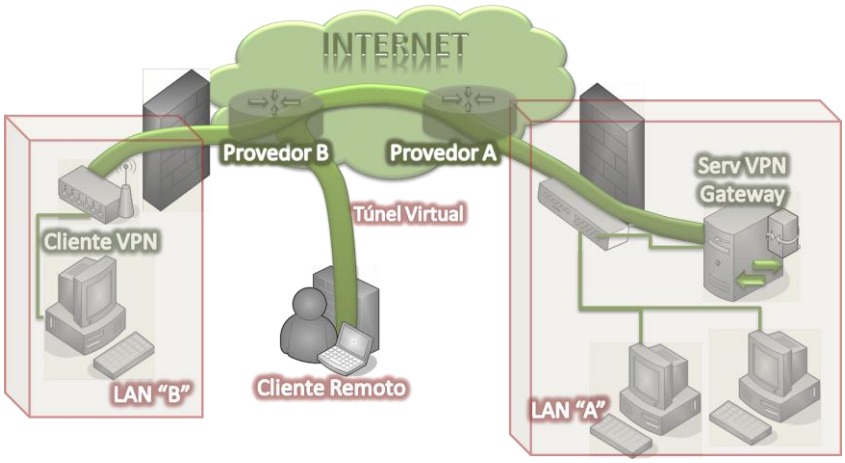

Figura 1 - Topologia VPN

A tecnologia VPN é baseada na ideia de tunelamento que envolve o estabelecimento e manutenção da ligação à rede lógica. Os pacotes utilizados nas redes VPNs são encapsulados e transmitidos entre um cliente VPN e o servidor. Chegando ao destinatário, os pacotes são desbloqueados ou descapsulados.

O protocolo utilizado comumente para realizar a segurança é o IPSec (*Internet Protocol Security* – Protocolo de Segurança da Internet), para montar uma VPN. Além de facilitar a administração dos serviços de rede, por tratar de diversas questões de segurança num mesmo pacote, tem-se a garantia de ser um protocolo padronizado que garante: privacidade, integridade e autenticidade. Esta facilidade é devido à internet e às redes locais (LANs) serem baseadas no protocolo da internet o TCP/IP (*Transmission Control Protocol Internet Protocol* – Protocolo de Controle de Transmissão / Protocolo de Interconexão).

O protocolo IPSec, criptografa o texto original da mensagem a ser transmitida (texto normal). O texto original da mensagem a ser transmitida (texto normal) é transformado, gerando texto criptografado na origem, através de um processo de codificação. O texto (ou a mensagem) protegido é então transmitido e, no destino, o processo inverso ocorre, isto é, o método de criptografia é aplicado também para decodificar o texto criptografado retornando-o ao texto

HOLOS
ISSN 1807 - 1600

original (SOARES *et al.*, 1995). Este processo contorna e evita que um intruso intercepte o fluxo de dados para leitura (intruso passivo) ou para modificá-lo (intruso ativo) (Figura 2).

Figura 2 - Processo de criptografia

A criptografia é geralmente baseada em algoritmos matemáticos, que não devem ser confundidos com externografia. Essa se refere à informação "escondida", através de símbolos ou imagens, sejam figuras impressas, em mídias ou até mesmo tatuadas no corpo.

3 TECNOLOGIAS DISPONÍVEIS PARA AMBIENTE SOHO

Ao se pensar em ambiente desprovido de infraestrutura na área de TI e inclusive na necessidade de gerar uma infraestrutura rápida, de baixo custo, é normal se direcionar para as redes *wireless* (redes sem fios). Este padrão de rede não é inseguro, desde que seja devidamente configurado o formato de acesso, no entanto, não possui o mesmo aproveitamento de uma rede cabeada.

Bolzani (2004) afirma que, no sentido mais amplo, as redes domésticas são interconexões de eletroeletrônicos de uso residencial através de um meio que possibilite a troca de dados entre eles. Esse tipo de rede pode possibilitar o controle remoto de equipamentos, a automação de processos e a distribuição de conteúdo digital, como vídeos de alta resolução e som, ou seja, todos os dispositivos ditos como "inteligente".

Campos, Araújo e Moreira (2006) consideram que a opção é a rede sem fio. Porém, comentam ainda, que para se cobrir um ambiente inteiro com uma rede "*wireless* infraestruturada", é necessário o uso de certa quantidade de dispositivos. Observando essa afirmação, pode-se constatar também que o aumento de um equipamento remete a uma nova aquisição de dispositivos (placa ou adaptadores USB – *Universal Serial Bus*), o qual gera o problema a ser contornado: a compatibilidade, pois normalmente não será igual aos já existentes no parque tecnológico. Rubinstein e Rezende (2002) corroboram ao afirmar que diferentes padrões e tecnologias de rede sem fios surgiram para acomodar a vasta gama de aplicação e cobertura de sinal. Assim o avanço tecnológico destes equipamentos diferencia-se sempre dos anteriores.

Além dos processos de transmissão e recepção sem fios, os sinais são geralmente transmitidos por alguma forma especializada, com meios desenvolvidos para tal. Por exemplo: (i) cabos de áudio e vídeo transportam sinais sonoros e de imagens; (ii) os cabos coaxiais, transportam sinais de imagem de sistemas de TV e dados; (iii) cabos par trançado (categoria especial) encaminham sinais de dados e voz; (iv) cabos par trançados telefônicos, carregam sinais de voz. Os cabos ou fios de cobre dos sistemas elétricos foram desenvolvidos para suportar frequências dos sinais de energia elétrica. No entanto, com o advento da tecnologia PLC (*Power Line Communications* – Comunicações por Linha de Força), pode ocorrer todas as transmissões de dados, áudio e vídeo pelo mesmo meio dos cabos desenvolvidos para as frequências elétricas.

HOLOS
ISSN 1807 - 1600

A tecnologia PLC, através da rede de energia elétrica, transporta todos os sinais em alta velocidade numa infraestrutura já pronta, sem custos adicionais com cabos ou fios. Possibilita assim, conectar-se à rede de dados em qualquer ponto de acesso da rede de energia elétrica. Este padrão de tecnologia sem novos fios tem sido alvo de estudo dos ambientes acadêmicos de forma mais discreta. Sendo mais comum no Brasil, o estudo por empresas concessionárias de energia elétrica, como novo mercado entrante para estas, ou até mesmo figurando como atrativo ao cliente.

A recepção do sinal de energia elétrica e a de internet não necessitam de tratamentos adicionais (Figura 3). No interior da residência ou escritório é que o sinal de acesso à internet será convertido através de um adaptador para a rede elétrica, ao invés de empregar cabos para rede de dados ou rede sem fios.

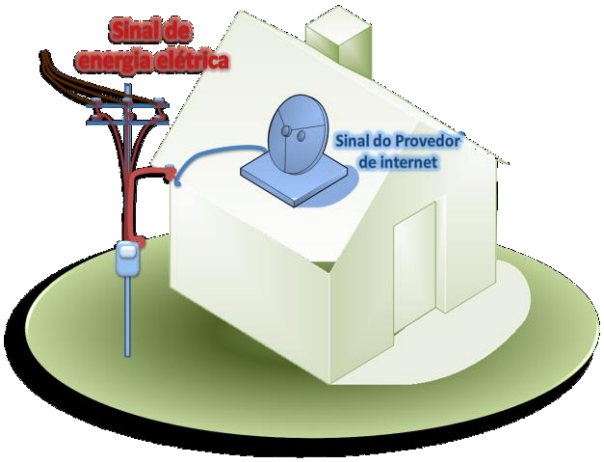

Figura 3 - Recepção do sinal de energia e do provedor de acesso à internet

A recepção do sinal da tecnologia sem fio ou sem novos fios ocorre de mesma forma que ocorrem as tecnologias cabeadas. Seja pelo provedor de acesso a internet da rede cabeada de Televisão (*cable modem* – Modulador e Demodulador a cabo), pela linha telefônica (ADSL modem – modem *Asymmetric Digital Subscriber Line* - modulação Assimétrica da Linha Digital do Assinante) ou através de sinal via satélite (satélite modem), conforme sugere a Figura 3.

Para este estudo não há necessidade de estudar as redes *outdoor* ou redes de acesso de banda larga sobre linhas de energia (*Broadband over Power Lines* - BPL). A rede *indoor* PLC ou rede local é o padrão que atende ao objeto desta pesquisa, que são as redes SOHO e por não tratar-se de uma tecnologia comum será apresentada de forma mais detalhada adiante.

3.1 Redes sem fios

Silva e Souza (2003) argumentam que o padrão de redes sem fios, numa visão geral, pode ser visto em três fases (sondagem, autenticação e associação), necessárias a qualquer cliente deve realizar para obter acesso à rede.

O equipamento na fase de sondagem procura o sinal mais forte, entre as diferentes redes existentes. Após esta etapa realiza-se a autenticação, que pode ocorre de forma simples (sem nenhuma chave de segurança ou métodos complexos de criptografia). No caso de ser necessária uma chave de autenticação, a primeira autenticação deverá ser informada ao sistema “a chave”, bem como o método de criptografia, em alguns casos. Na etapa seguinte estabelece a associação e o acesso àquela rede.

HOLOS
ISSN 1807 - 1600

Peres e Welber (2003) citam que o usuário que optar pelo sistema de autenticação aberto não possuirá qualquer forma de confidencialidade, nem de autenticação de dispositivos, podendo ter problemas de captura de informações, nesse caso, os dados trafegam sem criptografia, onde os dispositivos passam a confiar informações sensíveis diretamente ao atacante, já que neste sistema não existe autenticação dos usuários. A autenticação e utilização de protocolos de criptografia não impedem o atacante, apenas aumenta a complexidade. No entanto, o padrão de rede *wirelles* com autenticação e criptografia está sujeito aos ataques estatísticos, cujo objetivo é descobrir o significado de textos cifrados. Também podem ocorrer ataques de injeção de tráfego, que tenta inserir dados na rede aproveitando pacotes enviados por dispositivo já autenticado, entre outros tipos de ataques que tem por finalidade o acesso à rede (Peres & Welber, 2003).

Outra questão da rede sem fio é qualidade do sinal. Rubinstein e Rezende (2002) comentam que as redes *wireless* têm problemas em compartilhamento do meio, necessita de mecanismos de controle de erro entre os nós e por final colocam também o problema de terminal escondido e exposto. Tais barreiras dificultam a provisão de QoS (*Quality of Service*) nestas redes.

3.2 Redes sem novos fios

O meio de transmissão da tecnologia PLC, rede elétrica, tem por sua natureza, uma capilaridade muito grande para o ambiente em que está inserido, o que viabiliza a disponibilização de sinais de rede de dados por todos os ambientes.

O fato de ser uma tecnologia de transmissão e recepção simétrica torna PLC *indoor* muito atraente, pois a busca no uso alternativo de energia elétrica traz enorme vantagem em relação a uma nova estrutura de cabeamento, considerando o ambiente arquitetônico. Além de ser possível em uma arquitetura já pronta, ela transmite dados em velocidade não encontrada em outras tecnologias mais simples.

Campos, Araújo e Moreira (2007) afirmam que o *HomePlug* (padrão desenvolvido pela *HomePlug Powerline Alliance*) veio para tentar suprir um "vácuo" entre as tecnologias "com fio" e "sem fio". Este protocolo evoluiu para o padrão *HomePlug* AV, o qual foi desenvolvido com intuito de fornecer uma conexão de alta qualidade, mantendo a interoperabilidade com o *HomePlug* 1.0. O padrão *HomePlug* AV utiliza técnicas avançadas de implementação, disponibilizando conexão de 200 Mbps (Mega bits por segundo) e inclui também o padrão de criptografia para segurança de dados em 128 bits (LEMOS, 2011).

O protocolo *HomePlug* utiliza o padrão de transmissão CSMA/CD (*Carrier Sense Multiple Access with Collision Detection* – Acesso múltiplo com detecção de portadora e detecção de colisão) para eliminar e minimizar as colisões. Para realizar as comunicações ponto a ponto é utilizado o protocolo *Token Bus*, que permite o controle e a inserção de novos *hosts*, utilizando o conceito *Plug and Play* (LEMOS, 2011).

Além da questão da largura de banda, o *HomePlug* AV insere na sua engenharia maior imunidade ao ruído elétrico, melhores garantias dos parâmetros QoS, garantindo simultaneamente a interoperabilidade com equipamentos *HomePlug* 1.0 (LEMOS, 2011).

Outra possibilidade de se aproveitar da capilaridade oferecida por esta tecnologia é que como a rede *wireless,* ela se obtém no mesmo espaço de conexão, pois todos os equipamentos

HOLOS
ISSN 1807 - 1600

necessitam de energia para funcionar, sem contar que qualquer projeto elétrico se dispõe de pontos de tomadas por vários espaços de uma residência, *campus* ou escritórios (Figura 4).

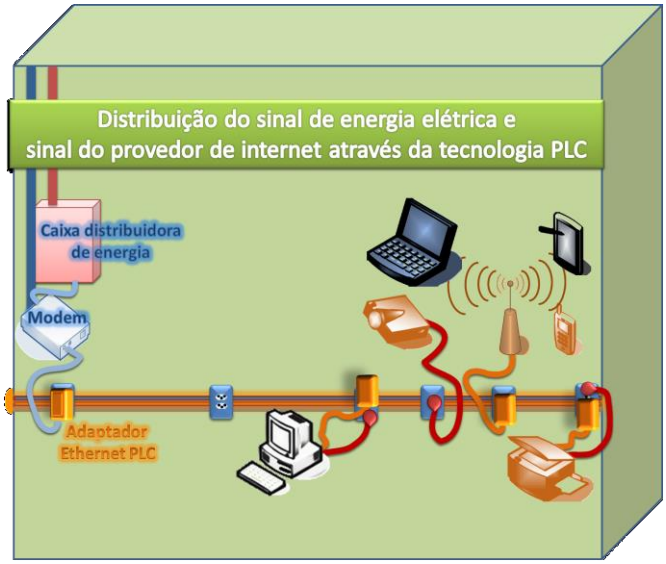

Figura 4 - Distribuição do sinal do provedor de acesso a internet com tecnologia PLC

A qualidade do serviço em PLC é garantida pelas técnicas de controle de acesso do meio, através do protocolo CSMA (*Ethernet*) e pela divisão ortogonal da frequência (*Orthogonal frequency-division multiplexing* - OFDM).

É necessário apresentar também que a rede *Power Line* não interfere na velocidade oferecida pelo provedor de acesso, ela é uma oportunidade de melhoria da rede LAN possibilitando acesso mais rápido a arquivos compartilhados, impressoras e etc.

3.3 Testes em acesso com rede PLC e rede sem fio

No período de três dias foram realizados testes entre três equipamentos *desktop*, com a mesma configuração, sendo um conectado através de tecnologia da rede PLC, outro conectado com rede sem fio e o terceiro conectado com a rede de cabos de cobre em par trançado. Os equipamentos estavam configurados no seguinte cenário:

- todos os equipamentos na mesma rede de domínio de *broadcast*, dentro da mesma faixa IP, conectados aos adaptadores de rede sem fio e rede PLC, por meio de rede cabeada em cabo de cobre par trançado (Cat5e);

- o equipamento de radio-transmissão para acesso a rede *wireless* configurado em função *access point*, com suporte a IEEE802.11g/b, taxa de transferência 150 Mbps, frequência 2,4 Ghz e alcance de 100 m;

- equipamentos adaptadores PLC/*Ethernet,* configurado em função *access point*, com protocolo *Home Plug* AV, com taxa de transferência 200 Mbps e alcance de 300m;

- os equipamentos estavam dispostos próximos: a rede *wireless* distava entre o *desktop* e o ponto de acesso de 30 cm, com visada direta, a rede PLC distanciava entre os adaptadores *ethernet* PLC de acesso à rede e o adaptador de modulação do *desktop* de 90 cm;

- todos os equipamentos de modulação de sinal (adaptador *ethernet* PLC e o *access point wireless* recebiam sinal da mesma rede cabeada que conectava o terceiro equipamento *desktop*;

- o *layout* dos equipamentos encontrava-se disposto na seguinte forma: (i) o primeiro equipamento (Eqp1), conectava-se diretamente a rede cabeada; (ii) o segundo equipamento (Eqp2), recebia sinal através do *access point wireless*; (iii) o terceiro equipamento conectava-se a rede através do adaptadores *ethernet* PLC, também configurados em modo *access point* (Figura 5).

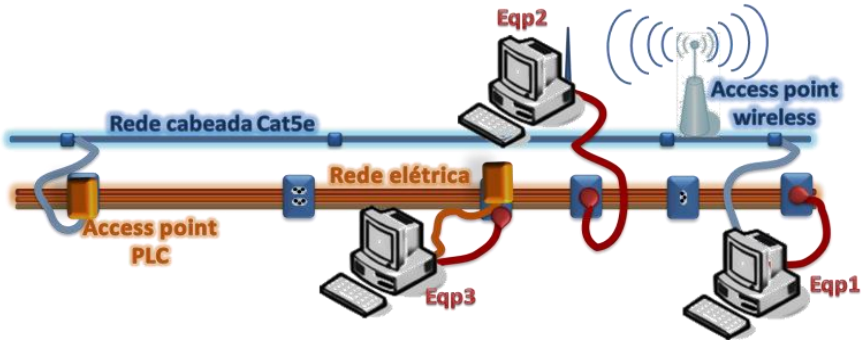

Figura 5 - *Layout* dos testes

Os testes ocorreram durante três dias, no período compreendido entre 14 h horas e 21 horas. Tiveram como padrão o acesso ao equipamento conectado à rede cabeada (Eqp1) pelos outros dois equipamentos (Eqp2 e Eqp3), e a média de testes (*averange*) manteve-se constante, com o download de um arquivo de 126 Mb. A conexão entre o equipamento da rede PLC realizava o *download* na metade do tempo do equipamento da rede *wireless*, dependendo das condições de tráfego da rede oscilando os dois acessos, ou seja, caso houvesse um tráfego maior na rede aumentava o *delay* para o equipamento PLC e para o equipamento *wireless*.

Para eliminar as dúvidas, foi montada uma rede, através do roteador local, com IP classe C (192.168.1.0), isolada das interferências do domínio de colisão da rede com acesso ao ambiente externo (internet), no mesmo *layout* descrito na Figura 5, onde o *access point* passou a realizar as funções de roteador, sem conexão com a internet, nem a rede local. Nessa ocasião, foi também realizado o comando "ping -n 100 192.168.1.50" (Eqp1) conectado diretamente ao roteador pelos demais equipamentos.

O sinal do equipamento ligado pelo adaptador PLC teve 0% de perda e mínimo de 3 metros por segundo e máximo de 5 metros por segundo (Figura 6). O sinal do equipamento com acesso pela rede sem fio teve 0% de perda e mínimo de 1 metro por segundo e máximo de 66 metros por segundo (Figura 7).

```
Resposta de 192.168.0.50: bytes=32 tempo=3ms TTL=128
Resposta de 192.168.0.50: bytes=32 tempo=3ms TTL=128
Resposta de 192.168.0.50: bytes=32 tempo=3ms TTL=128
Resposta de 192.168.0.50: bytes=32 tempo=3ms TTL=128
Resposta de 192.168.0.50: bytes=32 tempo=3ms TTL=128
Resposta de 192.168.0.50: bytes=32 tempo=3ms TTL=128

Estatísticas do Ping para 192.168.0.50:
    Pacotes: Enviados = 100, Recebidos = 100, Perdidos = 0 (0% de
             perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 3ms, Máximo = 5ms, Média = 3ms
```

Figura 6 - Resposta do comando *ping* no equipamento com PLC

```
Reply from 192.168.0.50: bytes=32 time=3ms TTL=128
Reply from 192.168.0.50: bytes=32 time=1ms TTL=128
Reply from 192.168.0.50: bytes=32 time=1ms TTL=128
Reply from 192.168.0.50: bytes=32 time=1ms TTL=128
Reply from 192.168.0.50: bytes=32 time=5ms TTL=128
Reply from 192.168.0.50: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.0.50:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 66ms, Average = 8ms
```

Figura 7 - Resposta do comando *ping* no equipamento com *wireless*

Para garantir a capacidade e integridade da rede, na configuração sem acesso a ambientes externos, foi conectado o equipamento que antes estava conectado pela rede *wireless* diretamente no roteador, desabilitado a rede sem fio deste equipamento e realizado outro "*ping"* no mesmo padrão, obtendo 0 % de perda e Mínimo e Máximo ficaram com zero metro por segundo (Figura 7).

Na ocasião não reduziu-se a carga da rede elétrica, nem isolou-se a rede de energia geral do ambiente de testes.

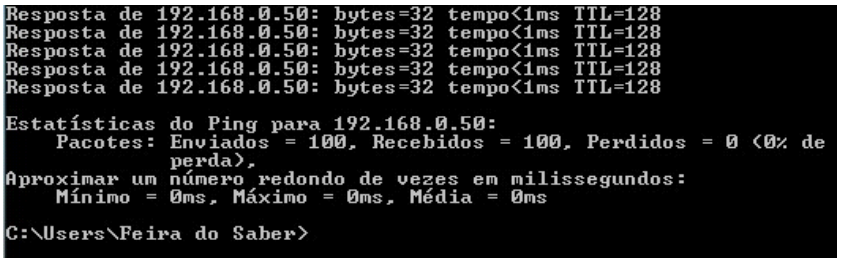

Figura 8 - Resposta do comando *ping* no equipamento conectado diretamente no roteador

Ficou comprovado desta forma, que a resposta dos equipamentos da rede *wireless* e da rede PLC, é diferente e a rede PLC mantem-se dentro de um padrão na transmissão (*average*), com menores taxas de erros entre os equipamentos. E ainda, com o último teste foi verificado que a rede respondia coerentemente ao que se pretendia: os erros e o *delay* de transmissão são das respectivas tecnologias, cabendo à tecnologia sem fio a maior taxa de erro e de atraso de resposta.

3.4 Comparação entre o acesso à rede com PLC e rede wireless

A tecnologia PLC, por ser cabeada e também utilizar criptografia no seu padrão de transmissão, apresenta-se mais segura que a rede *wireless*. No entanto, a rede sem fios é muito praticada hoje em dia. Outro aspecto favorável à tecnologia PLC é que essa pode ser instalada facilmente por qualquer usuário, devido à tecnologia *plug and play*.

Ao comparar os parâmetros entre as redes PLC e *Wireless* pode-se afirmar, pelo demonstrado até o presente estudo, que a rede PLC possui maior segurança em relação à rede sem fio. Peres e Welber (2003) concordam com a presente pesquisa ao afirmar que a utilização de uma rede sem fios implica em alguns aspectos especiais em relação à segurança comparando das redes cabeadas. Conforme demonstra a Tabela 1.

Tabela 1: Comparação entre as tecnologias de conexão de redes sem fio e redes PLC

	Limite físico	Controle do meio	Controle de acesso físico	Taxa de transmissão
Wireless	Sem limites	Por meio de regras e protocolos	Inviável	24 até 300 Mbps
Cabo da rede elétrica	Todos pontos de acesso a rede elétrica	Limita-se a extensão do cabeamento	Apenas dispositivos conectados	85 Mbps até 500 Mbps

Campos *et al.* (2007) fortalece o que foi demonstrado aqui, ao estudar outros

pesquisadores e realizar testes de compatibilidade da tecnologia PLC e de suas características em três cenários distintos (uma residência monofásica e dois prédios trifásicos), concluindo que este tipo de tecnologia é mais viável do que a rede *wireless*. Após rever a literatura e analisar os testes, Campos *et al.* (2007) reafirmam que a tecnologia estudada (ainda no *HomePlug* 1.0) atende perfeitamente ao seu intuito, sendo uma alternativa para as redes SOHO, podendo, contudo, ser utilizada em conjunto com a tecnologia *wireless*, para maior cobertura do sinal, se houver necessidade de maior mobilidade.

4 PROPOSTA DE SEGURANÇA EM AMBIENTE SOHO

A tecnologia PLC, apresenta-se de forma eficaz, como uma opção para as redes sem fio, em relação à qualidade, avanço tecnológico e segurança. Convém ressaltar, que ambas as tecnologias (*wireless* e PLC) são capazes de atender a uma rede SOHO.

As duas tecnologias aqui mencionadas possuem seu grau de criptografia e suas regras de segurança. Posto assim, a viabilidade técnica é o fator em que a tecnologia PLC sobressalta-se na frente, com novos investimentos e pesquisas, em relação à tecnologia *wireless*.

É notório que as redes SOHO, são concebidas sem distinção de segurança independentemente da tecnologia implementada. Schetina *et al.* (2002) colaboram com esse pensamento e, sem mencionar a tecnologia, defende os princípios tecnológicos em que uma rede SOHO deve ser concebida: (i) *firewall* – com regras que traduzam os endereços da rede interna e externa e que o equipamento com esta finalidade deve ter confiabilidade; (ii) *software* de análise de *log* dos *firewalls* – que dará pelo menos uma noção do tráfego da rede, com possibilidade de geração de gráfico, pois tal fator será um facilitador para o administrador; (iii) todos os equipamentos *desktop* devem ter instalado *firewall* e antivírus, com atualização automática de assinatura de vírus; (iv) se a rede for contemplada com servidor de Protocolo de Transferência de Arquivos (*File Transfer Protocol* - FTP) ou e-mail, deverá também ter um antivírus específico instalado; (v) treinamento para os usuários – as boas práticas de segurança surgem da conscientização de processo de criação de senhas eficientes e normas de conduta na rede; (vi) boas regras de segurança - as regras de segurança não devem gerar problemas de acesso à rede interna ou externa, mas deve impedir acesso a sites desnecessários, bem como tentativas de invasões ou técnicas como *ping da morte*, inundação e outras.

E no caso especial de prestação de serviço com acesso remoto, cabe a utilização da técnica de VPN. Neste caso, o cliente deverá estar também com o MAC devidamente cadastrado na rede, onde o gateway servidor de VPN está ativo.

Desta mesma forma, vale ratificar ainda que a utilização de VPN, dentro da própria rede SOHO, não é inviável, pode ser utilizada para acessar servidor de arquivos, de *e-mails* e outros ativos importantes da rede. Neste caso para não degradar muito o sinal, o emprego dos recursos do IPSec no modo transporte, tornar-se-ia muito útil e atraente, não sendo necessário o modo túnel, de cuja diferença encontra-se na criptografia do conteúdo. Na transmissão em modo transporte somente o conteúdo é criptografado, já no modo túnel todo o conteúdo, incluindo o cabeçalho do pacote será criptografado e este pacote receberá um endereçamento novo através do protocolo IPSec.

5 CONSIDERAÇÕES FINAIS

Nesta pesquisa não se intencionou desqualificar as redes *wireless*, apenas buscou-se mostrar a possibilidade de empregar outra tecnologia, que vem despontando no mercado com maior segurança.

A informação, independentemente do tamanho da empresa, é dos principais ativos. Neste sentido, cabe afirmar que a segurança da informação das prestadoras de serviço deve também ser considerada como um ativo prioritário, principalmente visando à segurança da empresa contratante de serviços.

Posto assim, a questão de rede SOHO com tecnologia PLC e a implementação de regras de segurança, torna a rede capaz de atender o mínimo necessário para as empresas que se inserem neste caminho de prestação de serviço, visto que, além de apresentar equipamentos viáveis também utiliza criptografia e o sinal é contido na rede elétrica.

REFERÊNCIAS BIBLIOGRÁFICAS

1. BOLZANI, C. A. M. (2004). *Residências Inteligentes: Domótica; Redes Domésticas; Automação Residencial* (1ª ed.). São Paulo: Editora livraria da Física.
2. CAMPOS, A. L. P. S.; ARAÚJO, L. M. & MOREIRA, R. C. O. (2006). *Investigação experimental da vazão de uma rede local de computadores HomePlug 1.0.* Holos, 3, 37-43.
3. _____. (2007). A*nálise de desempenho da tecnologia homeplug 1.0 em ambientes domésticos e não domésticos.* Holos, 2, 42-41.
4. Ed. GLOBO (2007). Revista Época: *Você quer mesmo quebrar paradigmas?.* São Paulo, SP: Gehringer, M.
5. LEMOS, J. P. G. (2011). A*valiação da rede Homeplug para suporte de aplicações industriais.* Tese de mestrado, Faculdade de Engenharia da Universidade do Porto. Porto, Lisboa, Portugal.
6. PERES, A. & WEBER, R. F. (2003, maio). *Considerações sobre Segurança em Redes Sem Fio IEEE 802.11.* Anais do 21º Simpósio Brasileiro de Redes de Computadores, Natal, RN, Brasil, 2.
7. RUBINSTEIN, M. G. & REZENDE, J. F. (2002, maio). *Qualidade de Serviço em Redes 802.11*. Anais do XX Simpósio Brasileiro de Redes de Computadores, Búzios, RJ, Brasil.
8. SARLO DA SILVA, L. (2003). *Virtual Private Network* (1ª ed). São Paulo: Novatec
9. SCHETINA, E.; GREEN, K. & JACOB, C.. (2002). *Sites seguros: aprenda a desenvolver e construír* (1ª ed). Rio de Janeiro/RJ: Campus.
10. SILVA, G. M. & SOUZA, J. N.. (2003, maio). *Uma análise dos mecanismos de segurança de redes locais sem fio e uma proposta de melhoria*. Anais do 21º Simpósio Brasileiro de Redes de Computadores, Natal, RN, Brasil, 1.
11. SOARES, L. F. G.; LEMOS, G. & COLCHER, S. (1995). *Redes de Computadores das LANs MANs e WANS as Redes ATM.* Rio de Janeiro: Campus Ltda.