14
ISSN 1982-8195

CADERNOS ANP

POLÍCIA FEDERAL

APLICAÇÕES DE REDES SEM FIO AD HOC MÓVEIS EM OPERAÇÕES POLICIAIS

José Helano Matos Nogueira

Brasília - DF
2012

CADERNOS ANP

APLICAÇÕES DE REDES SEM FIO *AD HOC* MÓVEIS EM OPERAÇÕES POLICIAIS

14
ISSN 1982-8195

CADERNOS ANP

Brasília, n. 14, 2012.

ISSN 1982-8195

MJ - Departamento de Polícia Federal
Diretoria de Gestão de Pessoal
Academia Nacional de Polícia

JOSÉ HELANO MATOS NOGUEIRA

APLICAÇÕES DE REDES SEM FIO *AD HOC* MÓVEIS EM OPERAÇÕES POLICIAIS

Primeiro Lugar no II Concurso Nacional de Monografias em Segurança Pública da Academia Nacional de Polícia - Curso de Gestão de Políticas de Segurança Pública, em 2009.

Brasília - DF
2012

CADERNOS ANP

Brasília, n. 14, 2012.
ISSN 1982-8195

Projeto Gráfico, Capa e Editoração: Roberto Carlos de Sousa, Guilherme Henrique Braga de Miranda e Gilson Matilde Diana

1ª Edição Julho/2012

Tiragem: 350 exemplares

Nogueira, José Helano Matos.

APLICAÇÕES DE REDES SEM FIO *AD HOC* MÓVEIS EM OPERAÇÕES POLICIAIS – Brasília: Academia Nacional de Polícia, 2012, 71 páginas.

Monografia para a obtenção do título de Especialista em Gestão de Política de Segurança Pública.

ISSN 1982-8195

1. Redes de computadores sem fio. 2. Redes *ad hoc*. 3. Rede móvel. I. NOGUEIRA, José Helano Matos. II. Academia Nacional de Polícia, Pós-Graduação em Gestão de Política de Segurança Pública. III. Título.

Correspondência Editorial
ACADEMIA NACIONAL DE POLÍCIA
ESCOLA SUPERIOR DE POLÍCIA
DF 001 - Estrada Parque do Contorno, Km 2
Setor Habitacional Taquari, Lago Norte - DF - CEP 71559-900

Sumário

RESUMO

Este trabalho se insere na área de novas tecnologias computacionais aplicadas, mais especificamente na subárea de rede de computadores sem fios e tem como objetivo principal propor a utilização de redes sem fios *ad hoc* móveis em algumas atividades da Polícia Federal, notadamente em situações temporárias: emergência, falta de infra-estrutura computacional, falta de tempo, necessidade de mobilidade, procedimento investigativo. Nesses casos, pode ser feito uso desta tecnologia para transferir dados, sons e imagens, compartilhar recursos, receber e enviar mensagens ou arquivos. Para esse tipo de cenário, está sendo proposta a montagem de uma rede sem fios *ad hoc* (chamada AdHocPF) na Superintendência Regional do Departamento de Polícia Federal no Estado do Ceará (SR/DPF/CE) visando analisar e avaliar o uso desse tipo de arquitetura de redes computacionais na práxis diária das atividades policiais. Ademais, nesse novo paradigma proposto, espera-se que seja possível obter uma redução dos custos operacionais para concretização das tarefas e missões, pois não são necessários grandes recursos e investimentos: cabos, fios e demais pontos fixos como no caso das redes cabeadas, nem dos pontos de acesso e roteadores dedicados se comparado com as redes sem fios tradicionais.

Palavras-Chave: Rede de computadores sem fios. Rede *ad hoc*. Rede móvel.

ABSTRACT

The work is inserted in the area of new applied computational technology, more specifically in the sub-area of wireless computer networks it has as a main objective and propose for the use of mobile *ad hoc* networks in some activities of the Brazilian Federal Police, mainly in temporary situations: emergency, computational infrastructure absence, time absence, mobility need, and investigative procedures. In these cases, it can be made use of this technology to transfer data, sounds and images, to share resources, to receive and to send messages or files. For this scenery type, the assembly of a mobile *ad hoc* computer network (called AdHocPF) at the Regional Superintendence of Federal Police Department at Ceará State (SR/DPF/CE) is being proposed to analyze and to evaluate the use of that type of computer networks architecture in the daily police activities praxis. Besides, in this new proposed paradigm, it is waited that is possible to obtain a reduction in the operational tasks and mission costs, because it is not necessary great resources and investments: cables, wires and other fixed points as in the case of wire networks, nor of the access points and gateways dedicated if it is compared with traditional wireless networks.

Keywords: Wireless computer network. *Ad hoc* network. Mobile network.

INTRODUÇÃO

As redes sem fios ganharam grande popularidade pela mobilidade, facilidade de instalação e possibilidade de uso em diversos ambientes, tais como: universidades, aeroportos, hospitais, livrarias, supermercados, restaurantes, cafés, residências e empresas públicas ou privadas dos mais variados tipos e tamanhos. Devido à facilidade encontrada nessa tecnologia, o uso vem crescendo rapidamente, pois na montagem de uma rede com fios (cabeada) é preciso a instalação de cabos e pontos de rede por toda a parte, caso haja necessidade de várias opções de conexão. Em determinados ambientes torna-se necessário, inclusive, quebrar paredes, pisos e até o teto, além de ser preciso utilizar ferramentas para testes, medição e colocação dos cabos. Enquanto isso, para montar uma rede sem fios nos padrões tradicionais, ou seja, com infra-estrutura, são necessários apenas os dispositivos (computadores de mesa ou portáteis, assistentes pessoais de dados, celulares) com as respectivas placas de rede sem fios e pontos de acesso.

Com o passar do tempo, percebeu-se que um dos principais motivos para o crescimento das redes sem fios é a praticidade e rapidez na instalação e manutenção. Com a introdução das novas tecnologias sem fios, foram criados, também, novos paradigmas de comunicação, onde diversos dispositivos podem comunicar-se sem a necessidade de muitos equipamentos e vultosos investimentos. Nesse novo contexto de tecnologia com ondas de radiofreqüência trafegando no ar, surgem as redes sem fios sem infra-estrutura, conhecidas como redes *ad hoc*. As redes *ad hoc* são ainda mais fáceis de serem instaladas do que as redes sem fios tradicionais, pois não precisam de estações base ou pontos de acesso. Normalmente elas são utilizadas para situações temporárias, ou seja, por pouco tempo, alguns minutos, horas ou poucos dias. A característica de mobilidade dessas redes fornece um ganho substancial quando é preciso serem realizadas tarefas que exijam deslocamento, flexibilidade e comunicação a poucos metros de distância. Essas redes sem fios de caráter temporário que possuem essa mobilidade são também conhecidas como redes sem fios *ad hoc* móveis ou simplesmente MANET (*Mobile Ad Hoc Networks*). Um bom exemplo da utilização e praticidade das MANET no contexto mundial atual é a tecnologia *Bluetooth*, já bastante utilizada e difundida comercialmente em vários equipamentos, desde dispositivos eletrônicos simples como rádios, agendas, fones de ouvido, celulares, até computadores mais potentes.

Portanto, esse trabalho se insere na área de novas tecnologias computacionais aplicadas, mais especificamente na subárea de rede de computadores sem fios e tem como objetivo principal propor a utilização de redes sem fios *ad hoc* móveis em algumas atividades da Polícia Federal que se enquadram no contexto de uso desse tipo de rede, notadamente em situações

temporárias: casos de emergência, falta de infra-estrutura computacional, falta de tempo, necessidade de mobilidade. Nesses cenários, é possível utilizar essa tecnologia para transferir dados, sons e imagens, compartilhar recursos, receber e enviar mensagens ou arquivos. Se em algum momento da comunicação houver a disponibilidade de outra rede, como por exemplo, a *Internet*, a rede *ad hoc* móvel poderá se conectar e utilizar os recursos e serviços fornecidos por essa nova conexão sem maiores problemas. Para essas situações, está sendo proposta a montagem de uma rede sem fios *ad hoc* (chamada AdHocPF) no Setor Técnico-Científico da Superintendência Regional do Departamento de Polícia Federal no Estado do Ceará (SETEC/SR/DPF/CE) visando analisar e avaliar o uso desse tipo de arquitetura de redes computacionais na práxis diária das atividades policiais. Durante a fase de testes a AdHocPF também foi montada no Laboratório de Redes e Segurança da Universidade Estadual do Ceará (LARCES/UECE). Nesse novo paradigma proposto, espera-se que seja possível obter uma redução dos custos operacionais para concretização das tarefas e missões policiais, haja vista não ser preciso investimentos em: cabos, fios e demais pontos fixos como no caso das redes cabeadas, nem dos pontos de acesso e roteadores dedicados no caso das redes sem fios tradicionais. Ademais, com esse trabalho busca-se uma melhoria na qualidade e na eficiencia e eficácia dos serviços de segurança pública fornecidos pela Polícia Federal para a sociedade.

No primeiro capítulo é realizado um levantamento bibliográfico sobre como estão os estudos e pesquisas sobre redes sem fios, no contexto brasileiro e mundial, desde a evolução dos computadores às redes de computadores, passando pelas tecnologias sem fios, para em seguida categorizá-las. No segundo capítulo são tratadas especificamente as redes sem fios *ad hoc* móveis com suas características de mobilidade, temporaneidade e alcance. No terceiro capítulo é criado um modelo de arquitetura de rede *ad hoc* móvel, a AdHocPF, usando máquinas, equipamentos e programas computacionais disponíveis na Criminalística do SETEC/SR/DPF/CE e no LARCES/UECE. Em seguida são fornecidas as etapas para criação e configuração da rede AdHocPF. O capítulo quarto, por sua vez, aborda a concretização do uso da AdHocPF em aplicações policiais, bem como apresenta os cenários de teste e os desafios enfrentados. Em seguida, são apresentadas as considerações finais e os trabalhos futuros.

1 REDES SEM FIOS

A popularização das redes de computadores, notadamente a *Internet*, universo então conhecido apenas nos meios acadêmicos e militares, acelerou os avanços tecnológicos chegando ao que hoje conhecemos como redes sem fios.

1.1 Evolução dos computadores isolados às redes de computadores

O mundo vem passando por verdadeiras revoluções tecnológicas no decorrer dos tempos. Na atualidade, as principais conquistas tecnológicas se deram no campo da Ciência da Computação com a aquisição, o processamento e a distribuição da informação cada vez mais rápida, eficiente e popularizada. Apesar da indústria de informática ainda ser jovem em comparação com outros setores industriais (por exemplo, o de telefonia, o de automóveis etc.) foi simplesmente espetacular o progresso que os computadores conheceram em um curto período de tempo. Vale destacar que somente em 1945 surgiu o primeiro computador, o ENIAC (*Electronic Numerical Integrator And Calculator*), ou seja, apenas 64 anos atrás. Durante as duas primeiras décadas de existência, havia basicamente grandes computadores (*mainframes*) com arquitetura e sistemas computacionais fortemente acoplados (altamente centralizados). De uma maneira geral esses computadores ficavam instalados em um salão com janelas de vidro, através das quais as pessoas que não trabalhavam na área podiam contemplar estupefatos, aquela máquina eletrônica. Segundo Tanenbaum (2003), entre outras inovações, foi possível acompanhar a instalação das redes de telefonia em escala mundial, a invenção do rádio e da televisão, o nascimento e o crescimento sem precedentes da indústria de informática e o lançamento dos satélites de comunicação. No entendimento de Comer (2007), com o progresso tecnológico, as áreas de telefonia e informática têm convergido rapidamente e são cada vez menores as diferenças entre coleta, transporte, armazenamento e processamento de informações. Empresas e corporações com centenas de lojas e escritórios dispersos por uma extensa área geográfica em vários países podem, com um simples apertar de um botão ou um clicar de *mouse*, examinar o desempenho das filiais nos locais mais remotos do globo terrestre.

À medida que cresce a capacidade de tratar com a informação, torna-se maior a demanda por formas eficientes e sofisticadas de gestão dessa informação. Com isso, o conceito de "Centro de Processamento de Dados – CPD", com uma sala contendo um grande computador onde os usuários levavam trabalhos para processamento, está obsoleto. O paradigma de tratamento dos dados e informação que utiliza um único computador atendendo a todas as demandas computacionais de uma organização foi substituído pelo das redes de

computadores, nas quais os trabalhos são realizados por vários computadores separados, mas interconectados através de algum meio físico (KUROSE; ROSS, 2006).

Já é possível compreender que as redes de computadores são e continuarão sendo por muito tempo uma tecnologia de grande relevância para todo tipo de organização, inclusive instituições de segurança pública e militares. Logo, é preciso definir, para o contexto desse trabalho, o que vem a ser uma rede de computadores de acordo com os autores e pesquisadores renomados na área. Existem diversas definições possíveis para redes de computadores, umas simples e outras complexas, mas em geral há uma harmonia entre essas definições. Esta pesquisa seguirá em consonância com Tanenbaum (2003) e Comer (2007) que definem uma rede de computadores como um conjunto de computadores autônomos interconectados que se comunicam por algum meio físico. Nesse caso, dois ou mais computadores estão interconectados quando podem trocar informações. Essa conexão não precisa ser feita por fios de cobre; também podem ser utilizadas fibras óticas, microondas, ondas de infravermelho e satélites de comunicações, pois existem redes de computadores de diversos modelos, tamanhos e formas.

1.2 Tecnologia sem fios

A tecnologia de sistema de comunicação sem fios não é uma idéia nova. No início do século XX, o físico italiano Guglielmo Marconi demonstrou como funcionava um telégrafo sem fios que transmitia informações de um navio para o continente por meio de código morse. Os modernos sistemas digitais sem fios têm um desempenho bem melhor, mas a idéia básica é a mesma. Segundo Kwok e Lau (2007) um sistema de comunicação consiste em um transmissor e um receptor conectados por algum meio físico de comunicação. Exemplos desses meios incluem cabo de telefone, cabo coaxial, fibra óptica e freqüência de rádio (RF). As redes sem fios operam basicamente através de ondas de radiofreqüência como meio de transmissão. Elas estiveram em desenvolvimento durante vários anos e o primeiro padrão, o IEEE 802.11, foi criado em meados de 1997.[1]

Independentemente do potencial de crescimento dos equipamentos sem fios, é evidente que as redes sem fios e os seus respectivos serviços móveis têm um grande alcance. Com o passar dos tempos os avanços em tecnologia de comunicações sem fios propiciaram a conexão de vários tipos de dispositivos para as mais variadas aplicações. Isso possibilita controle, acesso e informação compartilhada entre os dispositivos aumentando a familiaridade e a experiência dos usuários com essa nova tecnologia. O crescimento das redes sem fios e dos respectivos meios de acesso permitirão que haja comunicação entre os mais variados tipos de equipamentos portáteis. Todos esses dispositivos poderão vir no futuro com algum tipo de interface sem fios embutida (DIXIT; PRASAD, 2005). Isso vai requerer muitas pesqui-

1 Maiores detalhes sobre esse padrão podem ser encontrados em Gast (2002), Flickenger (2003) e Walke; Mangold; Belermann (2006).

sas em vários aspectos da área de redes de computadores sem fios, desde a transmissão, o desempenho, a conectividade até valores morais e éticos de segurança e privacidade na rede. Embora atualmente haja vários equipamentos portáteis manuais como celulares, PDAs e iPODs, imagine uma rede sem muitas complicações de instalação e com mobilidade de tal forma que possa permitir que uma pessoa, um grupo de pessoas ou toda uma organização possam ter conectividade e controle sem fios de um ou mais dispositivos eletrônicos. Essa é a motivação básica para o uso das redes sem fios.

Antes de propor aplicações e prover investimentos nessa nova tecnologia de comunicação sem fios é necessário fazer um estudo mais detalhado sobre os custos e benefícios. Conforme relatado nas pesquisas de Webb (2007) quase toda atividade no mundo das comunicações sem fios requer um olhar mais acurado. Os usuários que estão decidindo comprar equipamentos precisam avaliar os serviços oferecidos e a viabilidade do investimento nessa nova tecnologia. Os fabricantes por sua vez precisam decidir quais as áreas terão prioridades, as atividades de pesquisa a serem incentivadas, as tecnologias e os dispositivos a serem desenvolvidos e transformados em produtos finais. Por outro lado, os meios acadêmicos precisam entender quais áreas necessitarão os maiores avanços e conseqüentemente ensejarão mais pesquisa. É preciso fazer previsões e projetar cenários para as aplicações, pois existem muitos casos de insucesso devido a erros de avaliação. Um exemplo de previsão ruim é o caso do Irídium (telefone via satélite) onde o número de usuários que estariam preparados para o pagamento desse sistema de telefonia internacional seria bastante grande e cobriria todos os investimentos em poucos anos, o que de fato não ocorreu e o projeto fracassou.

De uma maneira geral as redes sem fios têm muitas utilidades conforme já relatado, desde o uso comum como escritório portátil até mesmo aplicá-las em situações policiais ou militares. Qualquer pessoa com um *notebook* e um modem sem fios pode simplesmente ligar o computador e se conectar, como se o computador estivesse ligado a uma rede com fiação (NIEBERT *et al*, 2007). Conforme mencionado em Kurose e Ross (2006), com algumas adaptações para esse trabalho é possível identificar, genericamente, os seguintes elementos em uma rede sem fios:

a) **Nós sem fios** (dispositivos, estações, terminais, *hosts*). Assim como nas redes cabeadas (com fios), os nós são equipamentos finais que executam processos e programas na camada de aplicação. Nesse caso, um nó sem fios pode ser um computador de mesa, um *notebook*, um *palmtop*, um Assistente Pessoal de Dados – PDA, ou mesmo um celular. Os nós podem ser fixos ou móveis, no caso dos dispositivos portáteis.

b) **Estação base**. A estação base é uma parte essencial para uma rede sem fios com infra-estrutura, pois ela é a responsável pelo envio e recebimento de dados (i.e. pacotes) de um nó sem fios para outro que está associado com a estação. Quando se usa o termo estar

"associado" significa dizer que o nó está dentro do alcance de comunicação da estação base e que o nó usa a estação base para retransmitir dados entre ele e a rede. Os pontos de acesso em uma rede local sem fios (padrão 802.11) e as torres de celulares são exemplos de estação base. Normalmente, uma estação base é encarregada da coordenação da transmissão de vários nós sem fios os quais fazem parte da infra-estrutura. Na Figura 1, a estação base está conectada à rede maior (e. g. *Internet*, rede local corporativa, rede telefônica) e, portanto, funciona como uma retransmissora de camada de enlace entre o nó sem fios e o resto do mundo com o qual esse nó se comunica.

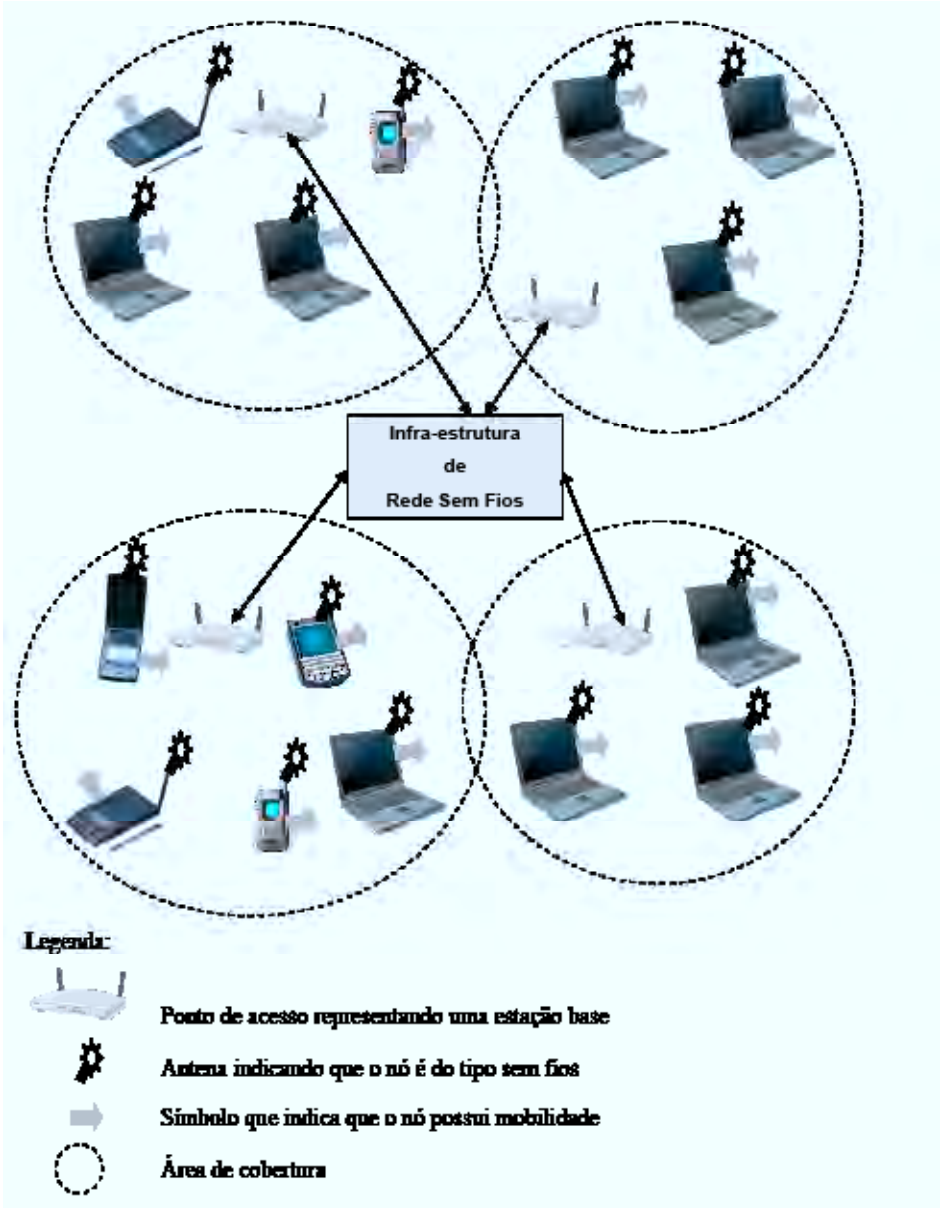

Figura 1 – Elementos de uma infra-estrutura de rede sem fios

c) **Enlace de comunicação sem fios**. Um nó se conecta a uma estação base ou a um outro nó por meio de um enlace de comunicação sem fios. As tecnologias que executam esses mecanismos de comunicação podem ter diferentes taxas de transmissão e podem transmitir dados e informações a diferentes distâncias. Esses mesmos enlaces sem fios podem ser utilizados para conectar roteadores, pontes, comutadores e outros equipamentos de rede. A Figura 1 representa uma infra-estrutura de rede sem fios onde os enlaces se conectam aos nós localizados na borda da rede de maior porte (alcance).

Dessa forma, podemos concluir que a infra-estrutura de rede é a rede de maior alcance, com a qual um nó sem fios pode se comunicar. Nesse mesmo sentido, quando vários nós estão associados com uma estação base, em geral diz-se que estão operando em modo de infra-estrutura, já que todos os serviços tradicionais de rede (por exemplo, tradução e atribuição de endereço, roteamento) são fornecidos pela rede com a qual estiverem conectados por meio da estação base. Por outro lado, quando os nós sem fios não dispõem de nenhuma infra-estrutura com a qual se conectar diz-se que a rede é do tipo *ad hoc*. Na rede *ad hoc* a ausência da infra-estrutura faz com que os próprios nós venham a prover os serviços necessários, tais como roteamento, endereçamento e outros serviços que seriam fornecidos pela infra-estrutura. As redes *ad hoc* serão objeto de estudo nas seções e capítulos seguintes.

Considerando que se for feita a substituição de uma rede cabeada por uma sem fios padrão 802.11 nos moldes referenciados por Gast (2002), Walke, Mangold e Belermann (2006), uma placa de rede sem fios poderia substituir as placas da rede cabeadas sem maiores complicações, pois na camada de rede ou acima dela, não haveria praticamente nenhuma mudança. Isso leva a deduzir que as pesquisas devem se concentrar na camada de enlace, pois, nessa camada há grandes diferenças entre uma rede com e sem fios. (FLICKENGER, 2003).

Para se aplicar redes sem fios em qualquer tipo de tarefa deve-se levar em consideração algumas nuances e fatores relevantes para o uso eficiente e eficaz desse tipo de tecnologia. Não é objetivo desse trabalho aprofundar as discussões sobre as vantagens e desvantagens do uso das tecnologias sem fios. Todavia, o momento é oportuno para levantar alguns alertas já comentados por alguns autores, destacando-se os trabalhos realizados por Nogueira (2004), Kurose e Ross (2006) que apresentam didaticamente algumas dessas realidades conforme pode ser evidenciado a seguir:

Vantagens da Rede Sem Fios

- Mobilidade

Os sistemas de redes locais sem fios podem ser transportados de um local para outro, fornecendo aos usuários acesso à informação em tempo real, em qualquer lugar, dentro ou fora das organizações.

- Instalação rápida e simples

A instalação de uma rede sem fios pode ser simples, rápida e fácil, além de eliminar a necessidade de atravessar cabos através de paredes, pisos, tetos e até entre andares de edifícios.

- Flexibilidade

A tecnologia sem fios permite que as redes cheguem a locais onde os cabos não conseguem ir.

- Custo Reduzido

Embora o custo inicial de uma rede sem fios pareça ser maior que de uma rede cabeada, nos dias de hoje isso não é verdade. A instalação e o ciclo de vida das redes sem fios são significantemente mais rápidos reduzindo drasticamente os custos e tornando-as muito mais atrativas e baratas do que as redes com fios.

- Escalonamento

As redes sem fios podem ser montadas segundo diversas topologias de configuração de rede, de acordo com as necessidades e aplicações dos usuários. As configurações podem ser mudadas facilmente e as distâncias entre as estações podem ser adaptadas desde poucos usuários até centenas.

Desvantagens da Rede Sem Fios

- Redução da força do sinal

As radiações eletromagnéticas são atenuadas quando atravessam alguns tipos de matéria (por exemplo, um sinal de rádio ao atravessar uma parede). Há ainda o problema do nó oculto, onde obstruções físicas presentes no ambiente (por exemplo, um outro nó, um anteparo, um edifício, uma montanha) criam um anteparo impedindo que haja comunicação entre os nós.

- Interferência de outras fontes

Várias fontes de rádio transmitindo na mesma banda de freqüência sofrerão interferências umas das outras. Por exemplo, telefones sem fios de 2,4 GHz podem interferir nas redes sem fios e não funcionar bem. Além da interferência de fontes transmissoras, o ruído eletromagnético presente no ambiente (por exemplo, um motor em ligado, um microondas em funcionamento) pode gerar interferências indesejáveis na rede sem fios.

- Propagação multivias

Quando a propagação do sinal de rádio usa múltiplos caminhos partes da onda eletromagnética se refletem em objetos (por exemplo, grandes porções de metais brilhosos, espelhos naturais e artificiais) e também no solo tomando caminhos com comprimentos de onda diferentes entre um emissor e um receptor. Isso resulta no embaralhamento do sinal recebido no nó final. Além disso, os objetos que se movimentam entre o emissor e o receptor também podem fazer com que a propagação multivias mude com o passar do tempo.

- Fragilidade da segurança

Ao contrário das redes cabeadas, onde a infra-estrutura fica dentro das corporações, as redes sem fios usam ondas de rádio como meio de transmissão, o que aumenta as chances de acessos não autorizados. Sendo, portanto, mais susceptíveis a ataques de *hackers* e pessoas mal intencionadas, quando não configuradas adequadamente. Maiores detalhes sobre as vulnerabilidades e os vários tipos de ataques sofridos pelas redes sem fios podem ser encontrados em (NOGUEIRA, 2004, 2006, 2007; NOGUEIRA; JÚNIOR, 2008).

1.3 Categorias de redes sem fios

Diversos autores classificam as redes sem fios em categorias, conforme o alcance dos sinais de radiofreqüência. Tomando como referencial inicial os estudos de Tanenbaum (2003), as redes sem fios podem ser divididas em três categorias principais:

i) Redes sem fios de alcance pessoal (WPAN) ou redes de interconexão de sistemas.

ii) Redes sem fios locais (WLAN).

iii) Redes sem fios geograficamente distribuídas (WWAN).

As redes sem fios de alcance pessoal (*Wireless Personal Area Networks* – WPAN), também conhecidas como redes de interconexão de sistemas, ou simplesmente redes sem fios pessoais, consistem em interligar componentes e periféricos de um computador através de ondas com freqüência de alcance limitada. Como quase todo computador possui gabinete, diversas placas, monitor, teclado e *mouse*, conectados por cabos à unidade principal, isso pode causar alguns transtornos para montagem dessa infra-estrutura. Logo, algumas empresas se uniram para projetar uma rede *ad hoc* comercial de alcance limitado, a chamada rede *Bluetooth*, que pudesse interconectar o computador com os seus periféricos sem que fosse preciso a utilização de fios. Além de prover conexão entre computadores tradicionais (estações de trabalho, *desktops*, *notebooks*) a rede *Bluetooth* permite a conexão dos mais variados tipos de equipamentos como PDAs, celulares, agendas eletrônicas, câmeras digitais, fones de ouvido, dentre outros, simplesmente trazendo-os para dentro do alcance da rede. Nada de cabos, nada de instalação de programas de configuração de equipamentos (*drivers*); basta juntá-los, ligá-los e eles funcionam. Para muitas pessoas essa facilidade de operação é uma grande vantagem. Em sua forma mais simples, as redes de interconexão de sistemas utilizam o paradigma de mestre-escravo, conforme visto na Figura 2 a seguir. A unidade central normalmente é o mestre, comunicando-se com dispositivos secundários, tais como mouse, teclado e impressora que atuam como escravos. O mestre informa aos escravos o protocolo e os endereços que vão ser utilizados, quando eles podem transmitir, por quanto tempo, que freqüências podem usar e assim por diante.

Figura 2 – Uma rede sem fios de alcance pessoal (WPAN) do tipo Bluetooth

Por sua vez, as redes sem fios locais (*Wireless Local Area Networks* – WLAN) são formadas por dispositivos com modem de radiofreqüência, placa de rede sem fios e antena de alcance limitado que provê a comunicação com outros dispositivos (KAVEH, 2005). Normalmente, estas redes possuem estação base para permitir a comunicação entre máquinas, como mostra a Figura 3. Todavia, o uso de estação base não é condição *sine qua non* para as redes sem fios dessa categoria já é possível a montagem de redes sem infra-estrutura, conforme poderá ser verificado no próximo capítulo. As WLAN estão se tornando cada vez mais comuns principalmente em locais onde a instalação da fiação é considerada trabalhosa demais. Como mencionado anteriormente, há um padrão para WLAN sem fios, definido no IEEE 802.11 e implementado pela maioria dos sistemas e que está bastante difundido.

Figura 3 – Um modelo de rede sem fios local (WLAN)

No mesmo tema, Nogueira (2004) entende que as redes locais sem fios, também conhecidas vulgarmente como wireless, Wi-Fi (*Wireless Fidelity*), padrão IEEE 802.11, ou simplesmente WLAN são sistemas de transmissão de dados flexíveis e que podem ser utilizadas como alternativa para as redes com fios. Logo, representa uma tecnologia promissora que permite a comunicação entre equipamentos sem uma conexão física direta. O princípio de funcionamento das redes sem fios se baseia na transmissão de dados através da camada atmosférica utilizando a propagação das ondas eletromagnéticas. Analisando a realidade brasileira, Nogueira (2004) levanta a questão e preocupação sobre qual a faixa de freqüência a ser utilizada pelas redes sem fios, pois poucas faixas dispensam a autorização prévia dos órgãos de controle (Agência Nacional de Telecomunicações – Anatel, no Brasil) para o uso do espectro de freqüências. Isso se torna um ponto relevante, pois de acordo com a utilização do meio físico, da banda e do tipo de mecanismo de modulação usado para transmissão, as redes sem fios podem utilizar vários tipos de espectros, por exemplo, as ondas de banda estreita (ondas de rádio, infravermelho, ondas milimétricas, microondas, ondas luminosas), apesar das ondas de rádio serem as mais difundidas.

As redes sem fios geograficamente distribuídas (WWAN) se assemelham as WLAN quando ao funcionamento. Todavia, como a onda na WWAN se propaga por grandes distâncias então é necessário o uso de equipamentos e tecnologias especiais para gestão do sinal transmitido e recepcionado. Nesse tipo de rede são utilizados os satélites de comunicação compartilhados com as redes de telefonia. Entretanto, não há muitas aplicações de redes sem fios móveis *ad hoc* nesse contexto devido à grande distância entre transmissor e receptor, o alto custo da infra-estrutura e o agravamento dos problemas de transmissão.

2 REDES SEM FIOS *AD HOC* MÓVEIS

O conceito de rede *ad hoc* não é novo, existe há pelo menos 20 anos. Tradicionalmente as redes de inteligência estratégica de cunho militar eram as únicas aplicações para comunicação em redes que utilizavam o paradigma *ad hoc*. Todavia, a introdução de novas tecnologias como o Bluetooth e as variadas classes do padrão IEEE 802.11 têm possibilitado a criação e distribuição de outras aplicações públicas e privadas das redes sem fios *ad hoc* móveis, comumente chamadas de MANET (*Mobile Ad Hoc Networks*), para além dos tradicionais domínios militares. Dessa feita, a utilização das redes ad hoc tem crescido bastante nos últimos anos, possuindo atualmente as mais variadas aplicações (WU; TSENG, 2007). Portanto, esse capítulo visa mostrar alguns aspectos teóricos que irão influenciar em aplicações e cenários que serão apresentados no capítulo 4, mas para isso torna-se mister que se conheçam as bases da mobilidade em uma rede sem fios, bem como as características e tecnologias de alcance das redes do tipo *ad hoc*.

2.1 Mobilidade

O crescimento dos equipamentos computacionais portáteis (*notebooks, palmtops, PDAs*) e alguns tipos de dispositivos automatizados industriais e comerciais portáteis (celulares, máquinas sem fios para compras via cartão de crédito, máquinas sem fios para controle de processos industriais etc.), com capacidade para se comunicar com a parte fixa de uma rede e com outros equipamentos computacionais móveis, criam a chamada computação móvel (BASAGNI *et al*, 2004). Dessa forma, as redes sem fios móveis têm despertado particular interesse nas mais variadas situações. Notadamente em aplicações policiais ou militares, a confiabilidade do meio de transmissão é um requisito indispensável, de modo que a utilização de cabos pode causar transtornos, uma vez que o rompimento de um desses cabos pode comprometer o sistema de defesa ou mesmo toda uma operação. Por outro lado, não é possível estabelecer a conexão por fios entre as viaturas policiais ou carros de combate, aeronaves, lanchas, navios etc. Essa mobilidade da rede, por sua vez, também pode apresentar papel relevante nas operações policiais, pois equipamentos computacionais portáteis podem ser utilizados por policiais para enviar mensagens, transferir arquivos com textos, sons e imagens de investigados e alvos, gravar registros, receber instruções dos seus chefes, mesmo em situações de crise, onde não haja infra-estrutura, nem tempo para montar uma rede de computadores nos padrões tradicionais com fios.

Já faz algum tempo que as forças militares mais avançadas tecnicamente estão desenvolvendo redes sem fios móveis em larga escala para apoiar vários tipos de comunicações em ambientes de atuação das forças táticas (HAAS; TABRIZI, 1998; PEREIRA, 2004). Enquanto isso, as forças policiais ainda subutilizam essa nova tecnologia e suas aplicações.

Nesse contexto, as novas tecnologias de redes sem fios móveis têm o intuito primordial de transportar dados e informações, onde a conectividade entre os roteadores sem fios deve considerar com muita atenção os critérios de robustez e segurança. Essas redes sem fios móveis são muito dinâmicas; os enlaces entre os nós podem surgir e desaparecer em questão de segundos. Desse modo, uma configuração de rede descentralizada e independente de estruturas fixas é uma importante vantagem ou, até mesmo, uma necessidade operacional para o sucesso de uma missão. Para que uma equipe ou tropa possa cumprir sua tarefa de forma adequada em situações reais de campo, ela depende, em grande parte, da eficiência e eficácia do seu sistema de comunicação. Logo, é primordial que esse sistema funcione perfeitamente, para que o chefe da equipe policial ou o comandante de um grupo possa controlar seus subordinados, obter e difundir informações e coordenar as ações de sua equipe.

Todavia, quando se trabalha com a mobilidade em redes sem fios alguns cuidados extras precisam ser tomados. Torna-se importante destacar, por exemplo, que quando há um deslocamento de um equipamento móvel para fora do alcance de uma estação base (conforme modelo apresentado na seção 1.3) e entra na faixa de outra, ele muda seu ponto de conexão para rede maior, ou seja, muda de uma estação base para outra em um processo chamado de transferência (*handoff*). Kurose e Ross (2006) destacam essa característica de transferência das redes sem fios com estação base apresentando várias questões, das quais se destacam:

- Se um equipamento portátil pode se mover, como descobrir sua localização atual na rede de modo que seja possível transmitir pacotes de dados para ele ?
- Como é realizado o endereçamento, dado que um equipamento sem fios conectado a rede pode estar em uma das muitas localizações possíveis ?
- Se o equipamento se movimentar durante uma comunicação, como os dados seguirão as rotas de modo que a conexão continue sem interrupções ?

Ainda considerando a mobilidade, as redes sem fios móveis podem ser classificadas de duas formas: as redes com infra-estrutura; e as redes sem infra-estrutura (*ad hoc*). Nas redes sem fios com infra-estrutura, toda comunicação entre os nós móveis é realizada por meio de estações bases que se encontram na rede fixa que dá suporte à mobilidade (conforme apresentado na Figura 1). Nesse tipo de rede, os nós, mesmo próximos um do outro, estão impossibilitados de estabelecer comunicação direta entre si. Já em uma rede sem infra-estrutura, tipo *ad hoc*, um conjunto de nós sem fios móveis é capaz de se comunicar diretamente entre si, formando dinamicamente uma rede temporária, sem o uso de qualquer ponto de acesso ou estação base. É por essas e outras situações que as redes sem fios *ad hoc* móveis têm gerado pesquisas científicas bastante desafiadoras.

2.2 Redes *ad hoc*

A locução adjetiva "*ad hoc*" pode ser compreendida em sentido geral como algo destinado a uma finalidade específica. Do latim, *ad hoc*, significa literalmente "para isto" realçando dessa forma o seu caráter temporário. Contudo, *ad hoc*, em termos de redes sem fios é mais abrangente. As redes sem fios podem ser divididas em duas categorias: as redes com infra-estrutura; e as redes sem infra-estrutura (*ad hoc*). Nas redes sem fios com infra-estrutura, toda a comunicação entre os nós é feita por meio de estações base que dão suporte à mobilidade na rede fixa. Nesse tipo de rede, os nós, mesmo dentro do alcance uns dos outros, estão impossibilitados de estabelecer comunicação direta entre si. Já em uma rede *ad hoc* um conjunto de nós sem fios é capaz de se comunicar diretamente entre si, formando dinamicamente uma rede temporária, sem o uso de qualquer ponto de acesso centralizado ou estação base. Nesse tipo de rede, os nós funcionam como roteadores, sendo capazes de descobrir e manter rotas para outros nós da rede; e como servidores, executando aplicações dos clientes. As redes *ad hoc*, por sua vez, podem ser divididas em: redes *ad hoc* de comunicação direta, Figura 4(a); e em redes *ad hoc* de comunicação por múltiplos saltos, Figura 4(b). Na comunicação direta, as estações se comunicam apenas com aquelas que estiverem dentro dos seus raios de alcance, denominadas estações vizinhas, logo, de alcance bem limitado. Nas redes de múltiplos saltos, todos os nós possuem, também, a propriedade de traçar a rota e encaminhar os pacotes de dados. Assim, os nós que estejam mutuamente fora de alcance podem se comunicar, se os pacotes de dados puderem ser encaminhados por meio de outros nós que estejam dispostos a cooperar na comunicação. A pesquisa aqui desenvolvida levará em consideração somente as redes sem fios *ad hoc* móveis de comunicação direta.

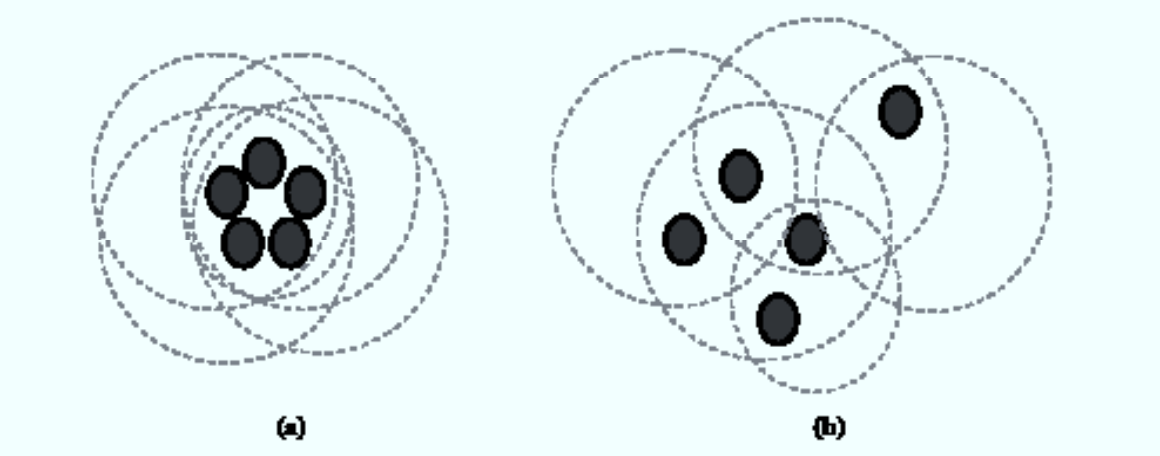

Figura 4 – Tipos de redes ad hoc*: (a) comunicação direta (b) multiplos saltos*

Na Figura 4, os nós pertencentes às redes *ad hoc* estão representados pelos círculos escuros preenchidos. Já as áreas de alcance dos nós estão representadas pelos círculos tracejados maiores. Um nó pode ser qualquer equipamento sem fios, ver na seção 1.2.

Detalhando tecnicamente o conceito do que vem a ser uma rede sem fios *ad hoc* móvel, Fernandes (2008) a define como sendo coleção de nós sem fios móveis (computadores ou roteadores) que dinamicamente formam rede temporária, sem o uso de qualquer infra-estrutura de rede existente ou administração centralizada. Os usuários estão livres para se movimentar aleatoriamente e se organizar de forma arbitrária. O caminho entre cada par de usuários pode ter múltiplas ligações e a comunicação entre eles pode ser heterogênea. Assim, a topologia de rede sem fios *ad hoc* pode mudar rapidamente e imprevisivelmente. Esse tipo de rede pode operar de forma isolada ou pode ser conectada a outra rede, por exemplo, a *Internet*. Múltiplas configurações e aplicações, mobilidade, diversidade de tamanho, heterogeneidade de dispositivo, largura da banda e restrições de consumo de energia (bateria) fazem com que os projetos dessas redes sejam repletos de desafios.

As redes sem fios *ad hoc* trazem ainda algumas características interessantes para as aplicações policias propostas nesse trabalho, tais como: a facilidade de conexão, a configuração dinâmica e a comunicação direta ponto a ponto (*peer-to-peer*). A idéia central é utilizar a tecnologia de redes sem fios *ad hoc* com comunicação direta para integração de computadores pessoais, celulares, PDAs e quando possível conectá-la à *Internet*. Essa idéia torna-se possível e praticável devido às áreas de telecomunicações e de computação terem evoluído de tal forma que hoje já é possível o acesso e a troca de informação entre os nós da rede a qualquer hora e em qualquer lugar. Dessa forma, a grande vantagem das redes sem fios *ad hoc* está em oferecer alta flexibilidade e robustez, mesmo quando não existe uma infra-estrutura de comunicação ou esta possui alto custo de instalação. Outras vantagens são o custo reduzido das redes sem fios *ad hoc*, implantações e reconfigurações rápidas e fáceis, ausência de infra-estruturada cabeada. Todavia, vale ressaltar que nas redes sem fios *ad hoc* móveis a cooperação entre os usuários da rede e a sinergia de esforços para se cumprir uma missão ou objetivo são fundamentais para o sucesso das aplicações previstas para essa nova tecnologia. Por sua vez, a principal desvantagem das redes *ad hoc*, principalmente as de múltiplos saltos, é a complexidade dos nós, pois cada um, além de possuir mecanismos de controle de acesso ao meio e mecanismos para evitar o problema dos terminais ocultos, deve atuar como roteador. A complexidade do roteamento aumenta numa rede *ad hoc*, pois, além de cada nó ter de agir como potencial roteador, a topologia da rede é dinâmica, já que os nós são móveis. Devem ser considerados os problemas típicos das redes sem fios já mencionados na seção 1.2.

2.3 Tecnologias de alcance para redes *ad hoc*

Outra forma de classificar as redes *ad hoc* é a partir do alcance dos sinais de radiofreqüência que trafega no ar. Essa classificação é na verdade um detalhamento e junção de várias abordagens encontradas em Tanenbaum (2003), Rodrigues (2004), Nogueira (2004), Kurose e Ross (2006). Concatenando as idéias desses autores foi possível criar a Figura 5 que classifica as redes *ad hoc* de acordo com a área de cobertura.

a) Redes sem fios corporais – *Wireless Body Area Networks* (WBAN);

b) Redes sem fios de alcance pessoal – *Wireless Personal Area Networks* (WPAN);

c) Redes sem fios locais – *Wireless Local Area Networks* (WLAN);

d) Redes sem fios metropolitanas – *Wireless Metropolitan Area Networks* (WMAN);

e) Redes sem fios geograficamente distribuídas – *Wireless Wide Area Networks* (WWAN)

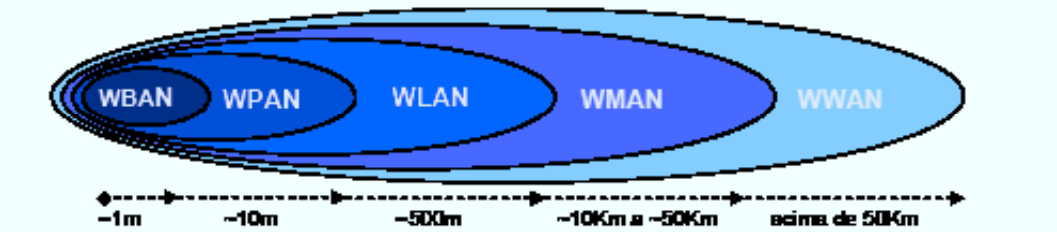

Figura 5 – Taxonomia para redes ad hoc

As redes sem fios *ad hoc* em áreas geograficamente distribuídas (WWAN) e as metropolitanas (WMAN) são redes móveis sem fios próprias para uso com múltiplos saltos (*multihop*) que por sua vez são mais complexas e ainda apresentam muitos desafios (endereçamento, roteamento, localização, segurança etc.) para serem resolvidos em relação às pesquisas científicas que existem na atualidade. Essas classes de redes *ad hoc* ainda não possuem tecnologia suficiente para resolver esses desafios, nem previsão, no curto prazo, para solução. Ademais, esses tipos de redes *ad hoc* não se aplicam ao objeto de estudo desse trabalho, logo não serão mais abordadas deste ponto em diante. Por outro lado, as redes sem fios *ad hoc* móveis com alcance de cobertura menor estão cada vez mais factíveis na atualidade e algumas experiências de sucesso já podem ser comprovadas. Especificamente, as tecnologias sem fios *ad hoc* de comunicação direta ou de único salto (*singlehop*) WBAN, WPAN e WLAN já são comuns no mercado. Por essa razão, as tecnologias WBAN, WPAN e WLAN constituem as tecnologias apropriadas para as redes *ad hoc* móveis que se quer estudar e aplicar nesse trabalho.

As WBAN estão fortemente correlacionadas com equipamentos sem fios que podem ser utilizados junto ao corpo ou muito próximo dele (por exemplo, microfones, fones de ouvido, relógios de pulso etc.). O alcance de comunicação da WBAN corresponde à escala do corpo humano. Alguns pesquisadores afirmam que as WBAN podem chegar ao alcance de até um metro. Como instalar fios no corpo normalmente é um incômodo, as tecnologias sem fios WBAN constituem a melhor solução para a interconexão desses tipos de dispositivos. Por sua vez, as WPAN conectam dispositivos sem fios móveis a outros dispositivos móveis ou fixos. Enquanto que a WBAN é voltada para interconexão de sistemas e dispositivos sem fios usados em uma única pessoa, a WPAN pode ser usada para conexão de rede em torno de várias pessoas ou equipamentos. Na Figura 2, é possível ver nitidamente as possibilidades de conexões de um computador sem fios com os respectivos periféricos: teclado, mouse e impressora. O alcance de comunicação da WPAN é tipicamente até 10 metros, dessa maneira ela permite a conexão com pessoas ou equipamentos próximos uns dos outros e em torno do ambiente. A faixa de freqüência de sinais mais promissora para WPAN está na banda de 2.4 GHz. Já as WLAN têm um alcance típico de um único edifício, ou um conjunto dos edifícios, até 500 metros. As WLAN devem satisfazer às mesmas exigências típicas de qualquer LAN com fios (cabeada), incluindo a distância, a quantidade máxima de conexões entre as estações, a potência de transmissão do sinal, dentre outras. Todavia, as WLAN precisam ser projetadas para enfrentar alguns problemas específicos do ambiente sem fios como a redução da força do sinal, a interferência de outras fontes, a propagação multivias e a fragilidade da segurança. Vale lembrar que há duas formas diferentes de montar as redes sem fios em uma WLAN: com infra-estrutura e sem infra-estrutura (*ad hoc*). O primeiro modelo com infra-estrutura já foi comentado e não interessa aos objetivos desta pesquisa, portanto não será aprofundado o tema. Já uma rede *ad hoc* móvel do tipo WLAN é uma rede montada ponto a ponto (*peer-to-peer*) por uma série de nós dentro dos limites de cada uma. Além disso, esses nós devem se configurar dinamicamente para criar uma rede temporária, conforme comentado.

O trabalho de Rodrigues (2004) destaca que o sucesso da tecnologia de rede sem fios, destacadamente a do tipo *ad hoc*, está relacionado ao desenvolvimento de uma variedade de produtos de rede a um preço competidor. Um fator relevante na concretização desse sucesso é a disponibilidade de padrões apropriados de redes. Atualmente, há dois padrões principais para redes *ad hoc* sem fios: o padrão IEEE 802.11, para as WLAN, e o padrão Bluetooth, para comunicações sem fios de curto alcance: WBAN e WPAN.

Devido à simplicidade e disseminação, o padrão IEEE 802.11 é um excelente ambiente para executar uma rede *ad hoc* do tipo WLAN de único salto ou de conexão direta, parte do escopo desta monografia. Todavia, as redes de múltiplos saltos que cobrem áreas por diversos quilômetros fogem totalmente ao tipo de aplicação que interessa a essa monografia.

Dada a importância desses dois padrões de redes sem fios *ad hoc* (IEEE 802.11 e Bluetooth) no mercado atual, maiores detalhes podem ser conferidos em Gast (2002), Nogueira (2004), Rodrigues (2004), Walke, Mangold; Belemann (2006), Niebert (2007), Sarkar; Basaravaju; Puttamadappa (2008).

3 REDE ADHOCPF

Considerando a conjuntura tecnológica disponível nas unidades centrais e descentralizadas de telecomunicações e informática da Polícia Federal, já é possível vislumbrar a possibilidade de montagem de redes sem fios *ad hoc* móveis para diversas aplicações policiais. A idéia é criar uma rede que seja simples de montar, que não exija grandes conhecimentos de informática e telecomunicações, e que também seja de fácil uso por qualquer policial. Ou seja, busca-se a praticidade. Por esse motivo, foi escolhido o ambiente operacional fornecido pelo Microsoft Windows® e os equipamentos portáteis disponíveis no Setor Técnico-Científico da Superintendência Regional da Polícia Federal no Estado do Ceará (SETEC/SR/DPF/CE) e no Laboratório de Redes de Computadores e Segurança da Universidade estadual do Ceará (LARCES/UECE). Todavia, a rede também pode ser construída em outros ambientes operacionais como o Linux® e o MacOS®.

O uso dessa tecnologia de redes sem fios *ad hoc* móveis é justificado em situações temporárias: casos de emergência, falta de infra-estrutura computacional, falta de tempo, necessidade de mobilidade, dentre outras aplicações que serão mostradas no capítulo 4. Nesses cenários, é possível utilizar essa tecnologia para transferir textos, sons e imagens, compartilhar recursos, enviar e receber mensagens ou arquivos. Se em algum momento da comunicação houver disponibilidade de alguma outra rede, como por exemplo, a *Internet*, a rede poderá se conectar e utilizar os recursos e serviços fornecidos por essa conexão sem maiores problemas. Para essas situações, é proposta a montagem de uma rede sem fios *ad hoc* móvel, chamada AdHocPF, com os recursos de *hardware* e *software* disponíveis no SETEC/SR/DPF/CE em um primeiro momento e em seguida usando os recursos do LARCES/UECE. Um dos objetivos deste trabalho é analisar e avaliar o uso desse tipo de arquitetura de redes computacionais na práxis diária das atividades policiais. Com esse novo paradigma proposto, espera-se que seja possível obter uma redução dos custos operacionais para concretização das tarefas ou missões, haja vista não ser preciso grandes recursos e investimentos: cabos, fios e demais pontos fixos como no caso das redes cabeadas, nem dos pontos de acesso e roteadores dedicados no caso das redes sem fios tradicionais.

3.1 Arquitetura

Diversas arquiteturas de redes com e sem infra-estrutura foram apresentadas nos capítulos e seções anteriores. Todavia, a que se mostrou mais adequada paras os fins pretendidos nessa pesquisa foi a rede sem fios *ad hoc* móvel do tipo comunicação direta e, por conseguinte, essa será a arquitetura a ser montada para AdHocPF (Figura 6).

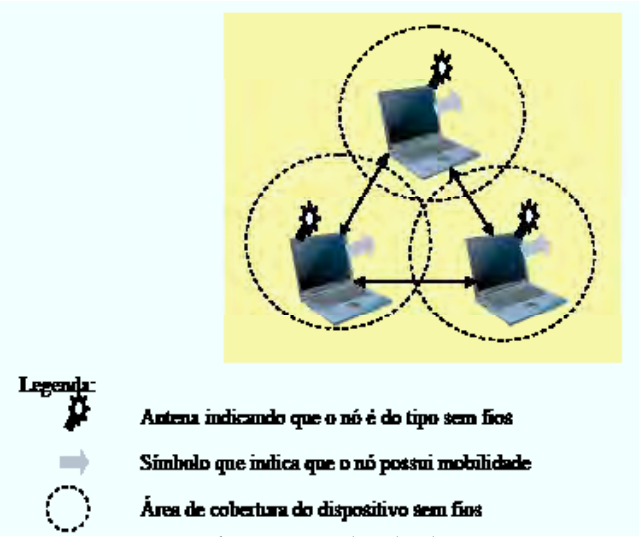

Figura 6 – Arquitetura da rede AdHocPF

A rede AdHocPF na Figura 6 está montada com três nós. Contudo, a rede pode ser montada com muito mais nós tendo como quantidade máxima as limitações impostas pelo alcance do sinal, pela placa de rede sem fios, pelo sistema operacional, dentre outros. Segundo alguns autores (KWOK, 2007), (SARANGAPANI, 2007), (WEBB, 2007), (WU; TSENG, 2007) a quantidade de nós pode chegar, sem maiores problemas, à casa das dezenas. Todavia, existem outras limitações dependendo do ambiente em que se encontram os nós, pois pode haver redução da força do sinal, interferência de outras fontes, propagação multivias, dentre outros problemas já relatados na seção 1.2.

3.1.1 Hardware

Os equipamentos podem ser bastante variados, pois dependem basicamente do tipo de aplicação que se quer para a rede. Todavia, os equipamentos abaixo foram testados e funcionaram a contento.

Configuração Mínima

- 02 (dois) nós móveis, onde cada nó pode ser um notebook, um palmtop ou um PDA.
- 02 (duas) placas ou cartões de rede sem fios, uma para cada nó.

Configuração Ideal

- Mais de 02 (dois) nós móveis, onde cada nó pode ser um *notebook*, um *palmtop*, ou um PDA. Foram realizados estudos práticos para esta monografia usando até 10

(dez) nós. A rede *ad hoc* funcionou bem, todavia quando conectada a *Internet* o desempenho caiu sensivelmente. Para esses testes foram utilizados computadores portáteis pessoais e alguns disponibilizados pelo LARCES/UECE.

- Placas ou cartões de rede sem fios para cada nó.

3.1.2 Software

No ambiente de testes (Windows XP e Windows Vista) não há necessidade de outro programa computacional (software) além do sistema operacional Windows. Haja vista que, uma vez configurado adequadamente (ver seção 3.2), o sistema operacional Windows (XP ou Vista) gerencia todo o processo de controle da rede *ad hoc* automaticamente. Inclusive, as transferências de dados, e informações (textos, sons, imagens, vídeos) podem ser realizadas também pelo próprio sistema operacional Windows sem a necessidade de outro *software* ou programa de apoio. Com isso, esse ambiente traz um efeito positivo, uma vez que policiais com conhecimentos variados de computação poderão operar essa arquitetura de rede *ad hoc* facilmente.

Configuração de *software* Mínima e Ideal

- Nós móveis executando o sistema operacional Microsoft Windows XP ou Vista de 32 bits ou 64 bits.

- Para este trabalho foi utilizado o Windows XP de 32 bits, pois todos os dispositivos disponíveis (no SETEC/SR/DPF/CE e na UECE) possuíam este sistema operacional. Todavia, também foram realizados testes com alguns dispositivos que possuíam o Windows Vista de 32 ou 64 bits tendo se comportado de forma semelhante aos dispositivos que usavam o Windows XP de 32 bits. Há apenas algumas diferenças quanto à apresentação das telas durante a configuração da rede no sistema operacional.

3.2 Configuração

Essa seção descreve o modo de configurar a rede AdHocPF nos moldes e características abordadas na seção 2.2. Como no modelo não se usa qualquer tipo de estação base (ponto de acesso) é preciso configurar um nó sem fios inicial para assumir as responsabilidades e os serviços da estação base, o nó principal.

O primeiro passo será verificar se o dispositivo (nó) principal possui placa ou cartão sem fios, padrão 802.11b, e em seguida configurá-lo como uma conexão sem fios ponto a ponto (*peer-to-peer, P2P*) que fará o papel *ad hoc*. Atualmente, boa parte dos equipamentos

(*notebooks*, *palmtops*, PDAs, etc) já vem com a placa de rede sem fios embutido na própria placa mãe do equipamento. Caso não venha com a placa ou cartão para conexão sem fios é possível comprar um adaptador e em seguida configurá-lo. Essa monografia não abordará a instalação de qualquer tipo de *hardware*, supondo que os nós já possuem os devidos equipamentos (hardware) para comunicação sem fios. O segundo passo será verificar se o segundo nó possui placa ou cartão sem fios, padrão 802.11b, e em seguida configurá-lo. Fazendo o mesmo para o terceiro nó, quarto nó e assim sucessivamente.

Para concluir a implantação da rede *ad hoc*, torna-se necessário providenciar o compartilhamento entre os nós, fornecendo a conectividade entre eles. Para isso, poderá ser utilizado o Compartilhamento de Conexão com a *Internet* (ICS) que já vem pronto no ambiente Windows.

3.2.1 Configurando o nó principal

Caso o nó já possua a tecnologia sem fios embargada então basta configurá-lo. Caso contrário, depois que já estiver instalado a placa ou o adaptador no nó, padrão 802.11b (e. g. cartão de rede sem fios Cisco, Orinoco, BroadCom, Linksys), o Windows XP ou Vista irá detectar automaticamente o cartão, instalar os programas de configuração de equipamentos (drivers) e exibir um ícone na área de notificação. Se o computador estiver em um ambiente em que haja outras redes sem fios ao alcance, o Windows deverá exibir automaticamente uma lista de redes disponíveis, conforme Figura 7 a seguir.

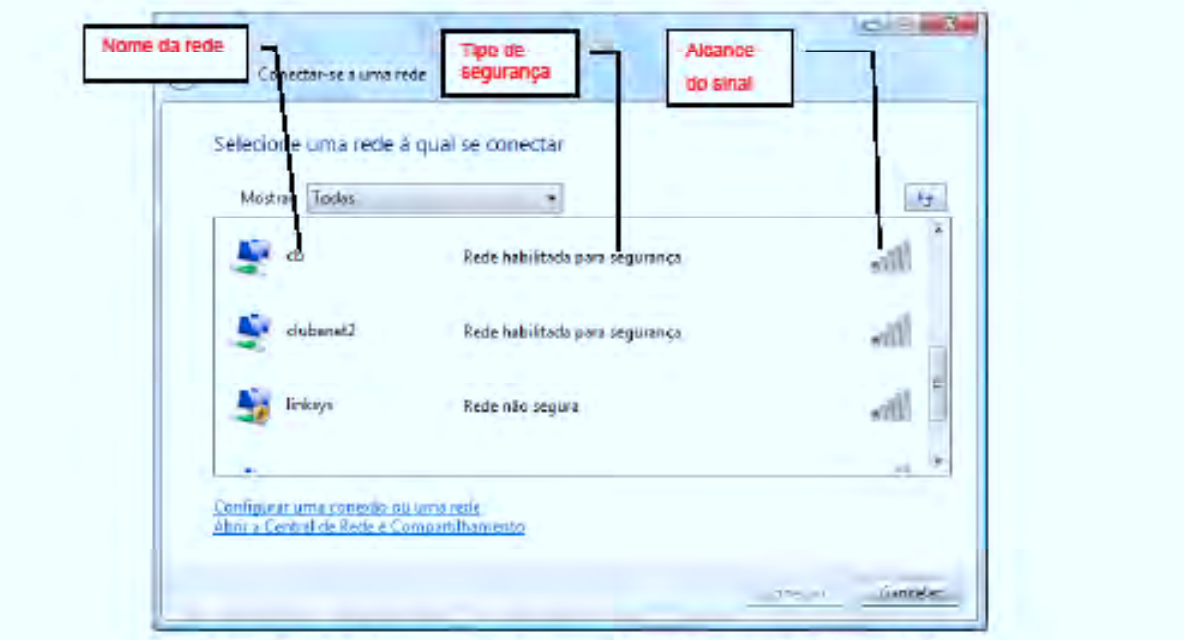

Figura 7 – Janela de reconhecimento das redes sem fios disponíveis

Caso o Windows não detecte automaticamente as redes disponíveis, basta ir no "Painel de controle" e selecionar "Conexões de rede e de *Internet*", como apresentado na Figura 8. Ao clicar nessa opção o Windows irá mostrar a lista de redes sem fios disponíveis que estão no alcance da placa de rede do dispositivo, semelhante à apresentada na Figura 7.

Figura 8 – Conexões de rede e de Internet *no painel de controle do Windows*

Na Figura 7 é possível verificar que há três redes sem fios ao alcance do nó inicial que se quer configurar e que são reconhecidas pelo Windows. No caso, existem as redes sem fios: cb, clubenet2 e linksys. No lado esquerdo aparecem os nomes das redes sem fios. No centro aparecem os tipos de segurança que as redes foram configuradas. Vale destacar que a rede linksys não possui nenhum mecanismo de segurança, podendo ser conectada por qualquer dispositivo que reconheça a rede. No lado direito aparecem os níveis do sinal captado pela placa de rede sem fios do nó. Veja que na Figura 7 o nó ainda não se conectou a nenhuma das redes supramencionadas.

Entretanto, se não houver redes sem fios ao alcance do nó, o ícone de conexão sem fios exibe um "X" vermelho, não abrindo automaticamente a janela "Exibir Redes Sem Fios". Para abrir essa janela, basta clicar no ícone para a conexão sem fios que aparece no canto inferior direito da tela, semelhante ao segundo ícone, da esquerda para direita na Figura 9.

Figura 9 – Ícone de não reconhecimento de rede

Se alguma rede for exibida na lista das "Redes Disponíveis" não faça nenhuma seleção nesse momento. Se seu computador se conectou anteriormente a uma rede sem fios com ou sem infra-estrutura, então remova todos os acessos preferidos "Redes Preferenciais". Para isso, clicar com o botão direito do mouse sobre a "Conexão de rede sem fios", ver Figura 10.

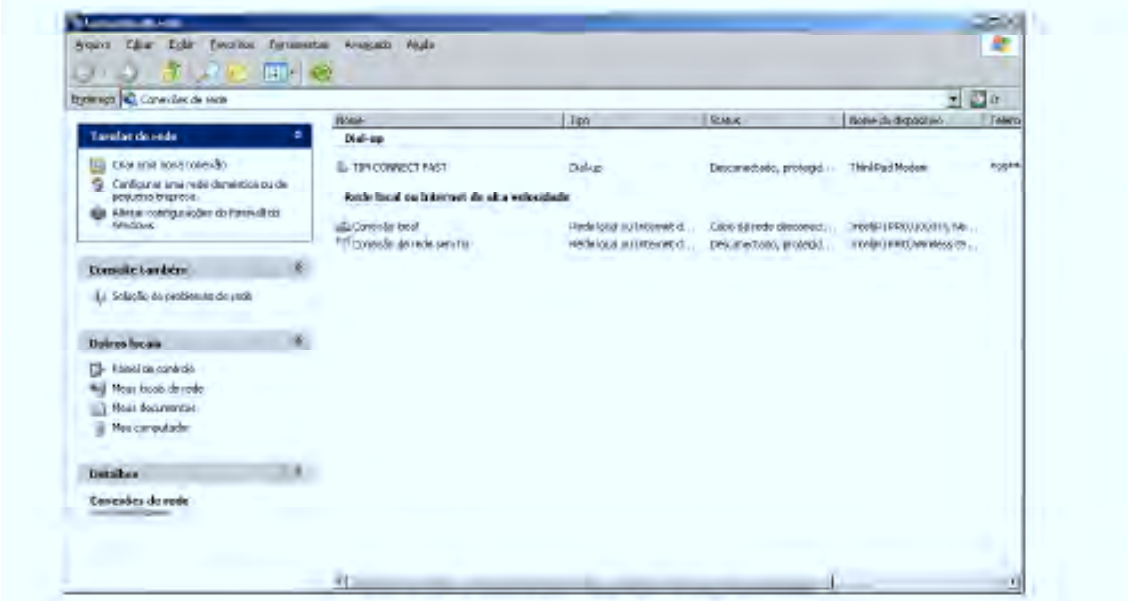

Figura 10 – Conexões de rede sem fios

Em seguida, na guia "Redes sem fios" da tela de "Propriedades de conexão de rede sem fios", remova as redes preferenciais existentes, ver Figura 11. Essa remoção irá assegurar que uma conexão seja estabelecida somente à rede *ad hoc* que será criada.

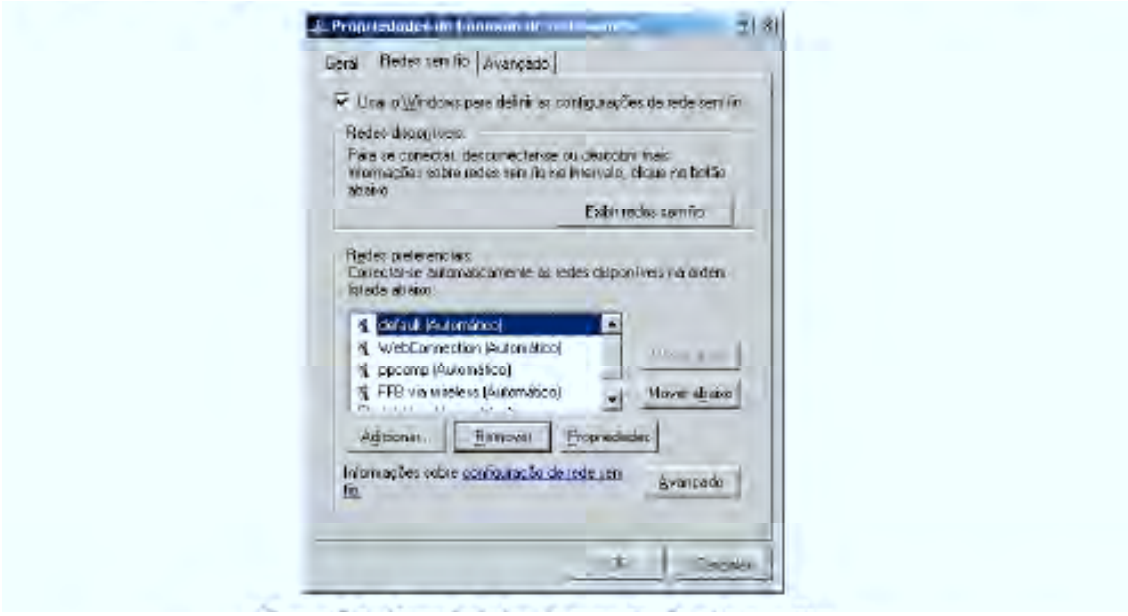

Figura 11 – Propriedades de conexão de rede sem fios

Em seguida, clique na guia "Avançado" no topo da janela. Selecione somente redes do tipo *ad hoc* (computador a computador) e desmarque a caixa "Conectar-se automaticamente as redes não preferenciais" se selecionada, conforme Figura 12. Essa configuração, junto com a remoção das redes preferenciais, irão assegurar conexão somente à rede *ad hoc* que está sendo criada.

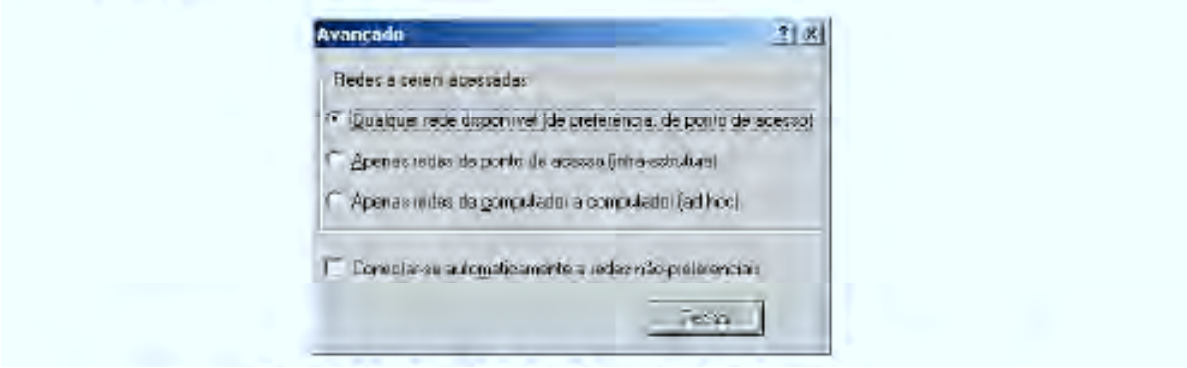

Figura 12 – Propriedades de conexão de rede sem fios

Clique novamente na guia "Redes sem fios". Abaixo de "Redes Preferidas", clique em "Adicionar". Na caixa de diálogo "Propriedades da Rede Sem Fios", especifique um "Nome da Rede (SSID)", como mostra a Figura 13. Utilize qualquer nome desejado (no caso, será utilizado o nome AdHocPF), mas assegure-se de usá-lo para configurar todos os nós sem fios (*notebooks*, *palmtops*, PDAs) que farão parte da rede AdHocPF. Observe na Figura 13 que o tipo de rede já está marcado como "Esta é uma rede de computador a computador (*ad hoc*); não são usados pontos de acesso" e que isso não pode ser mudado uma vez que já foi especificado que uma conexão deveria ser feita somente para redes *ad hoc*.

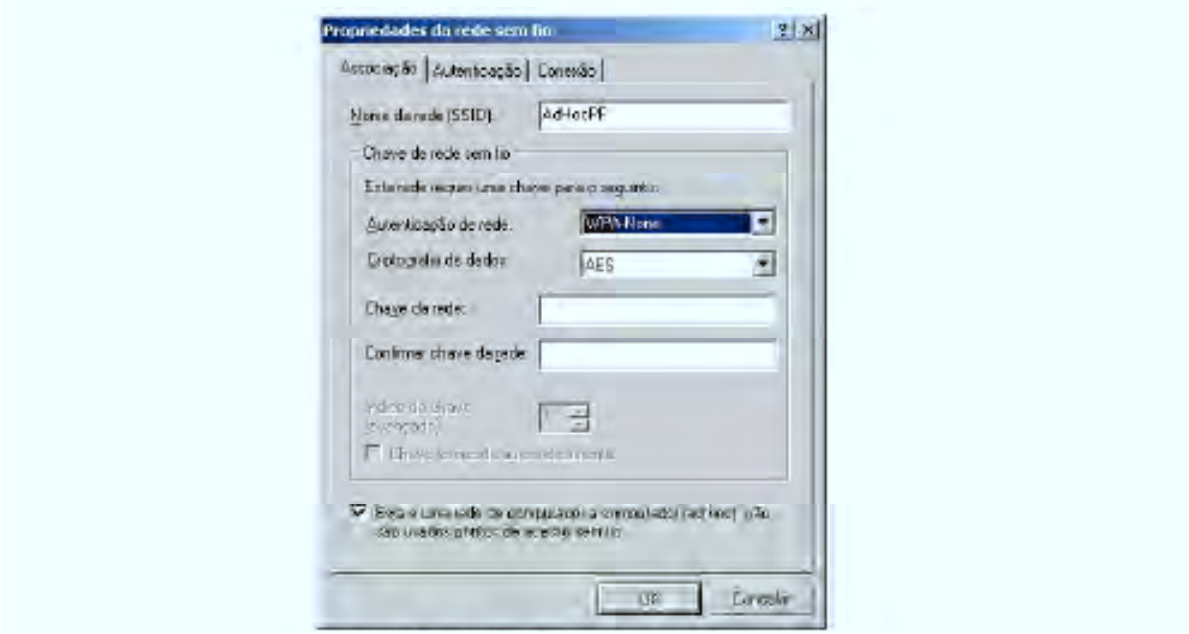

Figura 13 – Criação da rede sem fios ad hoc

3.2.2 Configurando a habilitação da segurança

A habilitação da segurança em uma rede sem fios no ambiente Windows é realizada através de criptografia simétrica (STALLINGS, 2006). As configurações de criptografia de segurança podem ser feitas nesse momento ou deixadas para depois de configurados todos os nós. Os dispositivos portáteis mais atuais que usam o ambiente Windows possuem basicamente dois tipos de protocolos de criptografia disponíveis: o *Wired Equivalent Privacy* (WEP) e o *Wi-Fi Protected Access* (WPA).

O objetivo inicial do WEP era dar maior segurança quanto a disponibilidade, integridade e confiabilidade na comunicação entre os dispositivos sem fios. Uma vez que o WEP é um protocolo de segurança que atua na camada de enlace ele fornece uma certa segurança para as redes sem fios semelhante a segurança das redes com fios. Conforme estudos realizados por Comer (2007), Stallings (2006) e Tanenbaum (2003) a criptografia do protocolo WEP utiliza uma cifra de fluxo baseada no algoritmo RC4. O RC4 gera um fluxo de chaves que sofre uma operação XOR com um texto simples para formar o texto cifrado. Contudo, após estudos e testes realizados com este protocolo, foram encontradas algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse quase toda a sua credibilidade. No WEP, os dois parâmetros que servem de entrada para o algoritmo RC4 são a chave secreta, C, de 40 bits ou 104 bits e um vetor, V, de inicialização com 24 bits. A partir desses dois parâmetros, o algoritmo gera uma seqüência criptografada RC4 (C,V). Porém, como no WEP a chave secreta é a mesma utilizada por todos os usuários de uma mesma rede, devemos ter um vetor de inicialização diferente para cada pacote a fim de evitar a repetição de uma mesma seqüência RC4 . Essa repetição de seqüência é extremamente indesejável, pois dá margem a ataques bem sucedidos e a conseqüente descoberta de pacotes por eventuais intrusos. O RC4 foi projetado e se manteve secreto até vazar e ser publicado na *Internet* em 1994. Além do RC4, o WEP utiliza a função de detecção de erros CRC-32 que é uma função detectar erros nas comunicações. A CRC-32 é uma função linear e não possui chave. Essas duas características da CRC-32 tornam o protocolo WEP suscetível a vários tipos de ataques prejudiciais e indesejáveis. Logo, a chave WEP não é tão difícil de ser quebrada (decifrada), mas os riscos são minimizados devido ao alcance reduzido das redes *ad hoc*.

A criptografia usada no protocolo WPA é bem melhor do que a utilizada no WEP. O WPA é um WEP melhorado. Também chamado de WEP2, ou *Temporal Key Integrity Protocol* (TKIP), a primeira versão do WPA surgiu a partir do esforço conjunto dos membros da Aliança Wi-Fi e dos membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fios ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP. Basicamente, trata-se de um subconjunto do padrão IEEEE 802.11i para cifrar o fluxo de dados usando uma tecnologia mais avançada do que o RC4. Para o WPA, a criptografia usando TKIP é necessária. O TKIP

substitui o WEP por um novo algoritmo de criptografia mais forte do que o RC4 fornecendo o seguinte: verificação da configuração de segurança após as chaves de criptografia serem determinadas; alteração sincronizada da chave de criptografia para cada quadro; determinação de uma única chave de criptografia de partida para cada autenticação de chave pré-compartilhada. Hoje já se encontra em uso a nova versão desse protocolo, o WPA 2.0, que utiliza protocolos padronizados por camadas. Tendo em vista que o WPA 2.0 se baseia no Protocolo da *Internet* (IP), ele permite o uso do IP seguro (IPsec) na camada de rede. Na camada de transporte, as conexões TCP podem ser protegidas pelo TLS, um padrão da IETF. Em um nível ainda mais alto, ele utiliza a autenticação de clientes HTTP, definida na RFC 2617. As bibliotecas de criptografia da camada de aplicação proporcionam controle de integridade e não repúdio. Outra vantagem do WPA é que a migração do WEP para ele requer somente a atualização de *software*.

No caso do Windows já existe pré-estabelecida a opção de usar o "WPA-None", uma versão simplificada do WPA, destinada para o uso em conexões *ad hoc*, onde é possível optar entre usar o modo de criptografia TKIP ou o AES. A maior deficiência do WPA-None em relação ao WPA ou WPA 2.0 usado em redes sem fios com infra-estrutura é que no WPA-None as chaves são estáticas e por isso são mais suscetíveis de serem quebradas. Na prática, o WPA-None com TKIP equivale a um WEP mais forte, pois usa chaves de tamanho maior, enquanto o AES é um pouco mais seguro. No Windows Vista também existe a opção de usar o WPA 2.0 para redes *ad hoc*, mas isso limita a compatibilidade com outros nós que estejam rodando outros sistemas, como no Windows XP onde não há essa opção.

Alguns profissionais não configuram a segurança nesse momento porque é mais fácil ter a rede sem fios *ad hoc* executando sem problemas antes de tentar configurar a criptografia de dados. Devido ao tipo de aplicação que a atividade policial requer é preferível criar as chaves de criptografia simétrica já durante a criação da rede *ad hoc*. A decisão sobre usar WEP ou WPA deve se basear no ambiente em que a aplicação será executada e na sensibilidade das informações que trafegarão na rede. No contexto desse trabalho, preferiu-se já configurar a AdHocPF com a criptografia WPA-None no momento de sua criação, haja vista que os dados que trafegarão na rede serão muitas vezes confidenciais, não podendo cair em mãos erradas. Vale lembrar que a qualquer momento pode ser realizada a troca da chave de segurança da criptografia. Basta acessar novamente as propriedades da rede que acabou de ser criada e alterar as chaves de acesso da rede AdHocPF. Para isso, é necessário abrir com o botão direito do mouse a caixa de diálogo "Conexão de rede sem fios", selecionar a caixa de opção "Propriedades" que aparecerá a rede AdHocPF como fazendo parte das redes preferenciais, conforme Figura 14.

É importante ressaltar que em uma rede *ad hoc* todos os nós (dispositivos) estão no mesmo nível hierárquico, sem uma autoridade central. Todos os nós na rede *ad hoc* estão

configurados para usarem o mesmo nome na rede (SSID), no caso AdHocPF, o mesmo tipo de algoritmo de criptografia e estabelecem conexões direta entre eles criando uma rede ponto a ponto. Inicialmente, os nós terão acesso apenas um ao outro, sem acesso à compartilhamento de arquivos, à web ou *Internet*. Depois de conectá-los à rede *ad hoc* é que será realizado o passo seguinte de compartilhamento, que é feito automaticamente usando uma faixa de IPs disponível pelo Windows.

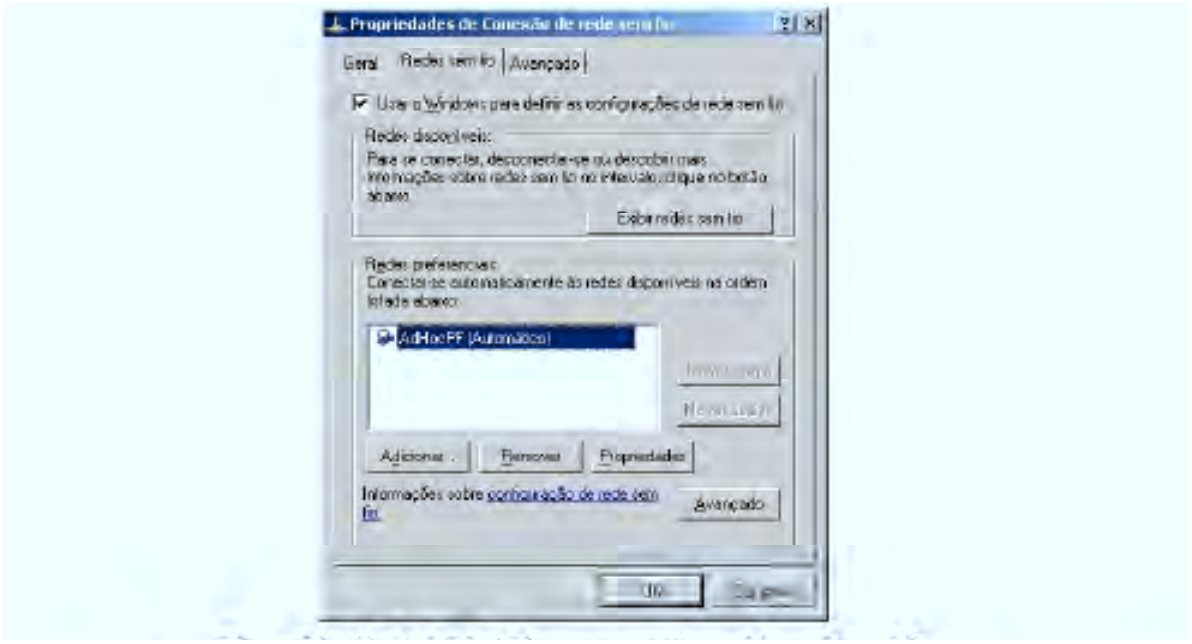

Figura 14 – Rede AdHocPF como parte das redes preferenciais

O passo seguinte para concretizar a mudança da chave ou senha de criptografia é selecionar a rede AdHocPF, clicar nas "Propriedades" que aparecerão as propriedades da rede já criada AdHocPF, conforme Figura 15.

O Windows XP fornece as seguintes opções para chave usando o protocolo WEP:

1) Autenticação de rede: aberta ou compartilhada;

2) Criptografia de dados: WEP ou desativado.

Enquanto para o protocolo WPA o Windows XP fornece as seguintes opções de chave de segurança:

1) Autenticação de rede: WPA - None;

2) Criptografia de dados: TKIP ou AES.

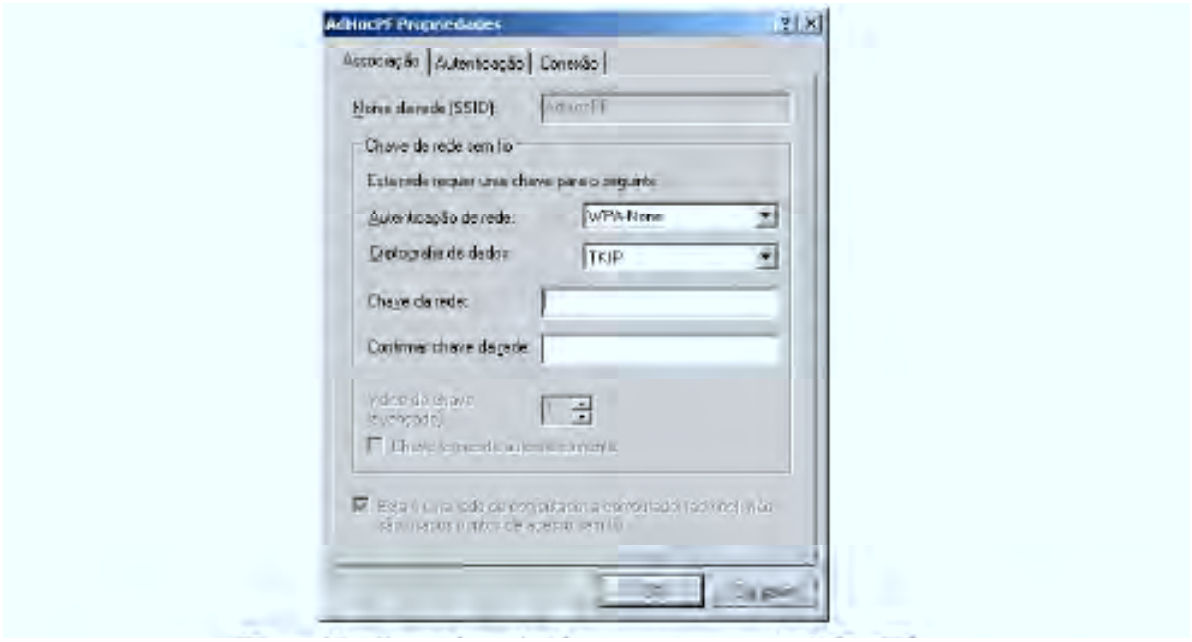

Figura 15 – Troca da senha de segurança na rede AdHocPF

É importante consultar a documentação fornecida pelo sistema operacional ou pelo fabricante da placa ou cartão sem fios quanto ao formato e comprimento das chaves de segurança da rede. Normalmente o Windows solicita uma chave ou senha para acessar a rede. Quando o protocolo de segurança utilizado for o WEP a chave precisa ser de 40 bits ou 104 bits, dependendo da configuração de segurança que se quer para rede. Essa chave WEP pode ser inserida com 5 ou 13 caracteres ASCII. Já quando o protocolo for o WPA (no Windows XP é chamado de WPA-None) a chave precisa ser de 128 bits ou 256 bits, dependendo do nível de segurança que se quer para a rede. Essa chave WPA pode ser cadastrada com tamanho de 8 a 63 caracteres ASCII. É fortemente recomendado o uso do protocolo WPA. Quando não for possível, então usar o protocolo WEP, mas nunca deixar a rede sem senha de acesso criptografada, pois a criptografia dificulta a atuação de pessoas desautorizadas e *hackers*. Maiores detalhes sobre a criptografia WEP e WPA consultar Stallings (2006).

Após esse estudo sobre chaves criptográficas é recomendado, sempre que possível, utilizar o nível mais alto de criptografia (maior comprimento da chave) que for suportado pelos equipamentos e seus respectivos programas computacionais. Se utilizar caracteres ASCII para criação da chave, assegure-se que sejam escolhidos letras e caracteres aleatórios que não sejam adivinhados facilmente. Por exemplo, não usar como chave palavras que estejam em dicionários, pois evitaria um ataque por dicionário à rede (NOGUEIRA, 2006). Esse pro-

cedimento de configuração de chave de criptografia deve ser repetido para cada nó na rede AdHocPF. Como segurança adicional, as chaves WEP ou WPA dos nós devem ser trocadas a cada missão ou periodicamente, o que ocorrer primeiro.

Depois de configurado o nome da rede (SSID) na caixa de diálogo das "Propriedades da Rede Sem Fios", bem como o protocolo de criptografia, a nova rede AdHocPF será exibida com um ícone para designar que essa é uma rede habilitada. Na Figura 16 é possível verificar que a rede AdHocPF já aparece na lista das redes sem fios disponíveis estando configurada e pronta para receber a conexão do dispositivo sem fios que a reconheceu. Note que nessa Figura 16 a placa de rede sem fios do dispositivo reconheceu três redes sem fios: a AdHocPF do tipo *ad hoc* (entre computadores) com segurança habilitada, a rede sem fios SETECCE com segurança habilitada e a rede sem fios NETGEAR sem segurança habilitada.

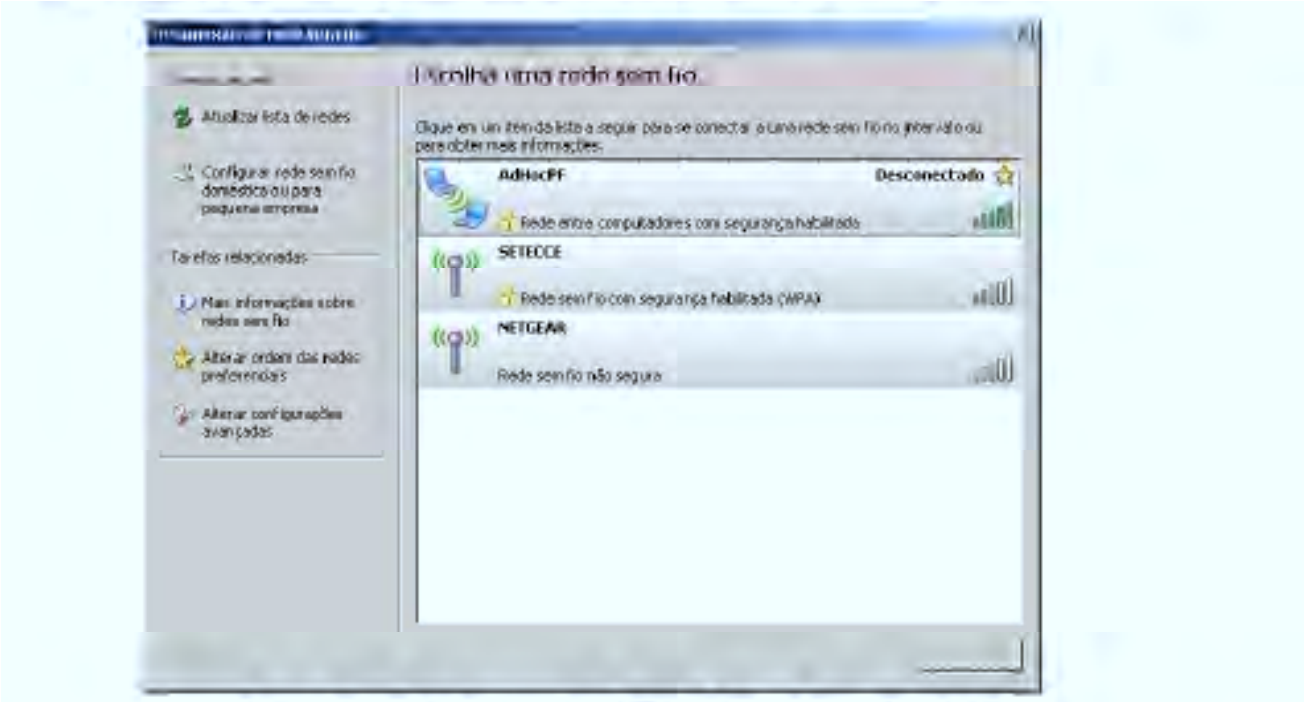

Figura 16 – Reconhecimento da rede AdHocPF no nó principal

3.2.3 Configurando os nós secundários

A partir desse momento qualquer nó que não seja o principal será um nó secundário. Para ser um nó secundário na rede AdHocPF basta que o dispositivo possua uma placa ou cartão de rede sem fios. A guia de "Redes Sem Fios" desse nó secundário exibe uma lista de redes sem fios que estão ao alcance do dispositivo, como mostra a Figura 17.

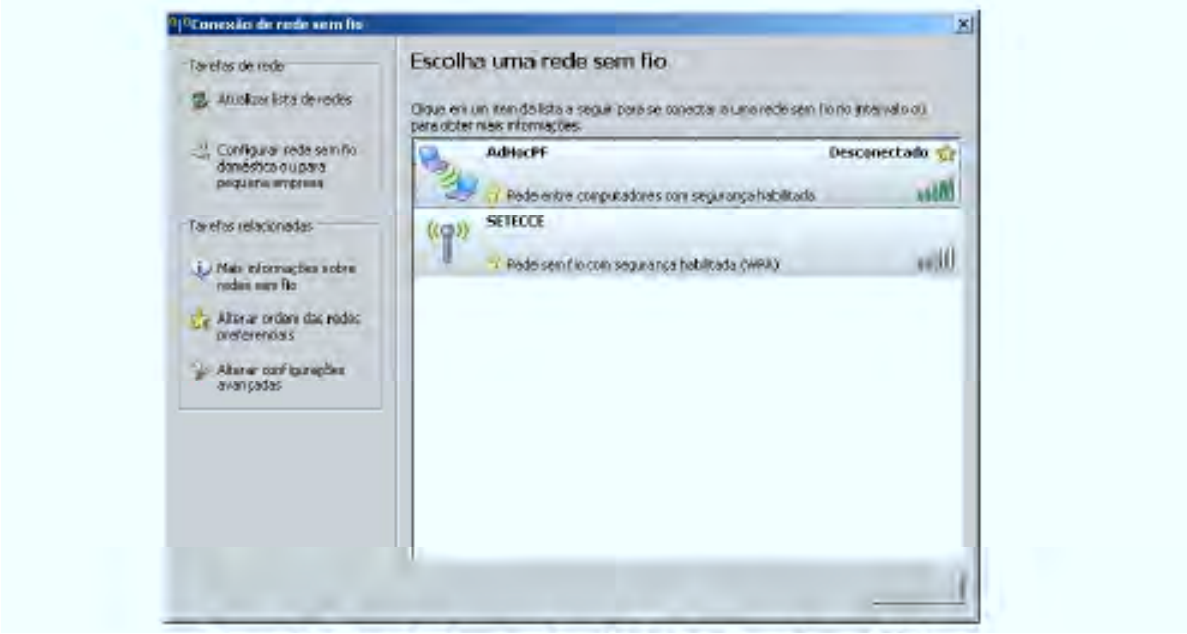

Figura 17 – Reconhecimento da rede AdHocPF no nó secundário

Como a rede AdHocPF já está configurada para uso ela aparecerá na lista de redes disponíveis no nó secundário. Uma vez que o protocolo WPA ou WEP já foi configurado para todos os nós que participarão da rede, então basta selecionar a rede AdHocPF, digitar a chave (senha) previamente estabelecida e clicar em OK. Logo, o nó secundário já está conectado e fará parte da rede AdHocPF, sem precisar configurar mais nada. Para compartilhar a conexão ou conectar-se a *Internet*, basta usar a faixa de IP fornecida automaticamente pelo Windows.

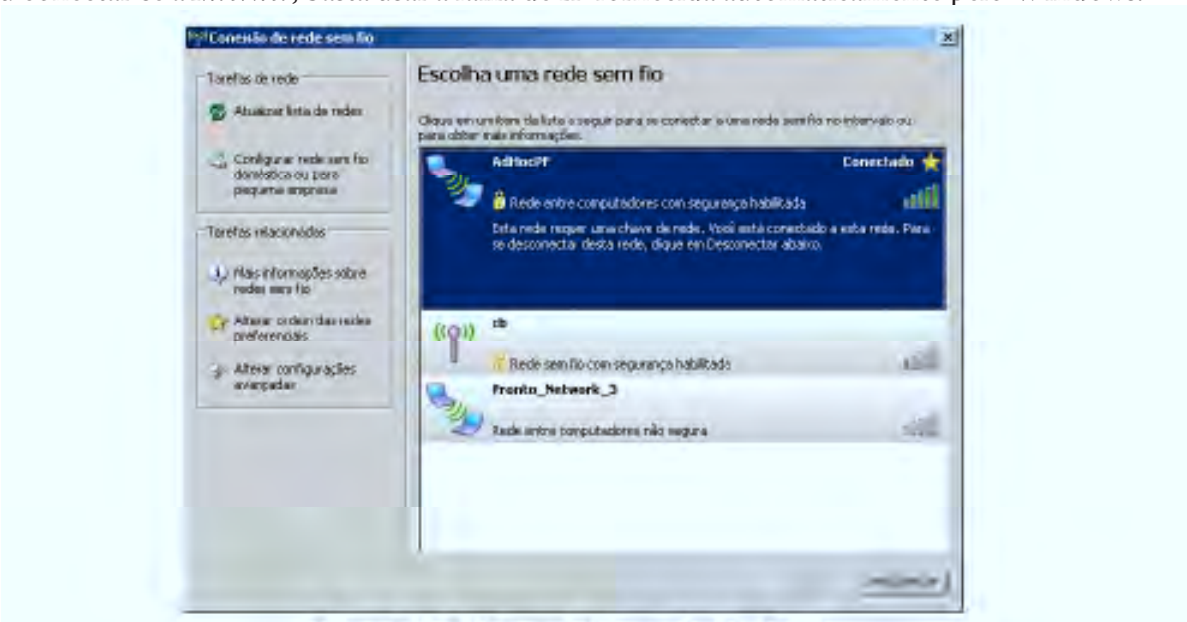

Figura 18 – Nó conectado na rede AdHocPF

A Figura 18 apresenta quando um nó secundário está conectado na rede AdHocPF. O mesmo procedimento deve ser efetuado para o terceiro nó, o quarto nó e assim sucessivamente até conectar todos os nós que farão parte da rede AdHocPF.

Vale destacar que a criação de nós no Windows XP tem procedimento semelhante no Windows Vista, modificando apenas algumas telas. Uma vez criada a rede AdHocPF ela será transparente para os usuários que utilizam esses dois tipos de sistemas operacionais, podendo inclusive ter dispositivos executando o Windows XP e outros executando o Windows Vista na mesma rede AdHocPF. A transparência e a portabilidade facilitam bastante o trabalho de inclusão de novos nós na rede, pois qualquer computador ou dispositivo sem fios usando o Windows XP ou Vista poderá reconhecer a rede AdHocPF sem maiores dificuldades e se conectar. Para ver como está se comportando a rede *ad hoc*, basta verificar o estado da sua conexão ("Iniciar" > "Painel de controle" > "Conexões de rede" > "Exibir o status desta conexão") que aparecerá uma tela semelhante a apresentada na Figura 19. Apesar de que qualquer pessoa que possua um dispositivo sem fios e que não faça parte da rede AdHocPF possa reconhecer a rede, somente os dispositivos e usuários que possuem a chave (i.e. senha da rede) poderão ter acesso aos recursos e serviços providos por ela. Daí a necessidade de se ter uma boa chave de rede, pois caso contrário qualquer pessoa com um dispositivo sem fios poderia conectar-se a AdHocPF como se fosse um nó válido da rede.

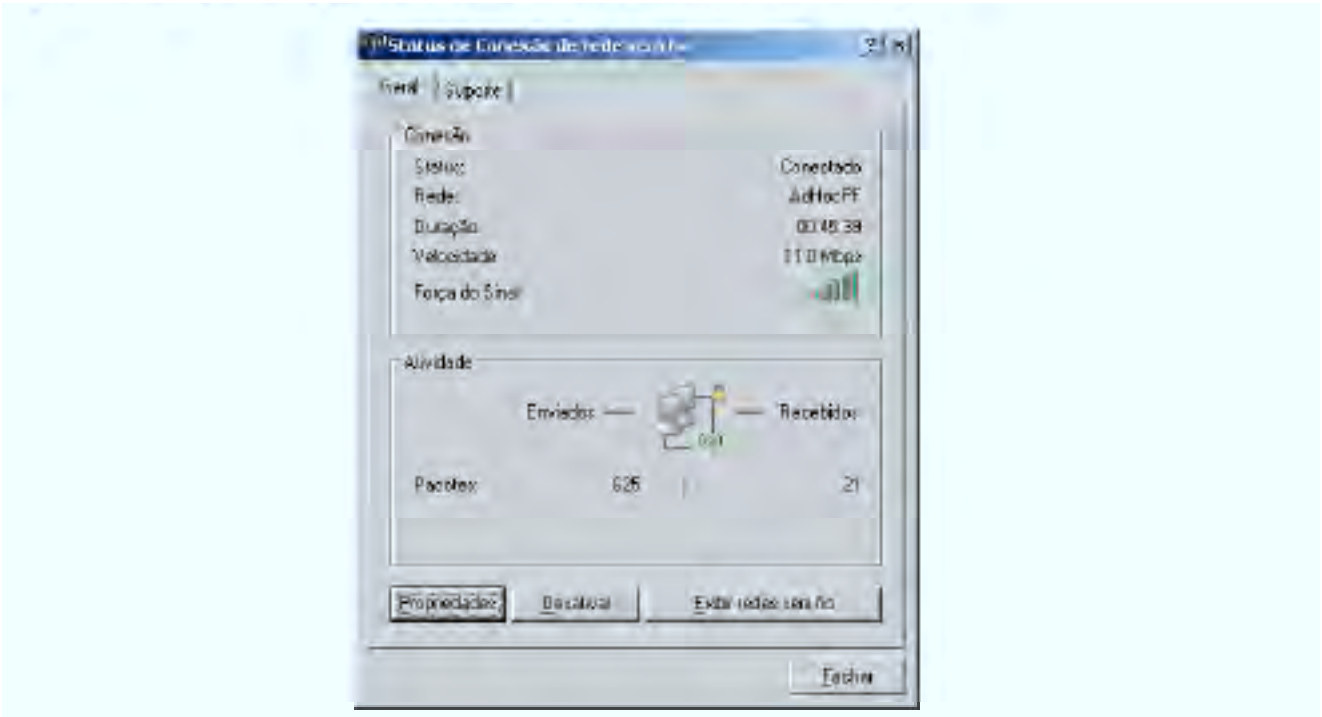

Figura 19 – Estado da conexão da rede AdHocPF

4 CENÁRIOS DE APLICAÇÕES

Vários fatores são favoráveis ao uso da tecnologia sem fios das redes *ad hoc* móveis, tais como aplicações nas áreas de: segurança, defesa, indústria, comércio, negócio, dentre outros. Graças à *Internet*, a comunicação de dados móvel sem fios está avançando em termos de tecnologia e penetração de uso, ainda mais com o sucesso da nova geração de equipamentos como o padrão 3G dos celulares. Quando se olha para os possíveis cenários de uso das redes sem fios *ad hoc* móveis é possível vislumbrar a computação com certa onipresença e com uso intenso nas vidas das pessoas e organizações. Em um futuro próximo, é esperado que as funções e as capacidades de transmissão de dados de alcance limitado das redes sem fios sejam ampliadas, servindo de complemento a comunicação tradicional em larga escala. As tecnologias de rede que usam a radiofreqüência (como *Bluetooth* e MANET) possibilitam a implantação de sistemas de comunicação e transferência de dados de forma bem mais simplificada e barata do que a comunicação com fios. Em termos de preço, portabilidade, flexibilidade, aplicabilidade e possibilidade de comunicação entre diversos dispositivos diferentes, tais como computadores portáteis, PDAs e celulares 3G, fazem com que as redes sem fios *ad hoc* móveis sejam bastante promissoras para um futuro próximo. Assim, a Polícia Federal brasileira, como órgão ícone em Segurança Pública, não pode ficar alheia às aplicações e facilidades que essa tecnologia pode fornecer.

Em termos de mercado, a aceitação e a formação de uma massa crítica para uso dessa tecnologia têm sido bastante positiva, basta ver o uso dos equipamentos com tecnologia Bluetooth nos dias atuais. Vale salientar que uma rede sem fios *ad hoc*, como a proposta pela arquitetura da AdHocPF, é uma rede de comunicação em que os dispositivos são móveis e não são amarrados a qualquer tipo de infra-estrutura fixa de topologia de rede. O dispositivo (nó) móvel na rede AdHocPF não tem o papel somente de fonte e destino de informação, mas também usa os nós participantes como intermediários para retransmitir informação de um nó para outro. Portanto, a AdHocPF tem grande potencial para aplicações em Segurança Pública, indústria, comércio e, é particularmente útil, no fornecimento de apoio a comunicação em locais onde nenhuma infra-estrutura de comunicação exista ou onde o desenvolvimento de uma infra-estrutura fixa não é economicamente viável ou factível.

4.1 Aplicações típicas na área policial

Não é de hoje que a área de Segurança Pública busca novos meios e formas de comunicar-se de forma rápida, eficiente e eficaz durante o cumprimento de tarefas e missões. Todavia, os policiais que participam da labuta diária reclamam da falta de equipamentos de

comunicação e de mecanismos para transferência de dados e informações. Essas situações têm dificultado sobremaneira as ações policiais, tais como: levantamento de local de crime, investigação de inteligência, operações de defesa nacional, identificação de vítimas, grande eventos, varreduras de segurança e antibomba, dente outras não menos importantes. Portanto, a seguir são apresentadas algumas soluções para esses problemas usando a tecnologia das redes sem fios *ad hoc* móveis através da AdHocPF.

4.1.1 Levantamento de local de crime

Local de crime é toda área onde tenha ocorrido um fato que assuma a configuração de infração penal, portanto exigindo as providências da Polícia Judiciária. Analisando esse conceito é possível verificar que estão compreendidos os crimes de qualquer espécie, bem como, todo fato que, não constituindo crime evidente, deva chegar ao conhecimento da polícia, para que seja investigado no intuito de esclarecer o ocorrido. Também nessa mesma linha de raciocínio, é possível compreender local de crime como abaixo se vê:

> Entende-se local de crime como sendo aquela porção do espaço, contínua ou descontínua, onde a infração se materializou por atos e onde, conseqüentemente, existem ou podem existir vestígios materiais da mesma, denunciadores a serem pesquisados. (RABELO, 1996, p.44).

Uma vez identificada a área de abrangência, bem como verificados os procedimentos de isolamento e preservação do local de crime, é chegado o momento de fazer o devido levantamento. O processamento do local de crime deve ser realizado em torno de toda a área onde tenha ocorrido a infração tipificada como crime. Esse levantamento consiste no conjunto de atos praticados pelos peritos criminais diretamente no local da constatação do fato, visando à busca, à identificação, o posicionamento e à coleta dos vestígios que serão utilizados para constatação da materialidade e elucidação da autoria do delito.

Uma grande dificuldade enfrentada pelos peritos é a falta de equipamentos eletrônicos ou computadores que possam armazenar e transferir dados e informações no próprio local de crime que está sendo periciado. A todo o momento, é preciso realizar fotografias, elaborar croquis, fazer descrições narrativas da cena. O levantamento pericial necessita de dispositivos portáteis conectados em uma rede de computadores, como a rede AdHocPF, que possam ser levados pelo perito e, in loco, armazenar, transferir e compartilhar todos os elementos de prova coletados. Dessa forma, os exames periciais serão efetuados com mais agilidade, eficiência e eficácia, não deixando passar despercebido qualquer vestígio coletado.

Outra vantagem, uma vez que se tenham os dispositivos fazendo parte de uma rede *ad hoc* móvel, é a possibilidades dos membros das equipes de perícia realizarem uma checagem e análise prévia de todo o material no próprio local de crime e com isso procederem a novos levantamentos, caso sejam necessários.

- Cenário:

  Locais de crime (morte violenta, acidente de trânsito, arrombamento, incêndios, explosões etc.).

- Serviços que podem ser fornecidos pela AdHocPF:

  1. Elaboração das descrições narrativas no próprio local de crime.

  2. Elaboração de croquis usando dispositivo portátil com programas computacionais especializados para essas tarefas.

  3. Elaboração do álbum de fotografias dos vestígios, já com os respectivos posicionamentos nos croquis.

  4. Elaboração de vídeo do local do crime e locais correlacionados.

  5. Verificação de coordenadas geográficas, imagens, plantas do local (área externa ou interna), mapas.

  6. Transferência de arquivos (textos, sons, imagens e vídeos) entre os peritos criminais usando dispositivos portáteis móveis.

  7. Compartilhamento, em mídia computacional, de trabalho pericial realizado pelos peritos no local. Esse procedimento automatiza a transferência de dados e informações de forma mais rápida, além de facilitar a elaboração do laudo de local uma vez que os dados e informações já estão armazenados em mídia computacional.

  8. Envio e recebimento de mensagens entre os componentes das equipes.

  9. Distribuição de dados e informações do local em tempo real.

10. Possibilidade do uso de equipamentos portáteis móveis (no*tebooks*, *palmtops*, PDAs) em atividades externas no próprio local de crime.

4.1.2 Inteligência policial

Dentre as competências das polícias judiciárias brasileiras estão as atividades de inteligência. A própria Polícia Federal tem uma diretoria em nível estratégico para tratar dos assuntos que dizem respeito às investigações de inteligência, tais como: planejar, orientar, coordenar, controlar, avaliar e promover as atividades de busca, coleta e análise de dados de inteligência policial, com vistas ao combate às organizações criminosas. As operações de inteligência policial são baseadas em dois pilares: a doutrina e a tecnologia de inteligência. A doutrina fornecerá os princípios, valores e metodologias a serem utilizados quando se tratar de investigações, operações e assuntos correlatos a atividade fim de inteligência. Todavia, para que a doutrina de inteligência seja colocada em prática é preciso que sejam fornecidos os meios para concretização dos objetivos. É nesse momento que entra o apoio tecnológico que facilitará e muitas vezes será primordial para o sucesso da operação. Nessa área de atuação policial, torna-se condição *sine qua non* a gestão dos dados, informações, conhecimentos e ações de inteligência. Várias unidades de uma instituição como a Polícia Federal ou mesmo entre os vários órgãos que compõem o Sistema Brasileiro de Inteligência – SISBIN precisam articular entre si para, de forma ágil e dinâmica, trocar as informações necessárias para o sucesso da missão.

Resumidamente, as atividades de inteligência policial envolvem as operações de inteligência, contra-inteligência, antiterrorismo, gerenciamento do banco de dados de inteligência e gestão dos documentos sensíveis. Em cada um desses momentos é importante que haja um processo de comunicação, preferencialmente automatizado, que seja rápido, seguro, dinâmico, flexível e eficiente, pois o tempo é fator primordial para todas as pessoas e organizações envolvidas no processo de busca, coleta e análise de dados, informações e conhecimentos de inteligência policial. É nesse momento que entra a tecnologia de redes sem fios *ad hoc* móveis.

O policial da área de inteligência necessita de uma grande quantidade de dados e informações para que ele possa atuar em uma operação ou missão, pois é necessário conhecer as informações sobre os alvos, os locais, os contatos, as fotos, as imagens, os vídeos, dentre outros. Com o uso da rede AdHocPF, o policial de inteligência poderá coletar, identificar, pesquisar e analisar em tempo real, em qualquer local de alcance da rede e de forma automatizada, os elementos e componentes necessários para que os objetivos da missão sejam alcançados. A grande vantagem do uso dessa tecnologia é que o policial in loco terá todos os dados e informações, sem a necessidade de voltar à base para verificar, compartilhar e transmitir o que foi obtido. Uma vez armazenado o conte-

údo, ao final do dia ou quando for possível o retorno à base de operações, as equipes de policiais terão em mídia computacional elementos de investigação que subsidiarão os chefes, supervisores e coordenadores. De posse de tais elementos obtidos a partir dos dispositivos portáteis sem fios conectados à rede AdHocPF, os responsáveis pela tomada de decisão poderão planejar, orientar, coordenar, controlar, avaliar e promover o aproveitamento dos dados e informações decorrentes das ações de inteligência. Portanto, o uso da rede AdHocPF torna-se ferramenta essencial tanto nos níveis operacional e tático quanto no nível estratégico da inteligência policial em uma instituição de Segurança Pública como a Polícia Federal ou demais órgãos integrantes do SISBIN.

- Cenário:

  Atividades de inteligência policial envolvendo ações, operações e missões de inteligência, contra-inteligência, antiterrorismo, gerenciamento do banco de dados de inteligência e gestão dos documentos sensíveis.

- Serviços que podem ser fornecidos pela AdHocPF:

  1. Identificação, em tempo real, de pessoas, lugares e contatos.

  2. Armazenamento do banco de dados e informações contendo documentos, fotos, imagens, vídeos, mapas, coordenadas, contatos, ou quaisquer elementos que possam auxiliar no processo investigativo.

  3. Compartilhamento do banco de dados e informações de inteligência entre os membros das equipes usando a arquitetura da rede.

  4. Possibilidade do uso de equipamentos sem fios, portáteis e móveis (*notebooks*, *palmtops*, PDAs) em investigações de inteligência policial em ambiente externo, bem como em atividades, operações e missões em campo.

  5. Provimento de comunicação e transferência de arquivos (texto, som, imagem, vídeo) entre os membros das equipes que estão em campo ou quando retornar a base.

  6. Aproveitamento de dados e informações mais realistas decorrentes das operações de inteligência efetuadas em campo para que os responsáveis pelos níveis táticos e estratégicos possam planejar, orientar, coordenar, controlar, avaliar e tomar decisões.

4.1.3 Identificação de vítimas em incidente de destruição em massa

Normalmente um incidente de destruição em massa causa grande impacto e apelo social por uma resposta rápida, eficiente e eficaz. Mas o que vem a ser um incidente de destruição em massa? Um incidente de destruição em massa não é necessariamente um incidente que atinge grandes áreas ou que tem imensa quantidade de mortos e feridos. Na verdade, conforme definido claramente em Jensen (1999), um incidente de destruição em massa é um evento repentino que produz mais mortos e feridos do que os recursos locais podem suportar. Tais incidentes podem ocorrer em qualquer local e a qualquer hora, nenhum país está imune a esse tipo de acontecimento. Exemplos recentes tiveram a participação primordial da Polícia Federal brasileira: as atuações da perícia nos casos do incêndio no supermercado no Paraguai, em 02/08/2004, com 311 mortos; a queda do avião da TAM, vôo JJ 3054, no aeroporto de Congonhas em São Paulo, em 17/07/2007, com 188 mortos; a queda do avião da Air France, vôo 447, próximo a ilha de Fernando de Noronha, em 31/05/2009, com 228 mortos. Todos esses eventos saturaram a infra-estrutura disponível para o pronto atendimento das vítimas. Conforme relatos dos peritos criminais federais que participaram ativamente nesses incidentes mencionados, uma das grandes dificuldades foi a falta de infra-estrutura de comunicação. A infra-estrutura deve ser montada de forma rápida e ao mesmo tempo precisa permitir o compartilhamento de todos os dados, informações e exames realizados em campo, seja na forma de texto, voz, imagem ou vídeo. Uma solução simples, rápida, barata, flexível e portátil seria o uso de nós atuando em uma rede sem fios *ad hoc* móvel com uma arquitetura semelhante à definida na seção 3.1. Nessa proposta, os equipamentos móveis poderiam ser levados para o local do incidente e, no final do dia, as informações obtidas poderiam ser compartilhadas através da rede por todos os membros das equipes por um coordenador geral. A grande vantagem dessa proposta em situações de incidentes de destruição em massa, semelhantes aos apresentados, é que seria possível montar uma rede como a AdHocPF, configurada e em pleno funcionamento em questão de minutos.[2]

Aplicações da AdHocPF

- Cenário:

  Incidente de destruição em massa: incêndio, enchente, desabamento, atentado terrorista, explosão, queda de aviões, colisões.

2 Maiores detalhes sobre como é a atuação da pericia da Polícia Federal em incidentes de destruição em massa podem ser obtidos em (BEZERRA; DAMASCENO, 2006).

- Serviços que podem ser fornecidos pela AdHocPF:

    1. Identificação das vítimas de acordo com os dados e informações coletadas previamente com os familiares.

    2. Montagem um banco de informações com documentos, fotos, vídeos, vestimentas ou qualquer elemento que possa identificar as vítimas. O banco de dados pode ser compartilhado entre os membros das equipes usando a arquitetura da rede no próprio local do incidente, por mais ermo e inóspito que seja.

    3. Provimento de comunicação e transferência de arquivos (texto, som, imagem, vídeo) entre os membros das equipes.

    4. Montagem rápida de um ambiente de rede sem fios para comunicação em tempo real.

    5. Comunicação entre os vários órgãos de Segurança Pública que estão atuando na área do incidente.

4.1.4 Busca e salvamento

Quando se enfrenta uma situação como um terremoto, furacão, incêndio de grandes proporções, atentado terrorista, incidente de destruição em massa, ou evento semelhante, lembra-se imediatamente de chamar os órgãos de Segurança Pública (e. g. polícias, bombeiros, defesa civil) e de Saúde Pública (e. g. hospitais, clínicas e institutos médico-legais). Nessas situações, uma rede tipo a AdHocPF pode ser bastante útil durante as operações de busca e salvamento de vítimas. Em geral, as grandes catástrofes deixam uma boa parte da população sem meios de comunicação ou deixam essa comunicação de forma bem precária. Isso ocorre porque os eventos provocados pelo homem ou os desastres naturais destroem as infra-estruturas existentes. As redes sem fios *ad hoc* móveis, por não usar qualquer tipo de infra-estrutura, podem fornecer a comunicação necessária entre as várias organizações e entidades que auxiliam nos resgates das vítimas e nas operações de salvamento.

Em médio prazo, a rede AdHocPF pode ser utilizada no planejamento, organização, coordenação e controle das buscas por sobreviventes em áreas de desastres, além poder administrar o uso de pequenos sensores computacionais automatizados (robôs) especializados em busca e salvamento (SARANGAPANI, 2007; CORDEIRO; AGRAWAL, 2006). O

uso de robôs não é algo futurista, haja vista que um conjunto de robôs pode compor uma rede de sensores, que nada mais é do que um tipo específico de rede sem fios *ad hoc* móvel. Os robôs podem se comunicar um com o outro usando para isso uma rede sem fios *ad hoc* que fica responsável pela coordenação de todas as atividades desenvolvidas entre os sensores. De acordo com o tamanho de área afetada por um desastre, os robôs (formando uma rede *ad hoc*) podem ser configurados em grupos para procurar áreas menores (zonas, setores, quadrantes) e em seguida juntar todas as informações coletadas em um espaço de tempo muito mais curto do que se fosse utilizada uma rede com fios ou mesmo uma rede sem fios com infra-estrutura. Desse modo, as informações que foram recolhidas em campo podem ser processadas e analisadas, via rede *ad hoc*, fazendo com que a ajuda possa ser direcionada de forma rápida, portátil e com mobilidade para as áreas prioritárias.

Aplicação da AdHocPF:

- Cenário:

  Busca e salvamento de vítimas de terremoto, furacão, enchente, desabamento, desmoronamento, incêndio, atentado terrorista, incidente de destruição em massa, ou evento semelhante.

- Serviços que podem ser fornecidos pela AdHocPF:

  1. Recebimento de dados e informações em tempo real dos membros das equipes de busca e salvamento, bem como dos possíveis sensores robôs.

  2. Provimento de comunicação e transferência de arquivos (texto, som, imagem, vídeo) entre os membros das equipes.

  3. Montagem rápida de um ambiente de rede sem fios para comunicação em tempo real.

  4. Comunicação entre os vários órgãos de Segurança na área do evento.

4.1.5 Segurança em grandes eventos

Para ser considerado como um grande evento na área policial ele deve demandar recursos além do que a força policial local possa dar conta, necessitando do auxílio de

outras unidades e até de outras forças policiais ou militares. Normalmente, esses eventos de segurança envolvem a presença de autoridades e dignitários de outros países, o que recai na competência constitucional da Polícia Federal. A Polícia Federal está constantemente atuando na segurança de grandes eventos, tais como: jogos pan-americanos e encontro mundial da Interpol no Rio de Janeiro, visita do Papa Bento XVI em São Paulo, encontro do Banco Mundial em Belo Horizonte, cúpula dos países árabes e América Latina em Brasília, fórum internacional do meio ambiente e fórum social mundial em Belém, dentre outros. Todavia, um grande problema enfrentado pelos profissionais que atuam nesses tipos de eventos é a falta de tecnologia de comunicação para enviar, receber e transmitir dados e informações no local do evento.

Os coordenadores responsáveis pela segurança (fixa, móvel, velada, tática, antiterrorista, antibomba) de grandes eventos necessitam constantemente de dados e informações sobre os locais onde irão atuar. Contudo, muitas vezes os integrantes das equipes desconhecem quais os locais exatos a serem vigiados, onde ficará cada equipe de segurança, quem são os responsáveis do evento em cada área ou setor onde precisará a segurança, faltam mapas e plantas das edificações, não se sabe quem são os dignitários e possíveis alvos. Essas são apenas algumas das situações enfrentadas pela segurança nesse tipo de cenário que é agravado pelo fato dos eventos estarem dispersos em grandes áreas e terem muitas instituições e pessoas envolvidas. Além disso, a todo o momento as informações sobre a segurança podem ser alteradas: mudanças de horário de partida ou chegada dos dignitários, novos alvos a serem protegidos, alterações do local de embarque e desembarque de autoridades, deslocamentos dos chefes de equipes, mudanças das rotas de escape. Portanto, torna-se imprescindível que todos os membros das equipes possuam dados e informações atualizadas, preferencialmente em tempo real, sobre as tarefas, alvos, deslocamentos, horários, locais e posicionamentos, formas de atuação e demais aspectos de segurança. É nesse momento que os policiais sentem a faltam de uma tecnologia de rede sem fios que seja portátil, flexível, rápida e que possa auxiliar no fornecimento de dados atualizados com mensagens, comandos, textos, fotos, imagens e vídeos necessários para o sucesso da missão. Assim, uma rede sem fios *ad hoc* móvel como a AdHocPF poderá suprir essas carências de segurança, uma vez que não necessita qualquer tipo de infra-estrutura, além de ter a portabilidade, flexibilidade, mobilidade, dinamicidade, rapidez de configuração e pronto atendimento para uso.

- Cenário:

Atividades de segurança policial em grandes eventos.

- Serviços que podem ser fornecidos pela AdHocPF:

    1. Identificação, em tempo real, de autoridades, dignitários, alvos, locais.

    2. Armazenamento do banco de dados e informações contendo documentos, fotos, imagens, vídeos, mapas, coordenadas, contatos, ou qualquer elemento que possa auxiliar na segurança do evento.

    3. Compartilhamento do banco de dados e informações entre os membros das equipes que atuaram no evento.

    4. Possibilidade do uso de equipamentos portáteis móveis (*notebooks*, *palmtops*, PDAs) durante a realização do evento e no ambiente interno e externo, bem como em atividades, operações e missões de prospecção de dados de campo.

    5. Provimento de comunicação e transferência de arquivos (texto, som, imagem, vídeo) entre os membros das equipes em campo ou no retorno à base.

    6. Aproveitamento de dados e informações mais atuais decorrentes das modificações efetuadas em tempo real para que os responsáveis pelos níveis operacionais, táticos e estratégicos possam planejar, orientar, coordenar, controlar, avaliar e promover a segurança do evento.

4.1.6 Varredura antibomba

Na Polícia Federal, a competência para atuar em varredura antibomba cabe aos Peritos Criminais Federais que se especializam durante o curso de formação policial e durante os cursos posteriores que são oferecidos pela instituição, tais como o Curso de Aperfeiçoamento em Contramedidas (CACON) e o Curso de Atualização em Bombas e Explosivos (CABE). Todavia, a atribuição pode ser compartilhada entre os demais integrantes da carreira policial. Uma vez que as competências e os papéis de cada policial estão definidos, cabe aos chefes das unidades técnico-científicas designarem aqueles que efetuarão a tarefa de varredura antibomba. O procedimento de varredura consiste em vistoriar áreas sensíveis, suscetíveis de atentados terroristas ou ações criminosas.

Quando se têm grandes áreas a serem vistoriadas é preciso que haja uma ação coordenada de todas as equipes para que ao final seja conferido se os ambientes foram vistoriados e podem ser liberados. Ocorre que nos locais de maior dimensão, como grandes edifícios, estádios de futebol, ginásios poliesportivos, teatros, centros de convenções, dentre outros, é necessário que os peritos especializados na atuação antibomba estejam com os dados e informações da varredura em tempo real. Atualmente, todo procedimento de coordenação dos trabalhos de varredura antibomba é realizado de forma manual. Usando a AdHocPF todos os chefes de equipes poderiam ter um dispositivos ligado em rede, onde a informação de cada área já vistoriada seria atualizada e enviada ao coordenador das equipes. Com isso, aperfeiçoa-se o trabalho, ganha-se tempo, economizam-se os gastos com mão de obra especializada, tornando a atividade de varredura mais ágil, eficiente, eficaz.

- Cenário:

  Atividades de varredura antibomba.

- Serviços que podem ser fornecidos pela AdHocPF:

  1. Identificação, *in loco*, das áreas a serem vistoriados com texto, imagens, fotos e vídeos.

  2. Armazenamento do banco de dados e informações contendo documentos, fotos, imagens, vídeos, mapas, coordenadas, contatos, ou qualquer elemento que possa auxiliar na varredura.

  3. Compartilhamento do banco de dados e informações entre os membros das equipes que atuaram na varredura.

  4. Possibilidade do uso de equipamentos portáteis móveis (notebooks, palmtops, PDAs) durante a realização das vistorias antibomba, tanto em ambiente interno quanto externo.

  5. Fornecimento de comunicação e transferência de arquivos (texto, som, imagem, vídeo) entre os membros das equipes que estão em campo ou quando retornar ao posto de comando.

  6. Aproveitamento de dados e informações em tempo real para que os responsáveis pelos níveis operacionais, táticos e estratégicos possam planejar, orientar, coordenar, controlar, promover a varredura antibomba.

4.1.7 Defesa e segurança nacional

Comunicações seguras são fundamentais para qualquer operação de defesa da soberania e segurança nacional. Muitas operações acontecem em locais onde a infra-estrutura de comunicação não está disponível. O uso de redes sem fios *ad hoc* móveis em tais situações faz com que as operações tenham mais possibilidades de sucesso. As unidades policiais, principalmente na fronteira brasileira, estão constantemente envolvidas na defesa do território nacional. Operações conjuntas da Polícia Federal com as forças armadas brasileira (marinha, exército e aeronáutica) e com as polícias de outros países fronteiriços envolvem momentos em que a comunicação entre as corporações é elemento de suma importância para o bom desfecho da missão. Nesse caso, a rede AdHocPF poderia ser usada para comunicação entre os integrantes das equipes.

O uso de helicópteros, aviões (tripulados ou não), lanchas e embarcações pela Polícia Federal em operações de defesa estratégica faz com que haja constantemente a necessidade de comunicação e transferência de informações entre as equipes com os mais variados tipos de equipamentos. Os meios de transporte usados pela Polícia Federal, além de outros providos pelas forças de defesa do território brasileiro, podem gerar problemas sérios nas comunicações, pois cada unidade de uma força tem os próprios equipamentos, muitas vezes incompatíveis com outros dispositivos de outras unidades que atuam na mesma missão. Uma solução para a situação seria a montagem de uma rede sem fios *ad hoc* móvel, como a proposta pela AdHocPF, que possibilitaria a comunicação, transmissão de dados em rede e o compartilhamento de arquivos.

Outra possibilidade do uso da AdHocPF na área de defesa e segurança nacional é aplicá-la para verificar o movimento de pessoas, infratores, criminosos, bandos e quadrilhas em determinada área: região de fronteira, favela, local ermo ou de difícil acesso. Nesse tipo de aplicação poderiam ser colocados centenas ou milhares de sensores (pequenos dispositivos sem fios) na área a ser policiada e que necessitasse de vigilância constante. O espalhamento dos sensores na área selecionada pode ser feito por via área, marítima, fluvial, lacustre, terrestre. Uma vez introduzidos esses sensores, eles transmitiriam os dados e informações para AdHocPF que estaria instalada em um meio de transporte rápido (avião, helicóptero, lancha) que ao passar pelo local faria a leitura dos dados contidos nos sensores e os enviaria para uma base segura. Portanto, haveria uma coleta de dados pela rede *ad hoc* e após processados seriam transformados em informações estratégicas com o propósito de defesa e segurança nacional.

A tecnologia de uso de sensores sem fios para tais aplicações já está disponível e em uso (WU; TSENG, 2007; CORDEIRO; AGRAWAL, 2006; SARANGAPANI, 2007). Devido ao tamanho minúsculo os sensores, quando espalhados por via aérea,

permanecem suspensos no ar durante algum tempo. Durante esse tempo, eles já podem coletar dados para os quais eles foram programados e em seguida enviar esses dados para processamento em uma local central onde tenha rede com características similares a AdHocPF. De posse de tais informações, os gestores e coordenadores da missão podem decidir quais os próximos passos a serem efetuados.

Esse tipo de aplicação já está sendo utilizada para verificação do deslocamento de tropas pelos exércitos de vários países desenvolvidos, tais como EUA, França, Inglaterra e outros (HAAS; TABRIZI, 1998; PEREIRA, 2004).

Aplicação da AdHocPF:

- Cenário:

  Ambiente hostil em região ou área fronteiriça de difícil acesso.

- Serviços que podem ser fornecidos pela AdHocPF:

  1. Coleta e processamento de dados fornecidos pelas equipes ou pelos sensores computacionais espalhados.

  2. Compartilhamento de dados e informações em tempo real entre os membros das equipes.

  3. Provimento de comunicação e transferência de arquivos (texto, som, imagem, vídeo) entre os membros das equipes.

  4. Montagem rápida de um ambiente de rede sem fios móvel para comunicação em tempo real.

  5. Comunicação entre os vários órgãos de que atuarão na missão de defesa e segurança nacional.

4.1.8 Ambiente acadêmico da ANP

A maioria das instituições acadêmicas já possui a tecnologia de comunicação sem fios ou está no processo de providenciá-la. A Academia Nacional de Polícia (ANP) ainda não possui esse modelo de rede, mas está estudando a forma de adquirir para alguns setores e unidades. Um ambiente de comunicação sem fios na ANP poderá fornecer aos estudantes e

à instituição de ensino um local apropriado para a difusão do conhecimento e para o cumprimento da missão pedagógica. No caso específico das redes do tipo sem fios *ad hoc* móveis, elas podem inovar as formas e os meios de transmissão desse conhecimento no ambiente de ensino e pesquisa. Por exemplo, a AdHocPF pode ser utilizada entre o professor e os estudantes para transferir arquivos (textos, sons, imagens e vídeos) e compartilhar recursos (impressoras, digitalizadores) durante uma aula específica e, ao final, basta encerrar a conexão. O uso desse tipo de rede pode prover um mecanismo fácil e conveniente para o professor distribuir os materiais didáticos em tempo real a todos os estudantes na sala de aula, como também para os estudantes submeterem as tarefas ao professor. Uma vez que os dispositivos estejam configurados, as transferências de dados e informações e o compartilhando de recursos entre os participantes da aula podem ser efetuados com o uso da AdHocPF de forma tão fácil quanto um simples clicar do teclado ou do *mouse*. Devido a portabilidade, a dinamicidade e a mobilidade que esse tipo de rede fornece, as tarefas de transferência e compartilhamento podem ser realizadas também em aulas externas ou em instruções de campo. Dessa forma o professor fica livre para ministrar o conteúdo programático, seja qual for o tipo e local de instrução: aula de armamento e tiro, bomba e explosivo, investigação operacional, vigilância, navegação, dentre outras.

Outrossim, uma rede como a projetada para AdHocPF também pode ser utilizada na apresentação de conferências, palestras e pesquisas, haja visto que essa tecnologia permite que os ouvintes e as partes interessadas possam acompanhar o conteúdo, em tempo real, nos próprios computadores ou dispositivos portáteis. Para isso, basta compartilhar os arquivos. Caso seja de interesse, a AdHocPF também pode se conectar com a *Internet* e fazer uso de todos os serviços fornecidos pela grande rede mundial.

Aplicação da AdHocPF:

- Cenário:

  6. Aula e instruções em ambientes fechados (salas de aula, auditórios) ou abertos (aula de campo), compartilhamento de recursos, apresentação de palestras, conferências e pesquisas avançadas.

- Serviços que podem ser fornecidos pela AdHocPF:

  1. Transferência de arquivos (textos, sons, imagens e vídeos) entre professores e alunos com o uso de dispositivos portáteis móveis.

2. Compartilhamento recursos (impressoras, digitalizadores, ou qualquer dispositivo com placa de rede sem fios).

3. Distribuição de materiais didáticos em tempo real a todos os estudantes na sala de aula.

4. Possibilidade do uso de equipamentos portáteis móveis (*notebooks*, *palmtops*, PDAs) em aulas externas e em atividades de campo.

5. Apresentação de conferências, palestras e pesquisas.

4.2 Testes

Depois de configurada a rede, é importante que sejam realizados testes e simulações da rede AdHocPF em pleno funcionamento. Inicialmente foram utilizados três nós com comunicação direta. Em seguida, os três nós foram compartilhados com a WLAN corporativa que estava conectada à *Internet*. Por último, foram utilizados dez dispositivos móveis, fornecidos por este signatário, pelo SETEC/SR/DPF/CE e pelo LARCES/UECE.

Vale destacar que para maioria das aplicações que se pretende utilizar para AdHocPF está previsto o uso de nós em rede sem fios *ad hoc* móvel do tipo comunicação direta (ver seção 2.2), como o pretendido nos testes das seções 4.2.1 e 4.2.2, a seguir. Contudo, também foi verificado a funcionalidade dos recursos e serviços da AdHocPF quando conectada a *Internet*, segundo pode ser verificado nas seções 4.2.3 e 4.2.4. Também se torna essencial esclarecer que a rede AdHocPF, quando em comunicação direta, trabalha com velocidade de 11Mbs (onze megabits por segundo), conforme indicador fornecido pelo Windows. Tal medida de desempenho de velocidade pode ser verificada na Figura 19.

4.2.1 AdHocPF com três nós

Inicialmente foram utilizados três nós comunicando diretamente um com o outro (ver seção 2.2). Com essa configuração foi possível transferir arquivos e compartilhar recursos de forma rápida, eficiente e sem maiores dificuldades. Mesmo quando da transferência de arquivos de grande capacidade (maiores do que 10MB).

- Configuração

Nós	
Qtd	Descrição
01	*Notebook* com placa de rede sem fios embutida, marca HP, modelo Pavilion dv 2000, fabricado na China. Proprietário: Uso pessoal desse signatário.
02	*Notebooks* com placas de rede sem fios embutidas, marca Lenovo, modelo 2008-CTO, fabricado na China. Proprietário: Grupo de Perícias de Informática do SETEC/SR/DPF/CE.

Serviços testados na AdHocPF	
Serviço	Desempenho
Compartilhamento de Arquivos	Todos os nós da rede visualizaram os outros nós e seus respectivos compartilhamentos.
	Foi possível compartilhamento de arquivos. Os nós puderam incluir, excluir e modificar os arquivos de acordo com as permissões fornecidas pelo proprietário dos arquivos (somente leitura, possível leitura e escrita, oculto). Foi possível o compartilhamento de periférico, no caso impressoras.
Transferência de Arquivos	Foi possível transferir arquivos de um nó para outro. Foi possível transferir arquivos do tipo texto, som, imagem e vídeo. Foi possível imprimir os arquivos nas impressoras compartilhadas.

4.2.2 AdHocPF com três nós conectados a Internet

Foram utilizados três nós comunicando diretamente um com o outro. Na configuração o nó principal foi conectado a uma WLAN que acessa a *Internet* sem fios do SETEC/SR/DPF/CE. Com essa configuração foi possível realizar todas as tarefas e serviços fornecidos anteriormente (seção 4.2.1), além de prover as facilidades e serviços da *Internet*.

- Configuração

Nós	
Qtd	Descrição
01	*Notebook* com placa de rede sem fios embutida, marca HP, modelo Pavilion dv 2000, fabricado na China. Proprietário: Uso pessoal desse signatário.
02	*Notebooks* com placas de rede sem fios embutidas, marca Lenovo, modelo 2008-CTO, fabricado na China. Proprietário: Grupo de Perícias de Informática do SETEC/SR/DPF/CE.

Serviços testados na AdHocPF	
Serviço	**Desempenho**
Compartilhamento de Arquivo	Todos os nós da rede visualizaram os outros nós e seus respectivos compartilhamentos.
Compartilhamento de Arquivo	Foi possível compartilhamento de arquivos. Os nós puderam incluir, excluir e modificar os arquivos de acordo com as permissões fornecidas pelo proprietário dos arquivos (somente leitura, possível leitura e escrita, oculto). Foi possível o compartilhamento de recursos, no caso impressoras.
Transferência de arquivos	Foi possível transferir arquivos de um nó para outro. Foi possível transferir arquivos do tipo texto, som, imagem e vídeo. Foi possível imprimir os arquivos nas impressoras compartilhadas.
Acesso a Internet	Todos os serviços fornecidos pela Internet, tais como: leitura de e-mails, acessos a sítios da Internet, envio e recebimento de mensagens, acesso a comunidades de relacionamentos, *download* de arquivos, dentre outros.

4.2.3 AdHocPF com dez nós

Foram utilizados dez dispositivos sem fios móveis, sendo fornecidos: dois por este signatário, dois pelo SETEC/SR/DPF/CE e seis pelo LARCES/UECE. Todos os nós formavam uma rede sem fios *ad hoc* móvel com comunicação direta (conforme definido na seção 2.2). Nessa configuração, todos os testes foram realizados na sala 01 do LARCES/UECE. Não foi possível medir com precisão (nó a nó) o decréscimo de desempenho da rede, pois não havia programas verificadores de desempenho real dos nós a época de realização dos testes. Mesmo assim, foram medidos os tempos de acesso a grandes arquivos (com capacidade acima de 10MB). Nesse caso, foi constatado que houve um decréscimo médio de tempo na ordem de 10% em relação aos acessos (envio e recebimento de pacotes de dados) quando havia apenas três nós. Vale relembrar que a rede AdHocPF trabalha com velocidade de 11Mbs (onze megabits por segundo), conforme indicador fornecido pelo Windows (ver Figura 19).

- Configuração

Nós	
Qtd	**Descrição**
01	Assistente Pessoal de Dados – PDA (iPAQ) com placa de rede sem fios embutida, marca HP, modelo Travel Companion, fabricado na China. Proprietário: Uso pessoal desse signatário.
01	*Notebook* com placa de rede sem fios embutida, marca HP, modelo Pavilion dv 2000, fabricado na China. Proprietário: Uso pessoal desse signatário.
02	*Notebooks* com placas de rede sem fios embutidas, marca Lenovo, modelo 2008-CTO, fabricado na China. Proprietário: Grupo de Informática do SETEC/SR/DPF/CE.
06	*Notebooks* com placas de rede sem fios embutidas, marca Toshiba, modelo Satellite, fabricado na China. Proprietário: LARCES/UECE.

Serviços testados na AdHocPF	
Serviço	**Desempenho**
Compartilhamento de Arquivo	Todos os nós da rede visualizaram os outros nós e seus respectivos compartilhamentos.
Compartilhamento de Arquivo	Foi possível compartilhamento de arquivos. Os nós puderam incluir, excluir e modificar os arquivos de acordo com as permissões fornecidas pelo proprietário dos arquivos (somente leitura, possível leitura e escrita, oculto). Foi possível o compartilhamento de recursos, no caso impressoras.
Transferência de arquivos	Foi possível transferir arquivos de um nó para outro. Foi possível transferir arquivos do tipo texto, som, imagem e vídeo. Foi possível imprimir os arquivos nas impressoras compartilhadas.

4.2.4 AdHocPF com dez nós conectados a Internet

Foram utilizados dez dispositivos sem fios, sendo fornecidos: dois por este signatário, dois pelo SETEC/SR/DPF/CE e seis pelo LARCES/UECE. Nessa configuração o nó principal foi conectado a WLAN que acessa a *Internet* sem fios do LARCES/UECE. Com a configuração foi possível realizar todas as tarefas e serviços fornecidos anteriormente (seção 4.2.2), inclusive com as mesmas facilidades e serviços da *Internet*. A rede do LARCES/UECE opera a uma velocidade de 2Gbps (dois gigabits por segundo). Não foi possível medir com precisão (nó a nó) o decréscimo de desempenho da rede, pois não havia programas verificadores de desempenho real dos nós a época de realização dos testes. Todavia, o desempenho médio dos acessos (envio e recebimento de pacotes de dados) a *Internet* caiu 15% em relação à rede AdHocPF que possuía apenas três nós conectados a *Internet*, principalmente no que

se refere ao download de arquivos grandes (superiores a 10MB).

- Configuração

Nós	
Qtd	**Descrição**
01	Assistente Pessoal de Dados – PDA (iPAQ) com placa de rede sem fios embutida, marca HP, modelo Travel Companion, fabricado na China. Proprietário: Uso pessoal desse signatário.
01	*Notebook* com placa de rede sem fios embutida, marca HP, modelo Pavilion dv 2000, fabricado na China. Proprietário: Uso pessoal desse signatário.
02	*Notebooks* com placas de rede sem fios embutidas, marca Lenovo, modelo 2008-CTO, fabricado na China. Proprietário: Grupo de Informática do SETEC/SR/DPF/CE.
06	*Notebooks* com placas de rede sem fios embutidas, marca Toshiba, modelo Satellite, fabricado na China. Proprietário: LARCES/UECE.

Serviços testados na AdHocPF	
Serviço	**Desempenho**
Compartilhamento de Arquivo	Todos os nós da rede visualizaram os outros nós e seus respectivos compartilhamentos.
Compartilhamento de Arquivo	Foi possível compartilhamento de arquivos. Os nós puderam incluir, excluir e modificar os arquivos de acordo com as permissões fornecidas pelo proprietário dos arquivos (somente leitura, possível leitura e escrita, oculto). Foi possível o compartilhamento de recursos, no caso impressoras.
Transferência de arquivos	Foi possível transferir arquivos de um nó para outro. Foi possível transferir arquivos do tipo texto, som, imagem e vídeo. Foi possível imprimir os arquivos nas impressoras compartilhadas.
Acesso a Internet	Todos os serviços fornecidos pela Internet, tais como: leitura de e-mails, acessos a sítios da Internet, envio e recebimento de mensagens, acesso a comunidades de relacionamentos, *download* de arquivos, dentre outros.

4.3 Desafios

Embora as redes sem fios *ad hoc* móveis sejam um grande avanço tecnológico, ainda há muitos desafios a serem localizados e ultrapassados para que se possa usufruir todos os benefícios que elas podem oferecer. Assim como qualquer rede sem fios *ad hoc* móvel, a AdHocPF pode operar em ambientes variados, desde os mais previsíveis até os mais inóspitos, todavia possui os seguintes desafios e restrições de uso:

- Limitação da largura da banda

As redes sem fios de uma forma geral possuem uma largura de banda limitada, conseqüentemente somente uma quantia limitada de informação pode ser transmitida durante certo período de tempo. Espera-se que novas técnicas de transmissão mais eficientes venham fazer com que esse tipo de rede tenha sua capacidade de largura de banda aumentada. Porém, com os novos avanços da telefonia móvel, tais como as tecnologias CDMA, GPRS e 3G fazem com que as redes móveis também possam utilizar essas tecnologias para aumentar a sua capacidade de transmissão em uma largura de banda.

- Limitação da capacidade e vida útil das baterias utilizadas nos dispositivos

Dispositivos de comunicação sem fios móveis não têm autonomia ilimitada para seu funcionamento. Esses dispositivos usam baterias que possuem poder de carga e vida útil bastante limitada. Quanto maior for o uso da rede sem fios mais curta será a vida útil das baterias dos dispositivos. Atualmente estão sendo realizados esforços para projetar dispositivos que consomem menos energia e ajustam a força dos sinais de comunicação conforme distância de comunicação. Além disso, estão sendo desenvolvidas técnicas de processamento de sinal mais eficientes e algoritmos que demandarão muito menos consumo de energia. Outro ponto a ser levado em consideração quando se trata de consumo de energia é que os avanços das tecnologias de semicondutor, fabricando componentes eletrônicos cada vez menores e menos consumidores de energia, fazem com que tenhamos um futuro promissor para as redes sem fios. Como o tamanho desses dispositivos móveis continua encolhendo, cada vez mais estão sendo acrescentadas características e funcionalidades a esses dispositivos de forma a consumir menos energia. O desafio atual é manter essa tendência de diminuição de consumo de energia. Uma esperança promissora são os estudos realizados com a nanotecnologia.

- Fragilidade na segurança;

Ambientes de comunicação sem fios são mais propensos a riscos de segurança que outros, e as redes sem fios *ad hoc* não são exceção. Qualquer nível de segurança de informação desejada pode ser alcançado nessas redes, mas isto levará a um custo adicional, além de requerer uma melhora na largura da banda para transmissão. Ao contrário das redes cabeadas, onde a infra-estrutura fica dentro das corporações, as redes sem fios usam ondas de rádio como meio de transmissão, o que aumenta as chances de acessos não autorizados. Sendo, portanto, mais susceptíveis a ataques de hackers e pessoas mal intencionadas, quando não configuradas adequadamente. As pesquisas sobre segurança em redes sem fios *ad hoc* móveis ainda estão nos primeiros momentos. Os pesquisadores estão trabalhando para descobrir mecanismos que possam fornecer informação segura e ao mesmo tempo deixar a rede viável para uso. Maiores detalhes sobre as vulnerabilidades da segurança e os vários tipos de ataques sofridos pelas redes sem fios podem ser encontrados em (NOGUEIRA, 2004, 2006; NOGUEIRA; JÚNIOR, 2008).

- Sobrecarga de comunicação;

Reduzir a sobrecarga de comunicação entre os dispositivos durante as transmissões é um dos maiores desafios para as redes sem fios do tipo *ad hoc*. Quando a informação precisa ser transmitida de um dispositivo para outro, uma rota ou caminho precisa ser estabelecido para que essa informação possa ser trocada. Além disso, quando há comunicação entre vários dispositivos é necessário que haja procedimento para compartilhamento dos recursos comuns o que gera uma nova demanda por comunicação e conseqüentemente mais largura de banda. A tecnologia de *Bluetooth* e a IEEE 802.11 provêem vários mecanismos para compartilhamento de recursos que atenuam a sobrecarga de comunicação. Outro desafio em relação à sobrecarga é que as redes *ad hoc* possuem topologia dinâmica. Logo, para estabelecer uma rota entre dois dispositivos que se comunicam, os nós da rede precisam ter a localização dos outros dispositivos. Os procedimentos para estabelecer as rotas têm que ser dinâmicos e adaptáveis, pois a rota que é estabelecida no começo de transferência da informação entre dois dispositivos móveis pode não ser a mesma quando a informação alcança seu destino final. Dessa forma, a rota percorrida pela informação precisa ser tão atual quanto possível todo o tempo. Há várias possibilidades de se estabelecer e manter rotas. Podem ser estabelecidas rotas de forma proativa ou reativa (sob demanda). Os procedimentos que estabelecem rotas de forma proativa causam mais sobrecarga nas comunicações, pois estabelecem todas as rotas possíveis. Por outro lado, as rotas sob demanda causarão menos sobrecarga, pois somente serão estabelecidas as rotas neces-

sárias para comunicação em cada momento e não todas as rotas como no caso proativo. Contudo, uma rota sob demanda introduzirá mais tempo de espera pelos dispositivos, haja vista que eles terão que esperar que a rota seja estabelecida antes da comunicação e transferência da informação. Hoje em dia há muitas propostas de mecanismos de roteamento híbridos que usam tanto o roteamento proativo quanto o reativo dependendo da situação. Assim, os desafios de se estabelecerem as melhores rotas possíveis com menos sobrecarga nas comunicações ainda continuam em aberto.

- Redução da força do sinal

As radiações eletromagnéticas são atenuadas quando atravessam alguns tipos de matéria como, por exemplo, quando um sinal de rádio atravessa uma parede. Há ainda o problema do nó oculto, onde obstruções físicas presentes no ambiente (por exemplo, um outro nó, um anteparo, um edifício, uma montanha) pode impedir que haja comunicação direta entre os nós. Além disso, seguindo esse mesmo raciocínio, o próprio sinal pode se dispersar no ar livre, resultando na redução da sua força (atenuação de percurso) à medida que aumenta a distância entre o emissor e o receptor. Isso pode causar uma redução da força do sinal de tal sorte que nós podem não ter potência suficiente para detectar as transmissões um do outro.

- Interferência de outras fontes

Várias fontes de rádio transmitindo na mesma banda de freqüência sofrerão interferências umas das outras. Por exemplo, telefones sem fios de 2,4 GHz podem interferir nas redes sem fios e fazer com que elas não funcionem bem. Além da interferência de fontes transmissoras, o ruído eletromagnético presente no ambiente (por exemplo, um motor ligado, um microondas em funcionamento) pode gerar interferências indesejáveis na rede sem fios.

- Propagação multivias

Quando a propagação do sinal de rádio usa múltiplos caminhos, parte da onda eletromagnética se reflete em objetos (por exemplo, grandes porções de metais brilhosos, espelhos naturais e artificiais) e também no solo tomando caminhos diferentes entre um emissor e um receptor. Isso resulta no embaralhamento do sinal recebido no nó destino. Além disso, os objetos que se movimentam entre o emissor e o receptor também podem fazer com que a propagação multivias crie dificuldades na transmissão entre os nós.

CONSIDERAÇÕES FINAIS

Cada vez mais o mundo globalizado faz uso dos recursos computacionais disponíveis com o objetivo de aplicá-los em diversas áreas de atuação e conhecimento. Com o passar do tempo, a popularização das redes de computadores, notadamente a *Internet*, acelerou os avanços tecnológicos chegando até às redes sem fios. Com isso, a sociedade contemporânea tem utilizado cada vez mais os dispositivos sem fios portáteis. Essa nova tecnologia sem fios, mas especificamente as redes sem fios sem infra-estrutura, também conhecida como redes *ad hoc*, corroboraram essa tendência mundial. Atualmente, em vários países desenvolvidos como Inglaterra, Estados Unidos, Alemanha e França, as operações táticas militares e operações de busca e salvamento são os principais segmentos de uso dessa tecnologia. Unidades de combate ou resgate, equipadas com dispositivos portáteis de comunicação sem fios, em incursão em terrenos hostis, perigosos ou de difícil acesso constituem exemplos práticos do uso dessas redes sem fios *ad hoc* móveis no contexto da segurança com a finalidade de trocar informações de forma simples, rápida, dinâmica e, na medida do possível, segura.

Destarte, a Polícia Federal brasileira, como instituição de Segurança Pública de abrangência nacional e ícone nos avanços tecnológicos de polícia científica, não pode ficar a margem dessa nova tecnologia. Logo, a matéria suscitou estudos e pesquisas pormenorizados sobre como, onde, quando e por que aplicar as redes sem fios *ad hoc* móveis nas ações policiais. Vale ressaltar que, na bibliografia pesquisada, foram encontrados somente aplicações do uso de redes *ad hoc* em segurança da área militar, o que caracteriza o ineditismo deste estudo e algo inovador para as polícias do Brasil e demais países.

Com o intuito de atingir os objetivos delimitados no escopo desse trabalho, foram direcionados os estudos metodológicos nas três principais categorias de pesquisa: a pesquisa bibliográfica, a pesquisa descritiva e a pesquisa experimental. Para isso foram formuladas várias hipóteses que ao final provaram ser válidas, haja vista que a atual conjuntura tecnológica da Polícia Federal já possui policiais com conhecimento técnico-científico, bem como dispositivos e equipamentos necessários para criar, configurar, aplicar, testar e manter a tecnologia das redes sem fios do tipo *ad hoc* móveis. Ademais, conforme demonstrado neste estudo, é possível aplicar esse tipo rede nas mais variadas ações policiais, tais como: atividades de inteligência policial, levantamentos de locais de crime, atividades de identificação de vítimas de incidentes de destruição em massa, operações de busca e salvamento, atividades de segurança de grandes eventos, varreduras antibomba, situações de defesa e segurança nacional, tarefas acadêmicas de formação policial, dentre outras aplicações não menos importante que a mente humana possa conceber como cenário favorável para o uso dessa nova tecnologia.

Como contribuições para as comunidades acadêmica, científica e policial este trabalho

apresentou o referencial teórico necessário para uso das novas tecnologias e padrões de redes sem fios; caracterizou as redes sem fios *ad hoc* móveis; construiu uma rede sem fios *ad hoc* móvel, a AdHocPF; estudou e testou o funcionamento da AdHocPF com vários equipamentos disponíveis no SETEC/SR/DPF/CE e no LARCES/UECE; analisou as vantagens e desvantagens do uso das redes sem fios do tipo *ad hoc*; efetuou o levantamento e prospecção de tarefas da rotina policial onde redes *ad hoc* móveis poderiam ser utilizadas; elaborou diversos cenários de aplicações para uso da AdHocPF; e, finalmente, demonstrou a aplicabilidade e a praticidade das redes sem fios *ad hoc* móveis em cenários policiais.

Vale destacar que, como toda nova tecnologia, as redes sem fios *ad hoc* móveis demandam pesquisas constantes e precisam superar vários desafios. Tais preocupações são objeto de estudo em muitas universidades e centros de pesquisa espalhados no mundo em várias dissertações de mestrado e teses de doutorado. Essa temática também foi abordada como parte deste trabalho onde vários desafios foram apresentados,como uma evolução natural das redes de computadores tradicionais até chegar às relevantes redes sem fios *ad hoc* móveis.

Portanto, a grande questão tratada neste trabalho foi verificar a possibilidade de se aplicar a tecnologia de rede sem fios *ad hoc* móvel na práxis policial, cuja aplicabilidade foi evidenciada nas pesquisas e testes de campo. Todavia, essa tecnologia não se restringe apenas a ser um instrumento policial de deslinde das infrações penais, mas principalmente como ferramenta de enfrentamento das adversidades e agruras da área de segurança pública, tornando as tarefas, operações e missões policiais simples, dinâmicas, eficientes e eficazes.

REFERÊNCIAS

BASAGNI, S. et al. **Mobile *Ad hoc* Networking**. Hoboken: Wiley-IEEE Press, 2004.

BEZERRA, C. C.; DAMASCENO, C. T. M. **Atuação Pericial em Incidentes em Massa: metrô de Brasília (Situação Hipotética)**, Brasília-DF, 2006. Monografia. Academia Nacional de Polícia.

COMER, D. E. **Redes de Computadores e *Internet***. 4. ed. São Paulo: Editora Bookman, 2007.

CORDEIRO, C. M.; AGRAWAL, D. P. ***Ad hoc* & Sensor Networks: theory and applications**. Hackensack: World Scientific Publishing, 2006.

DIXIT, S.; PRASAD, R. (Org.). **Technologies for Home Networking**. Hoboken: John Wiley & Sons, 2005.

FERNANDES, N. C. **Controle de Acesso Distribuído para Redes *Ad hoc***. Rio de Janeiro, 2008. Dissertação de Mestrado. Engenharia Elétrica – Universidade Federal do Rio de Janeiro.

FLICKENGER, R. **Building Wireless Community Networks**. Cambridge: O'Reilly, 2003.

GAST, M. 802.11 **Wireless Networks: The Definitive Guide**. Cambridge: O'Reilly, 2002.

HAAS, Z. J.; TABRIZI, S. **On Some Challenges and Design Choices in *Ad hoc* Communications**. In: International Conference for Military Communications, 1998, Bedford. Proceedings IEEE MILCOM. Bedford, 1998.

JENSEN, R. A. **Mass Fatality and Casualty Incidents – A Field Guide**. Washington, DC: CRC Press, 1999.

KAVEH, P. **Wireless Information Networks**. Hoboken: John Wiley & Sons, 2005.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a *Internet*: uma nova abordagem**. 3. ed. São Paulo: Addison Wesley; 2006.

KWOK, Y. K. R.; LAU, V. K. N. **Wireless *Internet* and Mobile Computing: Interoperability and Performance**. Hoboken: John Wiley & Sons, 2007.

NIEBERT, N. et al; **Ambient Networks Co-Operative Mobile Networking for Wireless World**. West Sussex: John Wiley & Sons, 2007.

NOGUEIRA, J. H. M. **Alerta: as redes sem fios chegaram**. In: I Conferência Internacional de Perícias em Crimes Cibernéticos, 1., 2004, Brasília. Anais I ICCyber. Brasília: DPF, 2004. p. 73-79.

_____. **Mobile Intelligent Agents to Fight Cyber Intrusions**. International Journal of Forensic Computer Science, Brasília: Brazil, 2006.

_____. **Ontology for Complex Mission Scenarios in Forensic Computing**. In: II Conferência Internacional de Perícias em Crimes Cibernéticos, 1., 2007, Guarujá. Anais II ICCyber. Guarujá: DPF, 2007. p. 25-29.

NOGUEIRA, J. H. M; JÚNIOR, J. C. **Computação Autonômica Aplicada à Criminalística Computacional**. In: VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2008, Gramado. Anais do SBSEG. Gramado. 2008. p. 263-266.

PEREIRA, I. C. M. **Análise do Roteamento em Redes Móveis *Ad hoc* em Cenários de Operações Militares**. Rio de Janeiro, 2004. Dissertação de Mestrado. Engenharia Elétrica – Universidade Federal do Rio de Janeiro.

RABELO, E. **Curso de Criminalística**. Porto Alegre: Editora Sagra-Luzzatto, 1996.

RODRIGUES, M. **Redes Móveis *Ad hoc*: necessidades e desafios**. Porto, 2004. Monografia de Engenharia Informática – Instituto Superior de Engenharia do Porto.

SARANGAPANI, J. **Wireless *Ad hoc* and Sensor: networks, protocols, performance, and Control**. Boca Raton: CRC Press, 2007.

SARKAR, S. K.; BASARAVAJU, T. G.; PUTTAMADAPPA, C. ***Ad hoc* Mobile Wireless Networks: principles, protocols, and applications**. Boca Raton: Auerbach Publications, 2008.

STALLINGS, W. **Criptografia e Segurança de Redes: princípios e práticas**. 4. ed. São Paulo: Editora Prentice Hall, 2006.

TANENBAUM, A. S. **Redes de Computadores**. 4. ed. São Paulo: Editora Campus, 2003.

WALKE, B. H.; MANGOLD, S.; BELERMANN, L. IEEE 802 **Wireless Systems Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence**. West Sussex: John Wiley & Sons, 2006.

WEBB, W. **Wireless Communications: the future**. Hoboken: John Wiley & Sons, 2007.

WU, S. L.; TSENG, Y. C. **Wireless *Ad hoc* Networking: personal-area, local-area, and the sensory-area networks**. Boca Raton: Auerbach Publications, 2007.