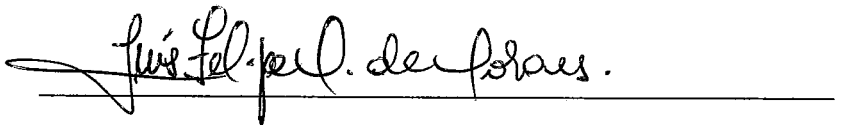
PROVA DE CONCEITO DE UM SISTEMA PARA O GERENCIAMENTO INTEGRADO DE SEGURANÇA EM REDES SEM FIO

Airon Fonteles da Silva

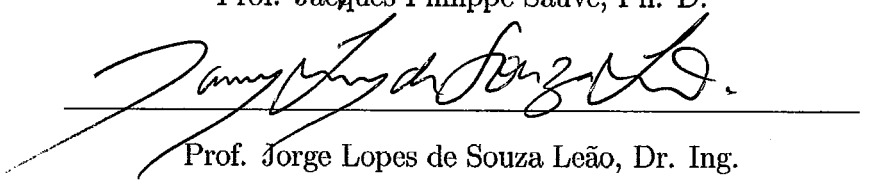
DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Aprovada por:

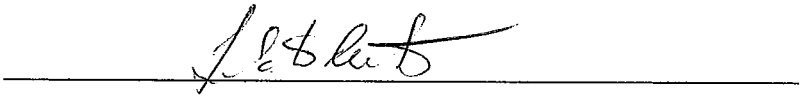


Prof. Luís Felipe Magalhães de Moraes, Ph. D.

Prof. Jacques Philippe Sauvé, Ph. D.



Prof. Jorge Lopes de Souza Leão, Dr. Ing.



Prof. Inês de Castro Dutra, Ph. D.

RIO DE JANEIRO, RJ - BRASIL

JULHO DE 2006

DA SILVA, AIRON FONTELES

Proposta de um Modelo Para o Gerenciamento Integrado de Segurança em Redes Sem Fio [Rio de Janeiro] 2006

XIV, 82 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006)

Dissertação - Universidade Federal do Rio de Janeiro, COPPE

1. Redes Locais Sem Fio
2. Gerenciamento
3. Segurança

I. COPPE/UFRJ II. Título (série)

Dedicatória

Aos meus pais Olympio Cipriano da Silva (in memoriam) e Maria de Lourdes Fonteles da Silva.

Agradecimentos

Primeiramente, gostaria de agradecer a Deus por me conceder a vida e por e pela graça de poder realizar este trabalho.

A minha querida mãe Maria de Lourdes, e meus irmãos Olympio e Ana Gardênia. Sempre me apoiaram nas minhas decisões e me deram força nos momentos mais difíceis dessa jornada. Agradeço também a meu tio Edmilson e tia Maria, por terem me acolhido assim que cheguei ao Rio e por me darem total apoio no início dessa caminhada. Em especial gostaria de agradecer a minha mãe, por pacientemente ter ouvido nas minhas ligações todos os problemas e dificuldades que enfrentei. Por todas as vezes em que suas palavras eram o único conforto e segurança disponíveis. Você foi desde muito cedo, mãe e pai para mim.

Agradeço ao meu orientador, Prof. Luís Felipe, pela oportunidade de realizar esta pesquisa, e aos demais integrantes da banca, os Professores Jacques P. Sauvé, Jorge L. S. Leão e Inês de C. Dutra, pela contribuição na avaliação deste trabalho.

Agradeço aos meus professores de graduação Jacques Philippe Sauvé, "Peter Nicolletti" e "Fubica Brasileiro", por terem despertado em mim a curiosidade pelo estudo e trabalho. A contribuição e ensinamento de vocês irão sempre estar presentes na minha caminhada, e compartilho com vocês todos os méritos do meu trabalho.

Agradeço a todos as amizades que construí neste período, em particular: Bruno, Pinaffi, Denilson, Victor, Luciano, Mendes, Vilela, Eduardo, Paulo, Cláudia, Marcos, Diogo, Michelini, Rafael, e todos os outros, que por ventura eu tenha esquecido.

Agradeço também a todos os amigos da velha turma da "Computaria". Vocês sempre me deram força e a prosseguir neste caminho. Amizades verdadeiras.

Ao Conselho Nacional de Pesquisa (CNPq), pelo financiamento da pesquisa e ao Programa de Engenharia de Sistemas e Computação (PESC/COPPE/UFRJ), pelo apoio operacional.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

PROPOSTA DE UM MODELO PARA O GERENCIAMENTO INTEGRADO DE SEGURANÇA EM REDES SEM FIO

Airon Fonteles da Silva

Julho/2006

Orientador: Luís Felipe Magalhães de Moraes

Programa: Engenharia de Sistemas e Computação

A segurança das redes locais sem fio no padrão IEEE 802.11 sempre foi alvo de estudos e críticas. Por muitas vezes o gerenciamento de segurança deste tipo de rede é tratado com os mesmos paradigmas das redes cabeadas convencionais, onde aspectos específicos do ambiente sem fio são simplesmente ignorados. Além disso, existe a lacuna na integração dos mecanismos de segurança que podem levar a um estado de inconsistência na rede. Neste trabalho é proposto um *framework* de gerenciamento de segurança integrado para redes sem fio, onde alterações no estado de determinadas ferramentas modificam automaticamente a configuração das ferramentas correlatas sem a intervenção do administrador.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

PROPOSITION OF A MODEL FOR INTEGRATED SECURITY MANAGEMENT IN WIRELESS NETWORKS

Airon Fonteles da Silva

July/2006

Advisor: Luís Felipe Magalhães de Moraes

Department: Systems Engineering and Computer Science

Security in Wireless Local Area Networks (WLANs) based on the IEEE 802.11 standard was always target of research. For many times security management for this type of networks have being treated with the same paradigms used in conventional wired networks, where specific aspects of wireless environment are simply ignored. Furthermore, there is a gap in the integration of security mechanisms that can lead to a state of network inconsistency. We propose a framework for integrated security management for WLANs, where changes in the state of specific tools leads to automatic changes in correlated tools configuration without system administrator intervention.

Lista de Acrônimos

API	:	*Application Programming Interface*;
CORBA	:	*Common Object Request Broker Architecture*;
DCOM	:	*Distributed Component Object Model*;
DNS	:	*Domain Name Service*;
DPD	:	*Dead Peer Detection*;
HTTP	:	*HyperText Transfer Protocol*;
IDL	:	*Interface Definition Language*;
IDS	:	*Intrusion Detection System*;
IEEE	:	*Institute of Electrical and Electronic Engineers*;
IIOP	:	*Internet Inter Orb Protocol*;
IP	:	*Internet Protocol*;
ISO	:	*International Standards Organization*;
JDBC	:	*Java Database Connectivity*;
JRMP	:	*Java Remote Method Protocol*;
JSP	:	*Java Server Pages*;
LAN	:	*Local Area Network*;
MAC	:	*Media Access Control*;
MIB	:	*Management Information Base*;
OMG	:	*Object Management Group*;
PDA	:	*Personal Digital Assistant*;
PF	:	*Packet Filter*;
RAP	:	*Rogue Access Point*;
RF	:	*Radiofrequência*;
RMI	:	*Remote Method Invocation*;

SNMP : *Simple Network Management Protocol*;

SSH : *Secure Shell*;

UML : *Unified Modeling Language*;

VPN : *Virtual Private Network*;

WDS : *Wireless Distribution System*;

WEP : *Wired Equivalent Privacy*;

WIP : *Wireless Intrusion Protection*;

WLAN : *Wireless Local Area Network*;

WPA : *Wi-Fi Protected Access*;

XML : *Extensible Markup Language*;

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

ESTE capítulo apresenta os conceitos básicos dos problemas de segurança envolvidos nas comunicações sem fio. Um breve histórico da evolução dos mecanismos de segurança propostos pelos padrões que regem este tipo de comunicação bem como as diversas falhas que já foram reportadas e corrigidas também são apresentadas.

Em decorrência destas falhas, serão apresentadas também algumas características de ambientes de acesso sem fio que acabam por requerer ferramentas de segurança adicionais além das propostas pelos padrões de segurança.

Além disso, também são discutidos alguns aspectos fundamentais sobre a necessidade do gerenciamento integrado. Posteriormente são apresentados os objetivos e contribuições do trabalho, bem como a organização do texto da tese.

1.1 Segurança em Redes sem Fio

Redes de computadores são atualmente elementos indispensáveis nas empresas por proverem aumento de comunicação entre funcionários, clientes e fornecedores e conseqüentemente, aumentando também o acesso à informação. Nos últimos anos, com o surgimento de novas tecnologias, as redes locais sem fio (WLANs - *Wireless Local Area Networks*) surgiram como nova proposta para superar limites de alcance e mobilidade. Esta nova modalidade de rede gerou vários desafios e, claro, ampliou os horizontes nas comunicações.

O padrão do IEEE (*Institute of Electrical and Electronics Engineers*) utilizado para este tipo de rede é principalmente o da classe 802.11 junto com suas variações (802.11a/b/g)[1]. Este tipo de rede foi adotado com uma velocidade consideravelmente alta. A cada dia mais usuários domésticos e empresas dos mais variados portes as utilizam para as mais diversas atividades.

No decorrer dos últimos anos, várias falhas de segurança foram identificadas nos padrões propostos. Estes problemas demonstram a fragilidade que envolve a questão da segurança deste tipo de rede. Estas fragilidades estão ligadas ao fato da ausência de limites físicos dos sinais transmitidos pelos equipamentos possibilitar a aquisição da informação que trafega entre as estações comunicantes mesmo a uma distância considerável. Com a utilização de equipamento adequado é possível ter acesso aos dados que trafegam em uma rede sem fio mesmo estando distante dela alguns quilômetros [2].

Durante a especificação dos padrões de segurança a serem utilizados nas redes 802.11 não houve o comedimento necessário para que fossem realizadas análises mais profundas acerca dos algoritmos que seriam empregados. No afinco de colocar disponíveis no mercado produtos que utilizassem estas tecnologias a discussão sobre a qualidade real dos protocolos de segurança foi colocada de lado. O resultado desta precipitação foram as falhas que foram identificadas a partir de então. Inicialmente a segurança deste tipo de rede era baseada na utilização do WEP (*Wired Equivalent Privacy*). O protocolo tinha como intuito garantir o mesmo nível de

confidencialidade de uma rede cabeada convencional. No entanto, segundo estudos publicados na literatura, há problemas em sua especificação que o tornam suscetíveis a ataques. Dentre os principais problemas podem ser citados a reutilização do vetor de inicialização que permite a quebra da chave, o uso do CRC32 como algoritmo de checagem, permitindo ataques de modificação controlada dos pacotes sem a identificação deste tipo de ocorrência pelas partes comunicantes, dentre outros. Mais informações acerca das falhas do WEP podem ser encontradas em [3] e [4].

Com a identificação de falhas no WEP logo surgiram diversas ferramentas capazes de quebrar as chaves utilizadas neste tipo de rede. Neste meio tempo, como forma de prover um maior nível de segurança, mesmo que como solução temporária, surgiu o WPA (*Wi-Fi Protected Acess*). Este sucessor surgiu como objetivo declarado de ser uma solução temporária enquanto a uma melhor descrição métodos e algoritmos de segurança a serem utilizados neste tipo de rede não fosse tornado disponível. Entretanto, logo após sua divulgação, novos estudos mostraram a fragilidade desta solução, sendo como exemplos, ataques do tipo dicionário e de homem no meio. O primeiro aplica-se ao WPA quando habilitado o método de autenticação baseado em PSK (*Pre-Shared Key*). Nele, os usuários da rede compartilham uma senha comum para autenticação. O problema surge quando senhas de tamanha inferior a vinte caracteres são usadas (o que costuma ser fato bastante comum).

O método de autenticação baseado no 802.1X merece atenção especial. Ele pode ser utilizado tanto no WPA como no WPA2. Estudos mostraram que alguns dos protocolos de segurança que podem ser utilizados no 802.1X podem sofrer ataques do tipo homem-no-meio e roubo de sessão. O primeiro consiste na interceptação de uma mensagem, onde o atacante pode ler e possivelmente modificar esta informação e passá-la adiante, quando o último trata de o atacante conseguir roubar uma sessão de um usuário válido que já fez sua autenticação se fazendo passar pelo mesmo. Estes problemas podem ser considerados sérios pois este método de autenticação pode ser usado tanto no WPA como no WPA2. Mais detalhes sobre estes problemas podem ser encontrados em [5], [6] e [7].

A tão esperada solução definitiva de segurança para redes 802.11 foi a divulgação

da versão final do grupo de trabalho do IEEE voltado para este foco, o *802.11i*. Embora várias melhorias e restrições tenham sido colocadas pelo novo padrão, este ainda se mostrou falho e suscetível a diversos tipos de ataques. Um dos pontos fracos da solução é o já discutido mecanismo de autenticação previsto, baseado no padrão 802.1X. Outras vulnerabilidades também foram reportadas conforme pode ser visto em [7] e [8].

Resumidamente temos então:

1. WEP - Reutilização do Vetor de Inicialização; Uso do CRC32;
2. WPA - Ataques do dicionário no WPA-PSK; Ataques do Homem-no-meio quando utilizado o 802.1X;
3. WPA2 - Ataques do Homem-no-meio quando utilizado o 802.1X;

O efeito destes diversos problemas de segurança nos padrões de segurança propostos pelo IEEE é a constante utilização de ferramentas de segurança adicionais para prover segurança ao ambiente sem fio. Esta afirmação pode ser constatada nos trabalhos publicados em [9], [10], [11] e [12], dentre outros. Estes trabalhos indicam a necessidade de se agregar a utilização destas ferramentas auxiliares ao ambiente. Logo, a situação *de facto* é que os ambientes de acesso sem fio contam, na maioria das vezes, com o uso destas diversas ferramentas de segurança alternativas visto que os métodos tradicionais previstos no padrão não são satisfatórios em seu propósito.

Dentre as ferramentas que podem ser utilizadas para prover este aumento no nível de segurança podem ser citados como exemplos mais comumente utilizados *Firewalls* e VPNs (*Virtual Private Networks*). O uso destas ou de outras ferramentas depende muito do tipo de ambiente e recurso a ser utilizado pelos usuários da rede. Torna-se inviável exigir que todos os ambientes de acesso sem fio possuam os mesmos requisitos de segurança pois as necessidades específicas que cercam os usuários destes ambientes bem como dos detentores da infra-estrutura geralmente divergem de maneira . Assim sendo, podem ser encontrar por exemplo situações onde os usuários requerem a utilização de VPN e provedores de serviço que sempre farão uso de Firewalls para proteger e limitar o acesso dos usuários.

Outro aspecto interessante no gerenciamento de segurança para WLANs é o fato de existirem aspectos específicos que devem ser tratados devido à natureza deste tipo de rede. Devido ao meio de transmissão e suas características particulares, surgem novos desafios e questões de segurança que muitas vezes são ignoradas pelas soluções e propostas disponíveis atualmente. Como exemplos destes aspectos específicos que não são levados em consideração no gerenciamento deste tipo de rede podem ser citados como exemplos:

- Handoff - permissão ou não de um dispositivo mudar de ponto de acesso;
- Dead Peer Detector - ferramenta de segurança que visa impedir ataques do tipo roubo de sessão;
- Localização - a localização de usuários é fonte útil de informação a respeito de pontos de acesso não autorizados, por exemplo;
- Wireless Distribution System - ferramenta que permite a ampliação da área de cobertura dos pontos de aceso, que pode ter implicações em segurança.

Estas questões específicas merecem tanta atenção como a utilização das ferramentas tradicionais de segurança (autenticação e autorização, por exemplo). É notório que tanto os aspectos específicos que cercam o ambiente sem fio como estas ferramentas tradicionais de segurança podem ser configurados e geridos individualmente. Porém, atinge-se um resultado mais interessante se todos estes fatores e ferramentas forem considerados como colaborativos. Desta forma, a alteração no estado e/ou configuração de determinado parâmetro pode influir na configuração das demais entidades presentes no ambiente. Assim, preferencialmente o desejável é que ambos possam ser tratados de maneira conjunta e colaborativa para obtenção de um ambiente de rede mais seguro.

1.2 A Questão do Gerenciamento de Segurança

Devido ao importante papel que as redes de computadores desempenham nos dias atuais, tornando-se muitas vezes recurso de missão crítica em vários ambientes, torna-se importante gerir tal recurso. Como poderá ser visto posteriormente na Seção 2.1, o gerenciamento de redes divide-se em áreas distintas. Uma destas áreas é o gerenciamento de segurança. Temos ainda suas grandes dimensões, heterogeneidade e complexidade como fatores que reforçam a necessidade do gerenciamento.

Como visto na seção anterior, existe a possibilidade de haver um grande número de dispositivos de segurança que podem ser acrescidos a um ambiente de rede sem fio com o intuito de torná-lo mais seguro. O processo de instalação e configuração destes dispositivos é denominado gerenciamento de configuração. É importante aqui ressaltar que, embora primordiais, a simples configuração adequada dos dispositivos a serem utilizados na rede sem fio não devem encerrar as atividades que cercam este ambiente.

A abordagem que por muitas vezes é utilizada é a simples configuração dos parâmetros e mecanismos de segurança do ambiente de rede sem posterior acompanhamento do seu estado. Este aspecto abre possibilidade para possíveis brechas na segurança do ambiente que se imaginava livre de perigos devido a uma configuração inicial realizada de maneira criteriosa.

O procedimento mais indicado seria como passo posterior à configuração a sua manutenção (ou monitoração). É nesse ponto que o fator humano tem papel muito importante. Sujeito a falhas que é, o indivíduo responsável por manter a rede tem pela frente um grande número de configurações a realizar. Caso haja alteração na configuração de determinada ferramenta o administrador tem que ter o discernimento de identificar quais ferramentas correlatas devem ter também suas configurações alteradas a fim de manter o estado de consistência da rede, onde se entende por correlação, o fato de haver duas ou mais ferramentas que possuem a característica de uma alteração no estado ou configuração em uma delas implicar em uma ação nas demais. Já a inconsistência ocorre quando estas dependências de

comportamento não são satisfeitas. Isto é importante devido ao fato de que sua ausência leva a uma falsa sensação de segurança ou até mesmo um funcionamento indevido da rede. É nesse ponto que um processo que automaticamente realizasse estas alterações seria extremamente útil e desejável por diminuir consideravelmente o risco de erros que o administrador estaria sujeito.

Com o que foi apresentado até é possível observar que a questão do gerenciamento é altamente relevante devido à complexidade inerente ao cenário desenhado. Além das questões até agora levantadas existe ainda outros complicadores presentes no ambiente. Como exemplos podem ser citados a existência de múltiplos pontos de acesso de fabricantes diversos e as várias versões diferentes de softwares ligados à segurança. Estas questões são complicadoras devido ao fato da necessidade de haver um amplo conhecimento acerca dos dispositivos e ferramentas presentes no ambiente para que seu gerenciamento seja possível, o que torna este processo bem mais complexo.

Diversas empresas propõem soluções ditas aptas a realizar a gerência de segurança das redes sem fio. Mas como poderá ser visto posteriormente, muitas das soluções disponíveis baseiam-se em paradigmas de gerenciamento das redes cabeadas que não são completamente adaptáveis aos aspectos de segurança das redes sem fio. Estes paradigmas são constituídos basicamente da utilização do protocolo de gerenciamento e monitoramento de redes SNMP (*Simple Network Management Protocol*) [13]. Basicamente dados referentes à utilização de canal e taxa de erro, dentre outros, são coletados e suas estatísticas apresentadas como o gerenciamento da rede sem fio. Nos melhores casos, quando as ferramentas abordam aspectos específicos das WLANs, existe o aspecto da falta de integração entre os mecanismos de segurança que já foi mencionada.

1.3 Objetivos e Contribuições do Trabalho

Como visto na seção anterior, várias limitações existem atualmente no gerenciamento de segurança de redes sem fio. Além da possibilidade de aplicação de

diversos mecanismos de segurança no ambiente, situação esta que é bastante usual, problemas específicos encontrados no ambiente sem fio não são abordados.

Com base nestes pontos apresentados o objetivo deste trabalho é apresentar um *framework* para o gerenciamento integrado e distribuído dos mecanismos de segurança que podem estar presentes em uma rede sem fio. Neste trabalho, um *framework* é definido como um software onde são acoplados componentes responsáveis pelo gerenciamento de cada aspecto de segurança identificado. O gerenciamento é dito integrado pois alterações que por ventura ocorram em determinada ferramenta de segurança devem automaticamente ter suas implicações nas ferramentas correlatas.

O que se busca é definir uma padronização nas interfaces de comunicação entre os diversos sistemas de segurança que possam eventualmente ser utilizados. Desta forma a interoperabilidade entre as mais diversas ferramentas é mantida de forma automática, sempre levando em conta aspectos específicos de segurança em WLANs.

Esta interoperabilidade entre os sistemas de segurança decorre do fato de que num ambiente real os diversos sistemas são colaborativos entre si. Relacionamentos entre os sistemas de segurança podem ser definidos quando existe algum aspecto de segurança que pode alterar o estado ou configuração de outros sistemas de segurança. Assim, cada ação do gerente do sistema em determinada ferramenta de segurança terá suas respectivas implicações nas outras ferramentas correlatas de maneira automática, de forma a manter íntegro o estado do sistema. As associações entre os mecanismos de segurança não são, de qualquer maneira, impostas ou limitadas. Desta forma é possível fazer com que ferramentas usadas para prover segurança se comuniquem com outras ferramentas em qualquer lugar da rede, desde que o administrador identifique uma correlação entre seus comportamentos.

Desta forma, a grande contribuição do presente trabalho é apresentar um novo framework de gerenciamento integrado das ferramentas de segurança para redes sem fio no padrão 802.11. De uma maneira como não foi abordada antes, os aspectos específicos de redes sem fio são levados em consideração e as questões referentes ao relacionamento entre as ferramentas são mantidas, permitindo que o administrador da rede possa ter controle sobre a rede de maneira a estar menos sujeito a falhas.

Além disso, o desenvolvimento de soluções personalizadas para gerenciamento de redes sem fio fica simplificado uma vez que os componentes já desenvolvidos podem ser reutilizados de maneira simples restando apenas a customização dos relacionamentos para alcançar este fim. Os detalhes e requisitos da solução proposta serão vistos em mais profundidade no Capítulo 3.

1.4 Organização do Texto

O texto deste trabalho está organizado da seguinte maneira. O estado da arte, representado pelas soluções acadêmicas, e uma breve descrição das soluções comerciais disponíveis no mercado são apresentados no Capítulo 2. O Capítulo 3 aborda os diferenciais da proposta aqui apresentada em relação às soluções já existentes no que diz respeito ao gerenciamento de segurança em redes sem fio. No Capítulo 4 são apresentados os detalhes da arquitetura proposta para o *framework* com os respectivos protocolos utilizados e ferramentas de segurança disponíveis. Alguns aspectos da implementação que foi feita para validação são mostrados no Capítulo 5. Por fim, as conclusões e trabalhos futuros estão presentes no Capítulo 6.

Capítulo 2

Estado da Arte e Ferramentas Atuais

NESTA seção serão apresentados os principais estudos disponíveis na área de gerenciamento de redes sem fio, bem como algumas soluções comerciais disponíveis no mercado para o mesmo fim.

Serão abordados aspectos fundamentais acerca das soluções disponíveis, seus pontos favoráveis e também os pontos que depõem contra elas. Será visto que a maioria dos estudos acadêmicos disponíveis atualmente se concentra na área da monitoração deste tipo de rede, muitas vezes simplesmente utilizando os mesmos paradigmas amplamente utilizados em redes cabeadas convencionais.

Pelo lado das soluções comerciais, a diversidade de soluções disponíveis, bem como as metodologias utilizadas definem um universo que dificulta a generalização das ferramentas, onde cada uma se caracteriza por particularidades e paradigmas associados. Como será visto no decorrer desta Seção, existem soluções mais complexas que contemplam um grande número de ferramentas de segurança para um ambiente sem fio, mas mesmo nestes casos as soluções apresentadas pecam pela falta de integração.

2.1 Estado da Arte

De acordo com o padrão ISO (*International Standards Organization*)[14], um sistema completo de gerência de redes deve ter cinco funções específicas. A seguir uma breve descrição acerca das características de cada uma:

- Gerência de falhas - Responsável pela detecção, isolamento e recuperação de falhas na rede.
- Gerência de desempenho - Responsável pela monitoração de desempenho da rede atrelada a certos indicadores, tais como atraso, vazão, disponibilidade, utilização, taxa de erros, etc. ;
- Gerência de contabilidade - Estabelecimento e aplicação de cotas de utilização e escalas de tarifação;
- Gerência de configuração - Responsável pelo descobrimento, manutenção, monitoração das mudanças à estrutura física e lógica da rede;
- Gerência de segurança - Provê mecanismos para criar, remover e controlar os serviços de segurança de rede;

De acordo com a classificação vista acima, alguns estudos vêm sendo feitos na parte de gerência de falhas, configuração e desempenho (também chamada de monitoração) para redes sem fio. Nos parágrafos a seguir, serão abordados alguns trabalhos acadêmicos apresentados nos últimos anos em conferências internacionais que indicam o que vem sendo feito nas respectivas áreas.

Um sistema de gerenciamento de segurança baseado em agentes móveis é proposto em [15]. Nele são descritos vários tipos de agentes que tem dentre suas principais características buscarem informações acerca das configurações de segurança, verificar se os dados coletados representam falhas e instruir o administrador com sugestões de ações para mitigar possíveis problemas. A solução em questão trata dos aspectos de segurança divididos em "camadas". Para atingir o objetivo final de informar ao administrador que ações devem ser tomadas para tornar o ambiente sem

fio mais seguro, agentes especializados realizam ataques simulados a estas camadas específicas em busca de possíveis falhas de segurança. Especificamente, o propósito de cada camada é assim descrito:

- Camada um - Assegurar que usuários não autorizados não acessem a WLAN;
- Camada dois - Prevenir a captura de tráfego;
- Camada três - Assegurar que dispositivos não autorizados acesse a WLAN.

De um modo geral a solução apresentada possui algumas características interessantes como, por exemplo, instruir o responsável pela rede a adotar soluções de VPN e Firewall para melhor segurança da rede. De resto, realiza testes para verificar a adoção de WEP/WPA na rede, dentre outras atividades. Como pontos fragilidades desta solução podem ser citados os seguintes aspectos:

- Ferramenta apenas identifica possíveis fragilidades;
- Em nenhum momento ela trata da integração das ferramentas de segurança que podem estar presentes na rede;
- Não considerar aspectos específicos de segurança em redes sem fio.

Em [16] é apresentado um sistema de auditoria de políticas de segurança de pontos de acesso. Com o auxílio do que o autor chama de "dispositivos confiáveis" a rede é monitorada em busca de pontos de acesso não autorizados ou com configuração inadequada. Para tal, softwares devem ser instalados nesses clientes confiáveis para que eles façam às vezes de *sniffers* do ambiente coletando informações. Uma vez coletadas, estas informações são enviadas por meio de uma conexão segura para o servidor da aplicação. Abaixo, seguem as atribuições de clientes e servidor, respectivamente:

Clientes:

- Coletar informações relacionadas a segurança dos pontos de acesso que estão em seu raio de alcance;

- Obter sua própria localização via nível de sinal recebido ou GPS;
- Periodicamente enviar ao servidor o resumo destas informações coletadas.

Servidor:

- Autenticar o cliente;
- Comparar os dados enviados pelos clientes com a lista de pontos de acesso autorizados e a política de segurança da organização;
- Determinar pontos de acesso não autorizados ou mal configurados;
- Ilustrar a localização física de tais dispositivos utilizando técnicas de triangulação e dados de localização dos dispositivos clientes.

Embora seja economicamente interessante o uso dos próprios dispositivos clientes na tarefa de monitoração do ambiente, o autor assume, dependendo das circunstâncias, a improdutividade ou mesmo inviabilidade dos clientes desempenharem tais funções. Outro importante ponto de discussão é o foco exclusivo na identificação de pontos de acesso não autorizados e/ou mal configurados. Notavelmente este é um ponto importante na segurança de redes sem fio, mas não deve ser o único. No trabalho, os autores simplesmente não abordam nenhum outro aspecto de segurança neste tipo de ambiente.

Uma outra ferramenta pode ser vista em [17]. Os autores apresentam um sistema distribuído para analisar a segurança e detectar possíveis vulnerabilidades na rede sem fio. Com uma solução dependente da distribuição Linux Debian, os autores realizam testes de segurança na rede sem fio automatizando tarefas baseados em uma metodologia já existente. Uma vez realizados estes testes, relatórios são colocados à disposição do administrador para que ele possa tomar as atitudes necessárias para deixar o ambiente mais seguro.

Como pode ser visto, esta solução obtém dados específicos de segurança da rede sem fio. No entanto, como em outros estudos debatidos até aqui, existem uma série de limitações e questões de segurança que não são abordados. O foco principal de

atuação da ferramenta proposta é a análise das camadas física e de enlace de acordo com o padrão OSI. Desta forma, questões relacionadas as camadas superiores não são considerados. Este fator leva à falha comumente encontrada até aqui: demais ferramentas de segurança que são muito comuns neste tipo de rede não são levadas em consideração. Além disso, novamente o administrador, uma vez de posse dos relatórios provenientes da utilização da ferramenta, tem que manualmente alterar as configurações de segurança que julgar pertinente.

Como pode ser visto até aqui, o número de trabalhos que tem foco específico na segurança das redes sem fio é limitado. Além disso, os trabalhos apresentados possuem uma série de limitações que podem assim serem sumarizadas:

1. Ausência de ferramentas tradicionais de segurança;
2. Ausência de aspectos específicos em redes sem fio;
3. Grande foco na detecção de pontos de acesso não autorizados em detrimento de outros aspectos de segurança;
4. Ausência de integração entre as ferramentas na rede.

2.2 Ferramentas Comerciais

Hoje é possível encontrar diversas soluções comerciais para a gerência de redes sem fio, cada uma com características, qualidades e deficiências próprias. A seguir, são apresentadas algumas destas soluções que já estão disponíveis no mercado juntamente com alguns breves comentários acerca de suas principais características.

2.2.1 Cisco - Cisco Wireless Control System

A Cisco, uma das maiores e mais renomadas empresas que oferecem soluções para redes de computadores, desenvolveu sua própria solução de redes sem-fio como também sua própria solução de gerenciamento. Esta solução foi batizada de *Cisco*

Wireless Control System, que atualmente, na sua versão 1.0, vem com as seguintes características no que diz respeito à gerência de segurança:

1. Sistema de localização de dispositivos;
2. Monitoração do espectro de freqüência, detecção de pontos de acesso não autorizados, configuração dos mecanismos de segurança do padrão;
3. Monitoramento das políticas de segurança em utilização nos pontos de acesso. Alertas são gerados e enviados aos responsáveis quando ocorre violação nessas políticas.
4. Acesso via interface WEB segura. Além dessa interface, é possível utilizar interface via linha de comando com acesso a partir de uma conexão *SSH (Secure Shell)* ou *telnet*.

Nos pontos de acesso desenvolvidos pela CISCO, existe um dispositivo que monitora os espectros de freqüência das redes IEEE 802.11 à procura de possíveis tentativas de invasão. É um aspecto interessante da solução da CISCO, pois IDS (*Intrusion Detection System)* eficientes para redes sem fio tem sido alvos de muitos estudos na comunidade acadêmica. Além disso, é possível potencializar o mecanismo acima além de capacitar a detecção de pontos de acessos não autorizados (os chamados *Rogue Access Points* - RAP).

A solução da empresa constitui-se de soluções e abordagens encontradas em praticamente todas as soluções que serão apresentadas. Existe o aspecto de configuração e monitoração de aspectos de segurança, radiofreqüência, autenticação, criptografia, dentre outros. Quando ocorre alguma alteração na política de segurança alarmes são gerados e os administradores notificados.Definitivamente, o ponto apresentado no item um seria de grande utilidade em uma solução de gerência. Agora é importante notar, que a solução apresentada pela CISCO é baseada na utilização de um ponto de acesso desenvolvido por eles. Isto limita bastante sua utilização quando ocorre da utilização de uma solução não proprietária ou não completamente homogênea, o

que geralmente é a situação mais comum, devido relativamente aos elevados custos associados em se adquirir uma solução deste tipo.

Outro ponto que merece bastante atenção é a notória grande preocupação identificada nas soluções existentes acerca da detecção de pontos de acesso não autorizados. Com a grande produção e conseqüente barateamento desta tecnologia que vem acontecendo gradativamente ano após ano, os empregados de uma empresa podem se sentir tentados a instalar seus próprios pontos de acesso para ampliar o acesso à rede corporativa. O grande problema desta abordagem é que na maioria das situações os critérios ou políticas de segurança da empresa são deixados de lado, fazendo com que o ponto de acesso recém instalado seja o elo fraco da cadeia que pode levar ao comprometimento de toda a segurança da rede. Isto acontece pois uma vez conseguindo acesso ao RAP que foi configurado de maneira incorreta, o usuário não autorizado ganha acesso a toda rede corporativa como se estivesse nas próprias instalações da empresa. A partir daí ele pode realizar um grande número de atividades não autorizadas na rede comprometendo severamente sua segurança.

Embora este seja visivelmente um problema grave que demanda um grande esforço no sentido de encontrar uma solução eficaz e eficiente, não deve receber todos os esforços de segurança disponíveis. Isto porque se trata de apenas mais um dos diversos problemas de segurança que atingem este tipo de rede.

2.2.2 Aruba OS

Esta solução de gerência é baseada na utilização de hardware e software proprietários. Os principais componentes da solução são os denominados *Aruba OS*, atualmente na versão 2.5, que é o sistema operacional executado pelos *Mobility Controllers*, equipamentos de rede onde os pontos de acesso devem ser conectados. Funcionalidades podem ser adicionadas acrescentando módulos de software no sistema operacional citado anteriormente.

A seguir são sumarizadas as características principais desta solução:

- Módulo *WIP (Wireless Intrusion Protection)* - Com a instalação deste módulo no software de gerência, são adicionadas as funcionalidades de detecção de intrusão, detecção de falsos pontos de acesso, identificação de tentativas de ataques de negação de serviço, dentre outros;

- Módulo *Firewall/VPN (Virtual Private Networks)* - Adiciona ao sistema de gerenciamento estas duas ferramentas de segurança que são de extrema importância em redes sem fio. Várias implementações de VPN são passíveis de serem utilizadas maximizando o tipo dos dispositivos sem fio que podem ser utilizados;

- Módulo RF Management/WLAN Switching - Adiciona ao sistema de gerência as seguintes funcionalidades: detecção de interferência, áreas de cobertura, autenticação no nível de camada física e de enlace (autenticação de endereços MAC, WEP, WPA);

- Módulo Secure Voice - Provê vários mecanismos para a utilização de voz sobre IP de maneira segura, incluindo um mecanismo de *handoff* eficiente para redução do tempo deste procedimento quando um usuário muda de um ponto de acesso para outro.

Como se pode observar pelas características acima descritas, a solução apresenta alguns pontos positivos como a possibilidade de adicionar ferramentas de segurança citadas na primeira característica colocada acima. Além de ser uma solução baseada em recursos proprietários, ela sofre com os mesmos problemas das demais soluções, não apresentando possibilidade de integração entre estas ferramentas. Mais informações acerca desta solução podem ser obtidas em [18].Como podemos observar pelas características descritas, o que se tem é uma solução que apresenta algumas limitações, principalmente no que diz respeito à obrigatoriedade da existência de uma infra-estrutura proprietária da empresa.

Um ponto positivo a ser ressaltado nesta solução, é o mecanismo de *handoff* rápido, minimizando os possíveis efeitos prejudiciais em aplicações multimídia, por

exemplo. Para chegar aos baixos tempos de *handoff* apresentados, a solução encontrada é manter o estado dos usuários em todos os pontos de acesso conectados.

2.2.3 AirWave - AirWave Management Plataform

A aplicação encontra-se na versão 4.0 e pode ser considerada uma boa solução presente no mercado, tendo a seu favor vários pontos que serão destacados a seguir:

- É uma solução que independe de hardware proprietário e tem compatibilidade com diversos fabricantes de hardware;
- Provê a monitoração de diversos mecanismos de segurança tais como *VPNs*, protocolos de autenticação utilizados, protocolos de criptografia ativos, etc;
- Utilização de uma interface WEB;
- Detecção de pontos de acesso não autorizados via *escaneamento* de radiofreqüência e ethernet.

O ponto forte dessa solução é que ela não é dependente de hardware proprietário, flexibilizando bastante sua utilização. Porém os problemas são também notórios. O foco do gerenciamento desta ferramenta é de configuração e monitoração. Assim sendo, o aspecto de integração proposto neste trabalho também não está coberto por esta solução, pois ela limita-se a prover a monitoração dos mecanismos de segurança provendo alarmes e notificações. Mais detalhes sobre ela podem ser obtidos em [19].

Como na maioria das soluções existentes, esta também se limita a prover a monitoração dos mecanismos de segurança provendo alarmes e notificações.

2.2.4 AirDefense Enterprise

Esta é mais uma solução proprietária que conta com a monitoração de alguns mecanismos de segurança. De fato, a solução consiste em um hardware propri-

etário com todas as funcionalidades de software incluídas e que tem como principais características na atual versão, 7.0:

- Utilização de sensores distribuídos no ambiente como suporte para a ferramenta de segurança;
- Detecção de intrusão e de falsos pontos de acesso;
- Definição de políticas de segurança e monitoração de desvios nessas políticas;
- Correlação de dados adquiridos através dos sensores;
- Uma biblioteca com cerca de duzentos eventos relacionados à segurança e desempenho, utilizadas junto à técnicas de correlação de eventos para inferir possíveis problemas.

Novamente temos a falta de integração entre os diversos mecanismos apresentados e a ausência de outras ferramentas de segurança importantes. Outro ponto negativo nesta solução é a utilização de hardware proprietário. O que se adquire é um hardware específico que faz às vezes de estação de gerenciamento e diversos sensores para serem dispostos no ambiente. Mais informações podem ser obtidas em [20].

2.2.5 Resumo

Como pode ser visto na Tabela 2.1 as soluções adotadas comercialmente podem ser consideradas mais completas dos que os estudos acadêmicos apresentados. É possível dizer isto pois estas ferramentas contemplam um número significante de características a mais para o gerenciamento de redes sem fio. Como exemplo, pode ser citada a presença de aspectos como Localização, IDS e uso de outras ferramentas.

Embora possuam características essenciais para o gerenciamento deste tipo de rede, elas possuem as mesmas deficiências encontradas anteriormente nos trabalhos acadêmicos:

	Localização	RF	IDS	Independência de Hardware Proprietário	Outras Ferramentas de Segurança	Integração
Cisco	OK	OK	OK	X	OK	X
Aruba	OK	OK	OK	X	OK	X
AirWave	OK	OK	OK	OK	OK	X
AirDefense	OK	OK	OK	X	OK	X

Tabela 2.1: Resumo das características das ferramentas comerciais disponíveis para redes sem fio

- Não lidam com alguns aspectos específicos deste tipo de rede;
- Não tratam do aspecto de integração entre estas ferramentas.

Capítulo 3

Contribuições da Proposta

NESTE capítulo serão apresentadas as principais contribuições da solução proposta em relação aos trabalhos e ferramentas previamente discutidas. Os pontos fracos das demais soluções são atacados e pontos que são ignorados nas demais ferramentas são aqui devidamente tratados.

Além disso, será discutido o principal ponto abordado nesta proposta: a integração das possíveis ferramentas de segurança presentes em um ambiente para acesso sem fio, característica que está ausente nas demais soluções.

Como se pode observar, as pesquisas acadêmicas e as tecnologias utilizadas na indústria não contemplam a parte de gerência integrada das soluções de segurança, segurança esta, descrita por todos eles como sendo de fundamental importância em uma área de características tão peculiares devido a sua natureza.

Muitas soluções estão disponíveis além das já citadas anteriormente. Seria praticamente impossível discorrer sobre cada uma delas. Entretanto, os pontos cruciais podem ser debatidos aqui. Estas soluções apresentadas tentam se apresentar como soluções para a gerência de redes sem fio. Através de uma análise mais detalhada, é possível verificar que a realidade não é exatamente essa. Muitas das soluções já propostas lidam com a gerência da rede sem fio como se fosse uma rede cabeada tradicional, usando muitas vezes os mesmos paradigmas. Algumas soluções encontradas chegam ao limite de apresentar gráficos de utilização do canal e outras estatísticas tão comuns em redes cabeadas e como sendo parte da gerência da rede sem fio.

Sabe-se que estas informações fazem parte e são muito importantes no gerenciamento de qualquer tipo rede. No entanto, redes sem fio possuem características que não estão presentes nas redes cabeadas convencionais. Neste caso, o principal problema é a limitação que existe ao utilizar-se somente o protocolo SNMP para realizar algumas medições, calcular e apresentar estatísticas de utilização do canal. Isso deixa de lado aspectos de segurança imprescindíveis que devem ser tratados.

Outras soluções já abordam itens e problemas específicos que uma rede sem fio pode apresentar. Nota-se, por exemplo, uma preocupação com a detecção de falsos pontos de acesso. Não que este não seja um aspecto de segurança de fundamental importância a ser gerido. Contudo não é o único. Aspectos específicos de rede sem fio tais como Handoff, DPD e WDS, dentre outros, bem como a integração destes mecanismos merecem tanta atenção como a identificação de pontos de acesso não autorizados. Este aspecto é o que leva a maior parte do foco atualmente, chegando ao ponto de algumas soluções contarem com dispositivos físicos específicos para a busca por falsos pontos de acesso.

Nas soluções mais completas, podem ser encontrados diversos mecanismos de segurança necessários para utilização em um ambiente sem fio. Nestes casos, é possível

encontrar gerenciamento de *firewalls, VPNs, Handoff*, autenticação e criptografia. Mas mesmo nestes casos a gerência apresentada peca pela falta de integração entre os mecanismos gerenciados. Há o problema da existência de um grande número de ferramentas de segurança que precisam ser verificadas e configuradas individualmente. O que é proposto neste trabalho é realização da gerência destas mesmas ferramentas de maneira integrada, onde o administrador da rede estará menos sujeito a falhas.

Desta maneira, propõe-se obter um framework de gerenciamento distribuído onde as entidades lógicas que monitoram e interagem com cada ferramenta de segurança prevista possam estar dispostos livremente na rede, não havendo necessidade de programas sendo executados de maneira centralizada. Além disso, cada ação do gerente do sistema em determinada ferramenta de segurança terá suas respectivas implicações nas outras ferramentas correlatas de maneira automática, de forma a manter íntegro o estado do sistema. Outra característica extremamente desejável no comportamento deste framework é que seus componentes possam, uma vez detectadas alterações em outros componentes, se adequarem a este evento sem a necessidade de intervenção do administrador, automatizando o processo de atualização de configurações ou estado atual dos sistemas envolvidos. Um outro diferencial importante de ser frisado, é que serão considerados aspectos específicos de redes sem fio que por muitas vezes são simplesmente ignorados pelas soluções disponíveis, tais como *handoff* e *Dead Peer Detection*.

Será especificada uma API para o *framework*. Foi feita a escolha pela especificação de uma API pois ela irá contar com a especificação do comportamento das ferramentas de segurança que em um primeiro momento foram identificadas para fazer parte do modelo. Isto irá propiciar que futuras implementações sejam "acopláveis" ao software desenvolvido, mesmo que estas implementações sejam desenvolvidas por terceiros em uma outra linguagem de programação. Como poderá ser visto posteriormente, a API poderá ser utilizadas tanto por aplicações clientes, como pelos próprios módulos do sistema para troca de mensagens e informações.

A integração entre as diversas ferramentas de segurança que possam existir no ambiente sem fio poderão ser definidas à medida que sejam identificados relaciona-

mentos entre as mesmas. Isto é extremamente importante pois o mecanismo de integração não prevê de forma alguma relacionamentos ou comportamentos pré-existentes entre as ferramentas de segurança. Uma vez identificado um destes relacionamentos, bastará um desenvolvedor implementar o comportamento e ações desejados quando da ocorrência de determinada evento nas ferramentas correlatas.

Como foi visto, as soluções atuais não são consideradas ideais pelos problemas identificados. Além disso, há também o aspecto da viabilidade econômica, pois outras tantas soluções são sujeitas à limitações de plataforma e dispositivos para funcionarem adequadamente, o que invariavelmente leva a um aumento no custo agregado ao se implantar uma destas soluções.

Para resumir uma lista de requisitos da solução proposta que irá suprir as deficiências anteriormente identificadas nas demais soluções tem-se:

- A solução deve contar com a utilização de sistemas de segurança que comumente são encontrados nas redes sem fio (Firewalls, VPN, etc);
- Deve contar com a utilização de sistemas ligados a segurança que usualmente exclusivos de ambientes sem fio (Handoff, Localização, etc);
- Possa permitir a integração entre os sistemas de segurança do ambiente;
- Genérica - A especificação das funcionalidades do sistema não devem ser restritas a um subconjunto definido por uma ferramenta específica;
- Escalável - O sistema não deve contar com limitações que impeçam sua adoção em ambientes de larga escala. Assim, deve suportar um grande número de usuários e dispositivos de rede e segurança;
- Flexível - As ações a serem tomadas de acordo com os eventos que ocorram no sistema podem ser alteradas de modo que o funcionamento dos componentes não necessite ser alterado.

Em relação a métricas objetivas de desempenho foi encontrada uma dificuldade considerável: como comparar os resultados obtidos? Como o aspecto da integração

não é levado em consideração em nenhuma das soluções já estudadas, não existe um ponto de partida para a definição destes valores. Neste sentido, uma análise futura pode ser realizada com base no aspecto de quanto tempo levaria para uma pessoa para realizar todas as atividades relacionadas aos sistemas de segurança quando ocorrer algum evento gerador de ações nos outros sistemas de segurança, dado que ela tivesse disponibilidade total para gerenciar o sistema. No Capítulo 5 será mostrado este comportamento com as respectivas comparações.

Capítulo 4

Arquitetura da Solução Proposta

NESTE capítulo serão apresentadas as características da arquitetura escolhida para o *framework* proposto. Como parte da arquitetura proposta, será feita uma breve justificativa sobre as escolhas dos protocolos que foram utilizados na comunicação entre as entidades do *framework*, bem como o paradigma de sistema escolhido.

Além disso, é apresentada uma breve descrição das principais ferramentas de segurança adicionadas ao ambiente, onde algumas delas, não estão presentes nas demais ferramentas apresentadas no Capítulo 2. Para estas ferramentas, são apresentadas as operações identificadas com base em diagramas UML (*Unified Modeling Language*). Também é apresentado o método que propicia a integração entre estes mecanismos.

4.1 Serviços de Segurança Previstos

Nas subseções a seguir, apresenta-se uma breve descrição dos serviços de segurança previstos inicialmente para gerência de segurança de um ambiente sem fio. Como poderá ser visto, o sistema prevê a utilização de diversos serviços de segurança complementares quando instalado um ambiente para acesso sem fio. Aqui são apresentadas as principais entidades identificadas na maioria dos ambientes pesquisados, e foram incluídas também algumas que não estão presentes atualmente nos diversos estudos e soluções comerciais que foram brevemente descritos na Seção 2.

4.1.1 Serviço de Autenticação

O controle de acesso aos recursos da rede sem fio é de extrema importância. Talvez até mais importante do que em uma rede cabeada convencional devido a sua natureza física específica (meio de transmissão não confinado). Sem esse controle de autenticação qualquer dispositivo sem fio pode ter acesso aos recursos como se estivesse localizado fisicamente na rede. Logo, é necessário um servidor de autenticação que possibilite a adição de usuários com as devidas restrições sobre quais pontos de acesso ele tem permissão de utilizar.

Há diversos métodos de autenticação em redes sem fio, dentre os quais podem ser citados:

- autenticação aberta, onde não é necessário informar nenhuma credencial para ter acesso aos recursos do sistema ;
- autenticação usando WEP, onde todos os usuários da rede possuem uma chave pré-compartilhada para autenticação;
- autenticação usando WPA que oferece um nível de segurança mais elevado do que utilizando WEP;
- autenticação usando WPA2, que requer um serviço de autenticação baseado no padrão 802.1X;

- Outros meios proprietários.

Em cada um destes métodos é possível monitorar a autenticação do usuário para que outras entidades presentes no modelo possam ter acesso a essa informação. Se for analisado com cuidado, esta informação pode ser muito relevante desde o mais simples cenário, onde é recomendável reportar quem está utilizando os recursos da rede, e fazer uma contabilidade desta informação, até um cenário mais complexo, onde apenas é permitido o acesso dos usuários após uma rigorosa autenticação e ainda sim, os recursos disponíveis são limitados de alguma maneira.

Além do serviço de autenticação em si, um aspecto importante a ser enquadrado neste item é o que corresponde a gerência de usuários. O ato de adicionar ou remover determinado usuário do ambiente pode acarretar alterações significativas no comportamento de outras entidades do sistema de gerenciamento. Como exemplos, podem ser citados as situações onde determinado usuário possui restrições de acesso em determinados pontos de acesso. Neste caso, é de extrema importância interagir com os dispositivos envolvidos e automaticamente, proibir ou liberar o acesso, conforme especificado no momento da criação do usuário, de maneira automática.

4.1.2 Serviço de *Virtual Private Networks*

Como já visto anteriormente, o nível de segurança provido ao serem aplicados os padrões do IEEE nem sempre estão de acordo com os requisitos de determinadas aplicações ou usuários distintos. Alguns destes requisitos são satisfeitos apenas com a utilização de *VPNs*. Embora haja muitas críticas na utilização desta ferramenta pelo considerável processamento e de maneira geral pelo impacto causado por sua utilização, esta é sem dúvida uma ferramenta importante que periodicamente é utilizada em ambientes sem fio.

Devido a estes fatores foi considerado incluir o gerenciamento de um *Gateway VPN* no ambiente. É indiscutível que quando uma VPN é utilizada adquire-se um maior nível de privacidade na comunicação entre as partes comunicantes independente do meio de transmissão. Através deste módulo deve ser possível alterar as

configurações do *Gateway VPN* presente na rede tais como *passphrase*, *policy*, etc.

4.1.3 Serviço de Localização

No nível de segurança, um sistema de localização é de vital importância no contexto de redes sem fio. Como foi visto nas soluções comerciais disponíveis existe um elevado nível de preocupação com detecção de pontos de acesso não autorizados. De maneira geral, um sistema de localização permite a identificação de qualquer dispositivo não autorizado. De posse desta informação, o administrador pode ir fisicamente ao local provável onde se encontra tal dispositivo e desabilitá-lo. Assim, esta ferramenta é essencial como auxiliar de muitas outras ferramentas na rede. Um sistema de intrusão ou de detecção de falsos dispositivos é, de maneira geral, muito dependente de um sistema de localização.

4.1.4 Serviço de Alarmes

Tão importante quanto as ferramentas de segurança em si são os mecanismos para identificar e reportar alarmes aos responsáveis da rede. Neste aspecto, alarmes vão muito mais do que reportar tentativas de intrusão em uma rede, mas toda a atividade que for contrária às políticas estabelecidas. Neste sentido, alterações indevidas nas configurações dos pontos de acesso, um intruso detectado, ou até mesmo a adição de usuários devem ser reportados de alguma maneira para os responsáveis.

Um ponto interessante a ser mostrado aqui é a diferença entre eventos e alarmes. Eventos são quaisquer atividades que sejam, de alguma maneira perceptíveis pelo sistema de gerenciamento. Isto inclui desde a alteração do endereço IP de um ponto de acesso até um sistema de detecção de intrusão reportando alguma atividade suspeita. Já os alarmes, são os eventos que de alguma maneira podem trazer conseqüências mais graves para a rede como um todo. Existem várias técnicas para geração de alarmes, como por exemplo, a correlação de eventos. Em todo caso, não é mérito deste trabalho enveredar por esta questão.

É trivial notar que todos os eventos que ocorrem nesta arquitetura proposta podem ser facilmente capturados e tratados por um servidor de alarmes específico. Não entrando no mérito da questão deste servidor de alarmes em si, suas ações no caso da ocorrência de determinado alarme podem ir desde informar o responsável pela rede através de um e-mail ou mensagem de texto para o celular, ou em uma postura mais ativa, tentar mitigar o problema previamente encontrado da maneira que for mais adequada.

4.1.5 Serviço Gerenciador de *Handoff*

O sistema gerenciador de *handoff* foi incluído por ser característico de dispositivos sem fio. O processo de *handoff* é uma prática prevista no padrão 802.11, onde uma estação está constantemente verificando quais pontos de acesso ela possui no alcance do seu rádio. Dependendo do seu nível de sinal em determinado momento, existe um algoritmo que compara com dados recebidos de outros pontos de acesso e caso seja viável, a estação faz o *handoff* para um novo ponto de acesso.

Não é considerada aqui a questão do algoritmo de *handoff* em si, nem tão pouco mecanismos para incrementar o desempenho deste processo. Embora estes tópicos já tenham sido alvo de inúmeras pesquisas e artigos publicados, o sistema de gerenciamento de *handoff* está presente no ambiente devido a outros aspectos. O que foi imaginado como ponto de partida foram restrições aplicadas devido a políticas de segurança. Determinada empresa pode ver com bastante interesse a possibilidade de restringir as permissões onde determinados usuários fazem *handoff*. Uma situação que ilustra com bastante precisão este comportamento é a que segue: usuários de departamentos diferentes em uma empresa que apenas podem ter acesso aos recursos quando estiverem no alcance de determinados pontos de acesso. Assim, se este usuário específico começar a se mover com seu dispositivo por outros departamentos não terá permissão de fazer *handoff* para os pontos de acesso em questão.

4.1.6 Serviço de Detecção de Intrusão

O principal tipo de ataque abordado pelas soluções comerciais sem sombra de dúvida é o da identificação de pontos de acesso não autorizados. Mas não é o único. Como foi visto anteriormente as redes sem fio são bastante suscetíveis a diversos tipos de ataques. Embora em um primeiro momento não seja trivial a identificação de alguns deles, um sistema que seja capaz de identificar tentativas de intrusão com algum grau de precisão é instrumento da mais alta importância neste tipo de rede.

Exemplificando uma vez mais, há diversos tipos de ataques que podem ser identificados por um sistema de detecção de intrusão. Tratando mais especificamente, o sistema de localização pode identificar na rede um ponto de acesso não autorizados e dispositivos válidos associados a ele. Desta maneira, é extremamente fácil identificar um ataque do tipo homem-no-meio (*man-in-the-middle*). Aqui, apenas foi exemplificada uma maneira de identificar um dos muitos tipos de ataque em redes sem fio. Mas para a aplicação de gerenciamento em si, o importante é reportar estas tentativas de ataques para que outros módulos possam tomar as providências consideradas cabíveis, seja notificar o administrador ou tentar mitigar o problema através de uma postura mais ativa, conforme o caso. Voltando ao exemplo acima, uma possível providência que poderia ser tomada seria a identificação da porta do switch onde se encontra conectado esse ponto de acesso não autorizado, seguido da sua desativação. Outros exemplos podem ser colocados aqui como sendo de interesse para a aplicação de gerência, a saber: ataques de interferência (*jamming*), e mac forjado (*mac spoofing*), dentre outros.

4.1.7 Serviço de *Firewall*

Mesmo em um sistema onde os usuários tenham se autenticado para ter acesso à rede, é possível que se queira restringir o acesso a determinados recursos. Nestas situações, um serviço de *firewall* é extremamente desejável para controlar o uso dos recursos da maneira que for mais conveniente, de acordo com a política pré-estabelecida. Para isto, deve ser possível poder reconfigurar as regras do *firewall*

Figura 4.14: Interfaces para Listener do AP