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 com Aplicação ao Padrão 802.11 [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 COM APLICAÇÃO AO PADRÃO 802.11

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 WITH APPLICATION ON THE 802.11 STANDARD

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

Resumo **v**

Abstract **vi**

Lista de Acrônimos **vii**

Lista de Figuras **xii**

Lista de Tabelas **xiv**

1 Introdução **1**

1.1 Segurança em Redes sem Fio 2

1.2 A Questão do Gerenciamento de Segurança 6

1.3 Objetivos e Contribuições do Trabalho 7

1.4 Organização do Texto 9

2 Estado da Arte e Ferramentas Atuais **10**

2.1 Estado da Arte 11

2.2 Ferramentas Comerciais 14

2.2.1 Cisco - Cisco Wireless Control System 14

2.2.2 Aruba OS 16

2.2.3 AirWave - AirWave Management Plataform 18

2.2.4 AirDefense Enterprise 18

2.2.5 Resumo 19

3 Contribuições da Proposta **21**

4 Arquitetura da Solução Proposta **26**

4.1 Serviços de Segurança Previstos 27

4.1.1 Serviço de Autenticação 27

4.1.2 Serviço de *Virtual Private Networks* 28

4.1.3 Serviço de Localização 29

4.1.4 Serviço de Alarmes 29

4.1.5 Serviço Gerenciador de *Handoff* 30

4.1.6 Serviço de Detecção de Intrusão 31

4.1.7 Serviço de *Firewall* 31

4.1.8 Serviço de Detecção de Desligamento de Estação 32

4.1.9 Serviço de WDS 32

4.2 Visão Geral do Cluster de Gerenciamento 33

4.3 Detalhamento do cluster de gerenciamento 35

4.4 A API 41

5 Implementação do Framework **54**

5.1 A implementação 55

5.2 Plataforma de Testes 60

5.2.1 AirStrike 60

5.2.2 Utilização de Pontos de Acesso Comerciais 62

5.2.3 Integração entre as Ferramentas 63

5.2.4 Desempenho do Sistema 66

5.2.5 Resultados Obtidos 72

6 Conclusão e trabalhos futuros **75**

6.1 Conclusões 75

6.2 Trabalhos Futuros 77

Bibliografia **79**

Lista de Figuras

4.1 Arquitetura Proposta - Visão geral do cluster de gerenciamento . . . 34

4.2 Arquitetura Proposta - Detalhamento do cluster 36

4.3 Arquitetura Proposta - Componentes disponibilizando suas APIs e ferramentas relacionadas aos dispositivos envolvidos 37

4.4 Interface Dead Peer Detector 42

4.5 Interface PacketFilter 45

4.6 Interface UserManager 46

4.7 Interface User 47

4.8 Interface Auth System 48

4.9 Interface Locator 48

4.10 Interface IDS 49

4.11 Interface Handoff 50

4.12 Interface VPN 51

4.13 Interface WDS 52

4.14 Interfaces para Listener do AP 53

5.1 Topologia do AirStrike 61

5.2 Tempo para realizar *lookup* de um objeto no Serv. de Nomes 66

5.3 Tempo para adicionar usuário com 1 dispositivo cliente no PA Cisco . 67

5.4 Tempo para adicionar usuário com 1 dispositivo cliente no PA 3Com 68

5.5 Tempo para adicionar usuário com 1 dispositivo cliente em 2 PAs . . 69

5.6 Tempo para adicionar usuário com 5 dispositivos clientes em 2 PAs . 70

5.7 Tempo para autenticar usuário 71

Lista de Tabelas

2.1 Resumo das características das ferramentas comerciais disponíveis para redes sem fio 19

5.1 Resumo das características das ferramentas comerciais disponíveis para redes sem fio comparadas com a solução proposta 73

5.2 Resumo dos requisitos, métricas de avaliação e cumprimento dos requisitos estabelecidos 74

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 confidenciali-

dade 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 radio-freqüência 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 proprietário 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

	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

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:

- 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 relacio-

namentos 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*

existente na rede, independente de fabricante, de maneira transparente. Assim, é possível definir níveis de acesso para os usuários cadastrados de maneira automática. Outro bom exemplo de uso desta ferramenta é a possibilidade de integração com o Sistema de Detecção de Intrusão, onde regras podem ser alteradas dinamicamente caso algum tipo de ataque seja detectado, bloqueando o acesso da estação não autorizada.

4.1.8 Serviço de Detecção de Desligamento de Estação

Está previsto no sistema de gerenciamento um dispositivo de Detecção de Desligamento de Estações. Este é mais um mecanismo específico para redes sem fio. O intuito de tal dispositivo é identificar uma situação que aparentemente não traz sérios riscos de segurança: a saída dos dispositivos móveis associados aos pontos de acesso sem o respectivo logoff. Isto acontece quando o usuário simplesmente desliga seu dispositivo, ou quando ele se desloca para uma região onde acaba por perder o sinal proveniente do ponto de acesso. O problema de segurança associado a estes casos são os ataques do tipo roubo de sessão (*session hijacking*). De maneira simplificada pode-se explicar este tipo de ataque da seguinte maneira: quando a conexão é interrompida pelo cliente sem fio abruptamente, o ponto de acesso mantém o estado da conexão que tinha anteriormente. Um atacante pode então, identificar esta situação, falsificar o seu endereço MAC, e roubar uma sessão válida se passando pelo usuário que simplesmente desligou seu comutador. Embora não presente na maioria das soluções comerciais analisadas, este mecanismo foi adicionado devido a sua visível importância para aumentar o nível de segurança da rede. Mas informações podem ser obtidas em [21].

4.1.9 Serviço de WDS

Um sistema de WDS (*Wireless Distribution System*) pode ser de extrema importância em um ambiente das WLANs. Embora ainda não padronizado, as operações básicas para tratar esta funcionalidade também devem estar presentes no *framework*.

A razão para isto é que a utilização deste dispositivo amplia o alcance que pode ser atingido por uma rede sem fio. Como já foi visto, o alcance de sinal de uma rede sem fio não está restrito aos limites físicos de prédios ou salas. Portanto, um mecanismo que seja capaz de ampliar ainda mais este alcance deve ser usado com extrema cautela, a fim de evitar que o sinal seja propagado de maneira irresponsável por áreas onde não se deseja ter cobertura, pois esta ampliação na área de cobertura pode potencializar os riscos associados à segurança da rede.

4.2 Visão Geral do Cluster de Gerenciamento

Um projeto arquitetural se faz extremamente necessário antes do desenvolvimento de qualquer aplicativo. Entende-se por arquitetura, o artefato onde estão definidos os protocolos, camadas e comunicação entre as entidades identificadas. Esta arquitetura deve ser escolhida de forma a permitir uma grande flexibilidade e nível de escalabilidade de modo que mudanças não previstas nesta fase inicial possam ser acomodadas no projeto em andamento de forma clara, rápida e fácil.

Aqui é apresentada a arquitetura proposta para a solução de gerência integrada de segurança. Todas as entidades lógicas e os protocolos de comunicação utilizados entre as entidades são apresentados.

O que se busca é uma solução o mais genérica, escalável e adaptável possível. A natureza do ambiente a ser modelado é distribuída portanto, também foi feita a opção por este modelo arquitetural para o projeto. Para tal, foram projetados clusters de gerenciamento conforme pode ser visto na Figura 4.1.

Um cluster pode ser definido como a entidade que agregará um ou mais pontos de acesso, as ferramentas de segurança inerentes ao funcionamento deste ambiente de acesso, juntamente com uma base de dados distribuída. Desta maneira, adquiri-se considerável escalabilidade, pois o sistema de gerenciamento proposto não provoca gargalos de comunicação e permite a execução de ações em uma área específica da infra-estrutura de acesso sem fio disponibilizada por uma instituição que detenha vários pontos de acesso.

Além disso, esta divisão em cluster permite uma administração mais voltada para ambientes encontrados mais facilmente no dia-a-dia, onde políticas diversas podem ser aplicadas a ambientes de acesso sem fio, maximizando as possibilidades de configuração diversas, facilitando o trabalho do responsável pela rede.

Com a disposição arquitetural projetada desta maneira, o software torna-se adaptável tanto a pequenos ambientes, como por exemplo, o gerenciamento de um único ponto de acesso, como também a ambientes maiores, com vários pontos de acesso e ferramentas de segurança sendo gerenciados, mesmo separados geograficamente.

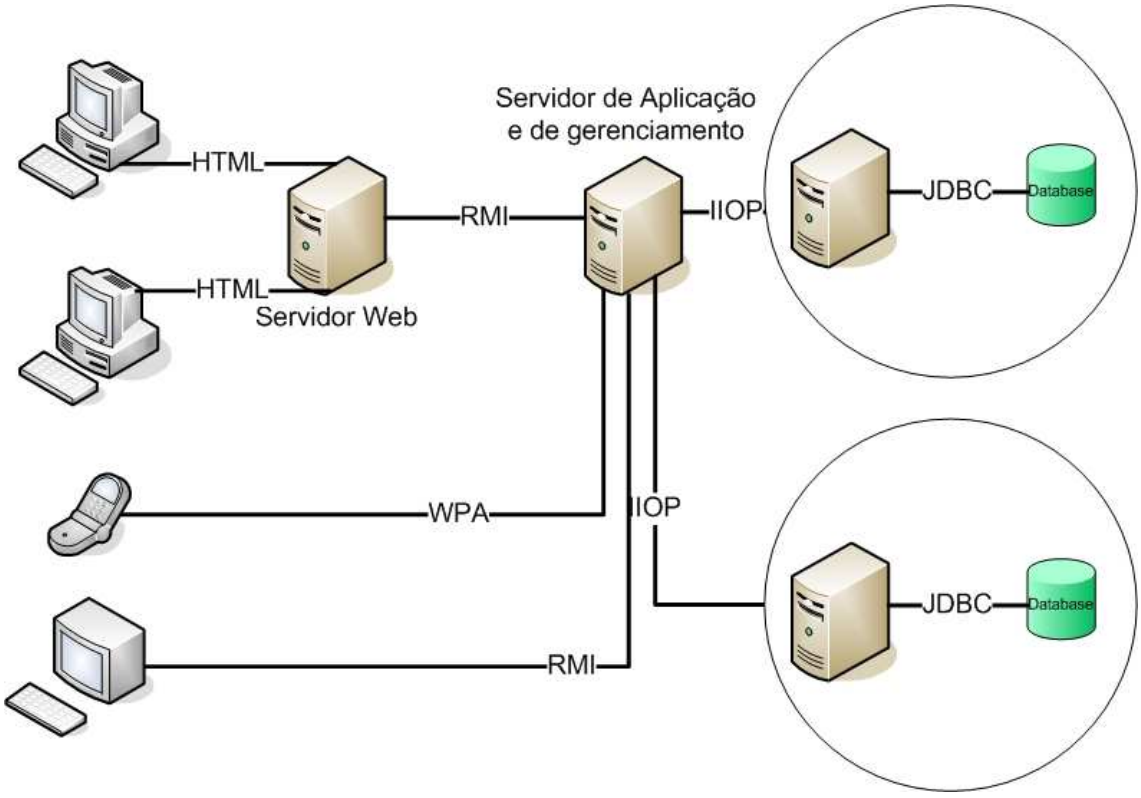

Figura 4.1: Arquitetura Proposta - Visão geral do cluster de gerenciamento

Algumas considerações precisam ser feitas neste ponto. A primeira delas é a razão pela qual há uma camada específica para prover a interface *Web* com as estações cliente. Através desta disposição é possível ter uma maior possibilidade de interfaces com o usuário e uma escalabilidade no servidor Web, pois desta forma torna-se viável o balanceamento de carga com a adição de outros servidores Web. Além disto, posteriormente outros tipos de interface capazes de acessar os dados diretamente no servidor de gerenciamento poderiam ser implementadas. Como exemplos de outros

tipos de interfaces, poderiam ser implementadas alternativas para PDA's (*Personal Digital Assistant*) ou mesmo uma interface gráfica para estação de trabalho.

A camada Web foi projetada para ser implementada utilizando páginas JSP (*Java Server Pages*) para gerar conteúdo dinamicamente. Estas páginas são capazes de obter informações remotamente do servidor de gerenciamento. Desta forma não há a necessidade do servidor Web e do servidor de gerenciamento estarem fisicamente na mesma estação.

4.3 Detalhamento do cluster de gerenciamento

No cluster de gerenciamento reside o núcleo do sistema proposto, tendo como componentes principais as ferramentas de segurança que devem estar presentes em um ambiente sem fio, conforme pode ser visto na Figura 4.2. A utilização destas diversas ferramentas faz-se necessária devido às diversas falhas de segurança presentes nos padrões do IEEE como também devido às necessidades de segurança específicas demandadas por certas aplicações e usuários. Geralmente a implementação de um ambiente para acesso a rede sem fio conta com a instalação de pelo menos algumas das ferramentas de segurança descritas. É exatamente por esta razão que elas aqui estão colocadas.

Deve ser ressaltado que um ambiente seguro não deve ter obrigatoriamente todas as ferramentas de segurança aqui mostradas. Deste modo foi realizado um levantamento das possíveis ferramentas que podem ser encontradas em um ambiente deste tipo chegando ao resultado da Figura 4.2. Mesmo que um ambiente específico não disponha de uma ou mais das ferramentas citadas, ainda assim é perfeitamente possível utilizar o *framework* proposto através da identificação de relacionamentos e dependências de comportamentos entre as ferramentas utilizadas, pois o mesmo é completamente adaptável ao cenário disponível. Já a base de dados incluída na figura deve, em princípio, possuir todos os dados para o gerenciamento do ambiente. É preciso observar que estas informações podem variar bastante, dependendo de que tipo de ferramentas de segurança estejam em uso no ambiente. Em geral, pode-se

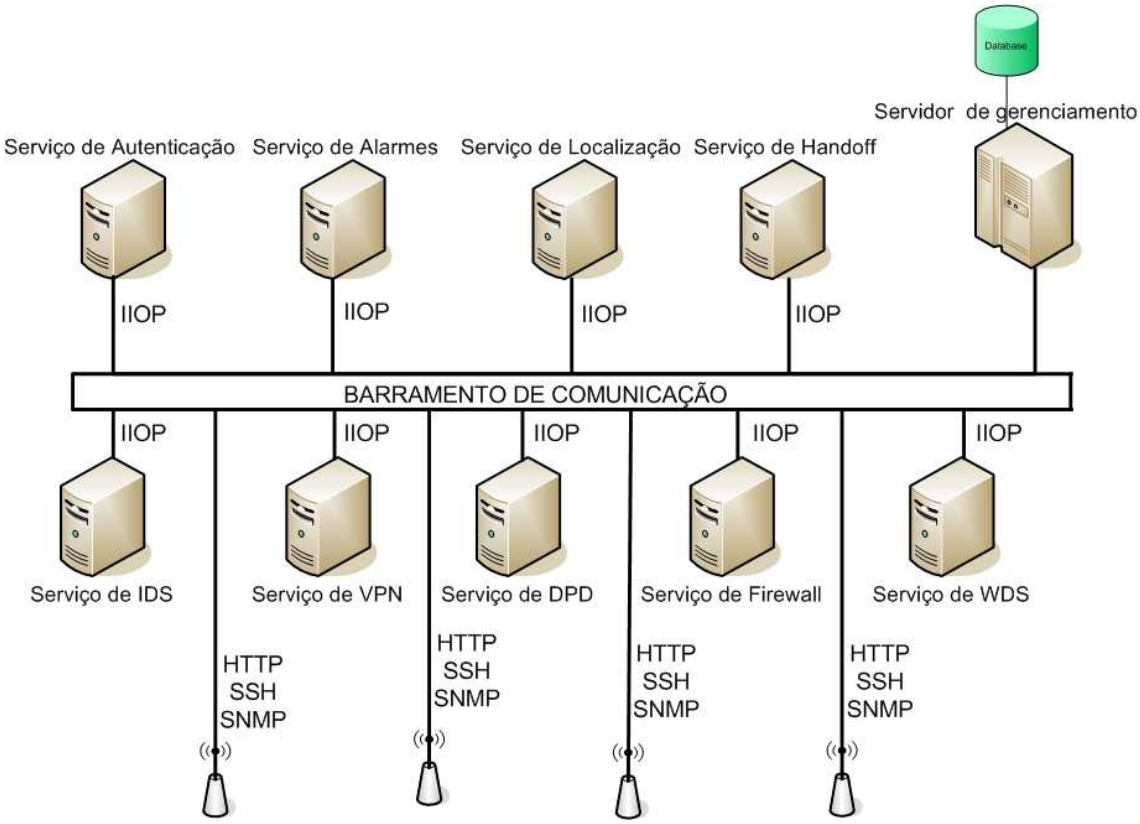

Figura 4.2: Arquitetura Proposta - Detalhamento do cluster

dizer que esta base poderia armazenar informações sobre usuários, dispositivos, permissões, configurações válidas para pontos de acesso e sistemas de segurança, dentre outras.

A Figura 4.3 indica como os componentes exportam suas APIs. É possível notar que todos os sistemas de segurança presentes no ambiente podem fazer uso da API entre si, pois se chegou a conclusão que em princípio, não deveria haver restrições sobre quais módulos podem se comunicar com quais. Isto porque num ambiente colaborativo, as relações entre os componentes do sistema devem ser as mais amplas possíveis. Outra característica que pode ser observada na figura é a camada de comunicação TCP/IP entre os sistemas de gerenciamento propostos e sua comunicação com as respectivas ferramentas envolvidas com um nível de abstração que não requer o prévio conhecimento de particularidades específicas de cada ferramenta.

Aqui vale a pena fazer uma ressalva importante. Como foi dito anteriormente, o sistema a ser desenvolvido será distribuído. Para tal, vários paradigmas de pro-

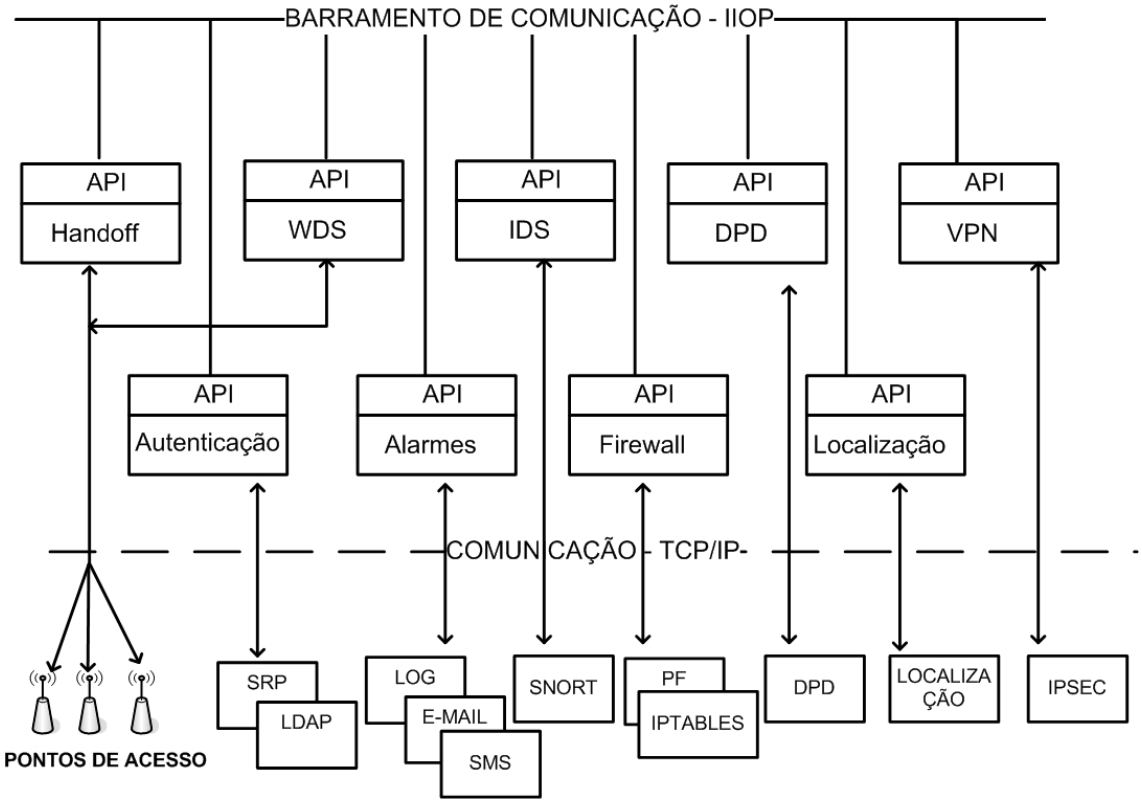

Figura 4.3: Arquitetura Proposta - Componentes disponibilizando suas APIs e ferramentas relacionadas aos dispositivos envolvidos

gramação diferentes poderiam ser usados, como por exemplo, a programação em *sockets*, Microsoft *DCOM* (*Distributed Component Object Model*) ou Java RMI (*Remote Method Invocation*), por exemplo. Cada um destes modelos de programação tem suas vantagens e desvantagens. Resumidamente podemos citar o elevado desempenho de aplicações baseadas em *sockets* contrastando com o baixo nível requerido para o desenvolvimento. Já o *DCOM* tem como principal vantagem funcionalidades semelhantes ao *middleware CORBA*, mas como ponto fraco sua relativa dependência às plataformas Microsoft. *RMI* também pode ser considerada uma solução que provê recursos similares à *CORBA*, no entanto, com sua utilização, todo o sistema deverá ser implementado em JAVA. Em se tratando de um novo projeto, como é o caso, esta seria uma solução viável. Porém, visando prover um maior escopo futuro de contribuições de terceiros, preferiu-se a adoção de uma outra tecnologia.

Como passo inicial para justificar a escolha que foi feita, é necessário inicialmente apresentar a opção por paradigma de programação. Devido à natureza distribuída

do sistema, optou-se pela orientação a objetos por ela prover um elevado grau de abstração, reusabilidade e facilidade de implementação. Desta maneira, é possível observar na Figura 4.2, o principal protocolo de comunicação entre as entidades presentes no modelo proposto: o IIOP (*Internet Inter Orb Protocol*) [22]. Este protocolo é especificado pelo OMG (*Object Management Group*), sendo considerado padrão de comunicação para sistemas distribuídos implementados utilizando o paradigma de orientação a objetos, sendo ele o protocolo que é utilizado pelo middleware CORBA da OMG. Além de ser um padrão reconhecido, ele possui várias implementações em diversas linguagens e uma vasta documentação para desenvolvedores, o que depõe como mais um motivo para sua escolha.

A utilização de um protocolo com estas características abre a possibilidade de implementação das aplicações na rede independentemente de sistema operacional, arquitetura ou linguagem de programação. Estas características são bastante úteis nesta aplicação de gerenciamento, visto que, como dito anteriormente, existe a grande necessidade de flexibilizações inerentes à proposta, o que acaba incorrendo em grandes possibilidades de desenvolvimento de novas funcionalidades futuras.

É importante ressaltar também que através deste mecanismo de distribuição, as entidades participantes do *framework* podem se comunicar livremente, o que abre caminho para uma maior escalabilidade. Neste caso, não há a necessidade de uma única estação de gerenciamento controlar todos os pontos de acesso existentes, tão pouco as ferramentas de segurança disponíveis. Assim, caso um cluster de gerenciamento possua várias entidades a serem gerenciadas, é possível distribuir a carga causada pelo gerenciamento destes múltiplos pontos de acesso através de mais de uma estação de gerenciamento onde cada estação de gerenciamento pode ficar responsável por gerir um número limitado de pontos de acesso e ferramentas de segurança.

Outro aspecto importante é a necessidade de um serviço de nomes no ambiente. Este serviço de nomes deve ser responsável por cadastrar e centralizar as informações referentes aos nomes associados aos objetos. Apenas desta maneira é possível fazer uma associação entre o par objeto/nome. Esta relação é extremamente

importante pois é através deste dispositivo que é possível identificar os objetos remotamente. Este mecanismo funciona basicamente de maneira similar a um servidor de nomes DNS (*Domain Name Service*), onde existe uma relação biunívoca entre nome/endereço.

Não poderia deixar de existir no sistema proposto mecanismo semelhante para mapeamento de nomes objetos. Embora ele não esteja visível na Figura 4.2, deve-se considerar implicitamente sua existência, pois sem a presença do mesmo, a utilização do sistema é inviável. No caso específico do sistema proposto, foi utilizada também uma implementação do sistema de resolução de nomes baseado do padrão da OMG. O sistema de nomes em questão torna possíveis algumas operações, dentre as quais, no escopo deste projeto, são de particular importância as seguintes: cadastro, remoção, atualização e pesquisa por nomes. De posse de um nome, qualquer objeto distribuído na rede pode ter acesso a um objeto que está sendo executado em outra máquina.

Já o protocolo SNMP também foi adicionado ao modelo como podendo fazer parte da comunicação entre as entidades e os pontos de acesso comerciais devido a grande possibilidade da aquisição de informações relevantes de gerência junto aos pontos de acesso. Esta coleta de informação pode ser muito importante na avaliação de outras ferramentas de segurança do sistema. Além disso, o SNMP é sem dúvida, um dos padrões mais encontrados nas soluções de gerência atuais. Apesar das limitações desta alternativa em relação ao que se busca no *framework* proposto, com a integração dos mecanismos de segurança, a utilização deste protocolo pode ser de grande valia no caso, por exemplo, da monitoração de configuração de determinados dispositivos para a verificação de alteração de configuração de maneira não autorizada.

O protocolo HTTP também está presente no modelo devido a uma situação peculiar. Vários pontos de acesso comerciais permitem a gerência e configuração do equipamento pela interface Web. Uma vez detectada tal característica comum à maioria deste tipo de equipamento, faz-se necessário prever que alguns módulos para configuração de parâmetros nestes equipamentos deverão comunicar-se através da

utilização deste protocolo para que seja possível alterar as configurações dos pontos de acesso de maneira remota e automática. Neste caso específico, a aplicação cliente deve "enganar" o ponto de acesso se fazendo passar por um administrador utilizando a interface web do equipamento. Para isto, a aplicação deve ser hábil a utilizar o protocolo HTTP como meio de comunicação com o ponto de acesso.

Para o *framework* não ficar restrito ao protocolo HTTP para realização de configuração dos pontos de acesso, o protocolo SSH também foi adicionado como possibilidade de comunicação entre a estação de gerenciamento e os pontos de acesso comerciais. Em ambos os casos, a implementação das aplicações que irão controlar os pontos de acesso comerciais são dependentes dos fabricantes dos mesmos. Embora claramente possa haver uma semelhança entre modelos similares do mesmo fabricante, dificilmente a interface de comunicação ou até mesmo o protocolo usado na comunicação com o ponto de acesso são compatíveis. Desta forma, é necessário que os módulos do sistema responsáveis pela comunicação com os pontos de acesso comerciais sejam implementadas de maneira a refletir melhor o ambiente encontrado. É possível que posteriormente, para gerenciar um determinado ponto de acesso, clientes possam ser desenvolvidos por terceiros e acoplados ao *framework* pois a interface que especifica o comportamento dos pontos de acesso é a mesma.

Aqui entra um ponto interessante neste aspecto: a dificuldade encontrada no desenvolvimento de aplicações que interagem com pontos de acesso comerciais. Isso se deve à grande ausência de documentação por parte dos fabricantes. É praticamente impossível encontrar algo similar a uma API para interagir com pontos de acesso comerciais. A solução para este entrave é a realização de um processo similar a uma engenharia reversa, onde são analisados, no caso de interfaces HTTP com os respectivos dispositivos, o código-fonte das páginas da interface de gerenciamento web para que possam ser identificados os nomes dos campos a serem preenchidos e como fazer com que o ponto de acesso responda corretamente a uma requisição de configuração feita pela interface web. Neste trabalho, isto foi feito para os pontos de acesso *Cisco Aironet 1200* e um *3Com OfficceConnect*, conforme poderá ser visto em mais detalhes no Capítulo 5.

Resumidamente, os protocolos são:

- IIOP - O protocolo padrão da OMG será utilizado para a comunicação entre o servidor de gerenciamento e as entidades lógicas;
- SNMP - Este protocolo será utilizado para a comunicação entre o servidor de gerenciamento e o ponto de acesso para a busca de possíveis informações que sejam disponibilizadas por este protocolo de gerenciamento;
- HTTP - Será utilizado para realizar a comunicação com pontos de acesso comerciais fazendo às vezes de interface Web com os dispositivos;
- SSH - A mesma função do item anterior, utilizando uma interface de linha de comando;
- RMI - Será utilizado para que o servidor *WEB* possa buscar as informações no servidor de gerenciamento propriamente dito.

4.4 A API

O processo de desenvolvimento de software sempre trouxe desafios e dificuldades. Neste sentido, a utilização de uma API para o desenvolvimento de aplicações permite a abstração de funcionalidades e torna mais simples o processo de futuras implementações de módulos do sistema por terceiros. Isto ocorre devido ao formalismo contido na especificação da API, que traz as informações que devem ser seguidas pelo desenvolvedor para implementar determinado módulo. Desta forma, o software desenvolvido torna-se facilmente acoplável em relação ao *framework* como um todo, onde componentes podem ser desenvolvidos posteriormente de maneira a facilmente integrarem-se com outros componentes previamente existentes, uma vez respeitadas as especificações contidas na API descrita. Além disso, há também uma redução do tempo de implementação e maior facilidade de entendimento das necessidades básicas para que um determinado componente seja desenvolvido de forma a ser compatível com o que foi especificado, como características que reforçam o uso de uma API para a especificação do *framework*.

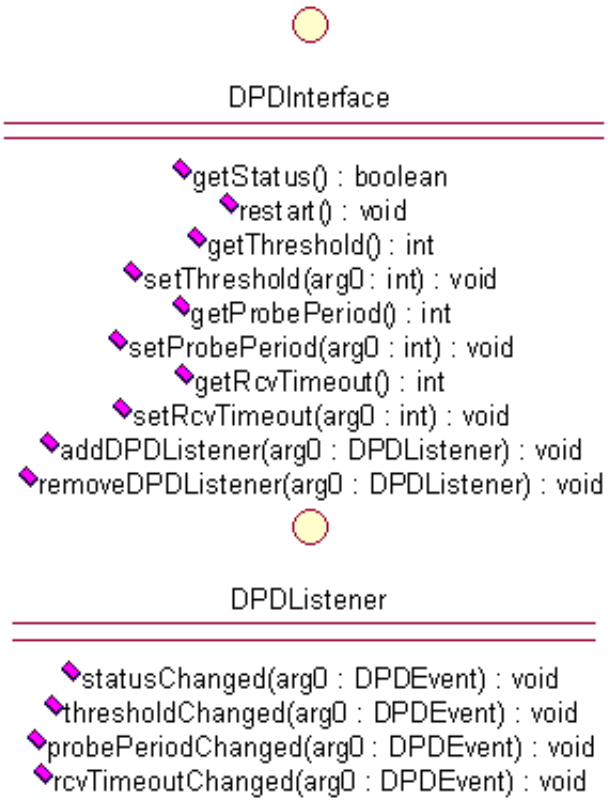

Figura 4.4: Interface Dead Peer Detector

A API foi especificada usando o formalismo UML (*Unified Modeling Language*) como linguagem de modelagem. UML é a linguagem padrão especificada pela OMG para definição de sistemas complexos e que foi amplamente adotada no mercado, sendo mundialmente compreendida e interpretada. Sua principal aplicação é a modelagem de sistemas que utilizam o paradigma de orientação a objetos, embora possa também ser utilizada na modelagem de sistemas que utilizam paradigmas procedurais.

Outro ponto que merece destaque na API é o mecanismo de "integração" entre as diversas ferramentas de segurança já descritas. É importante lembrar que um dos pré-requisitos da arquitetura proposta é que posteriormente componentes desenvolvidos por terceiros possam ser acoplados ao *framework* de maneira simples. A solução que possibilita esta característica é a utilização do padrão de projeto *Observer*. Este padrão surgiu para a resolução da seguinte questão: como acoplar dois objetos que não podem se conhecer em tempo de compilação? Se assim fosse feito,

o acoplamento e possíveis iterações entre as entidades do sistema teriam que ser pré-definidas, o que não é o caso. Embora em um primeiro esta característica possa não ser vista como um problema, a escolha feita permite um maior grau de adaptabilidade do *framework* em relação a novos relacionamentos não previstos neste trabalho.

Neste caso específico foi feita a utilização deste padrão de projeto de maneira distribuída. Desta maneira, um dado componente pode se cadastrar como interessado em mudanças de estados ou outros eventos ocorrendo em outros componentes. Quando esta mudança ocorre, todos os interessados cadastrados são comunicados automaticamente. Assim, podem realizar as alterações que julgarem relevantes de acordo com a mudança ocorrida. Ilustrativamente é possível indicar este comportamento como sendo similar a um "bus" distribuído: trata-se de um "bus" pois informações que são nele colocadas tornam-se disponíveis aos demais membros do bus (no caso, aos interessados cadastrados na informação). É importante aqui ressaltar a importância deste comportamento. É através dele que a integração entre os mecanismos de segurança é possível, independentemente dos detalhes que cercam a implementação de determinado componente. Mesmo podendo ser considerado um mecanismo de comunicação trivial, ele pode ser considerado também extremamente eficiente e indicado para os requisitos apresentados neste trabalho. Assim, unem-se dois mundos ideais: uma solução simples aplicada na resolução de um problema de maior complexidade. Mais detalhes sobre este padrão podem ser obtidos em [23].

Como exemplo, pode ser citada a seguinte situação hipotética ilustrativa: o sistema de detecção de intrusão identifica na rede um ponto de acesso não autorizado, ou ocorre a simples alteração do endereço IP de determinado ponto de acesso. O módulo responsável pelo sistema de *firewall* poderia estar interessado nestas informações para barrar o tráfego proveniente deste dispositivo alterando dinamicamente suas regras.

Para cada ação que altere o estado ou configuração dos mecanismos previstos no ambiente existe um método respectivo em uma outra interface que indica aos interessados o tipo de mudança ocorrida. Assim, as alterações podem ser feitas de

maneira específica pelos respectivos interessados.

Desta forma atinge-se um elevado grau de independência entre os componentes possibilitando que posteriormente um desenvolvedor possa implementar um novo componente, ou atualizar um pré-existente, da maneira que lhe for conveniente, obtendo todas as informações que são relevantes de maneira simples e transparente. Assim, uma vez seguidas as especificações descritas, é possível desenvolver uma aplicação de gerenciamento que utilize esta API para controlar os sistemas de segurança e dispositivos contidos na rede.

Como foi visto na seção 4.1 existe um número significativo de ferramentas de segurança previstas. Um dos grandes desafios foi identificar as operações que deveriam estar presentes na API de cada uma delas. Foi feito um esforço para que os métodos especificados para cada ferramenta representassem o mais fielmente possível o comportamento das mesmas. O resultado a que se chegou foi um conjunto inicial de cerca de cem operações que se julga ser um bom passo inicial. Obviamente que novas operações podem ser identificadas e agregadas ao modelo para torná-lo mais completo e funcional.

A seguir serão apresentados os diagramas com as especificações das interfaces das entidades presentes no sistema.

Na Figura 4.4 é possível verificar as interfaces associadas ao controle de dispositivos de DPD. Através desta interface é possível interagir com esse sistema e alterar seus parâmetros de configuração, que estão intimamente ligados principalmente às configurações de *timeout* em relação a conexão do cliente sem fio. Aqui é válido fazer uma breve explicação acerca de alguns dos métodos presentes do modelo. Os métodos relacionados ao campo *threshold* indicam operações que estão ligadas ao número máximo de tentativas de monitoração que serão feitas em relação a determinado cliente sem fio antes que ele seja declarado como inativo na rede. Já os métodos relacionados *probe period* dizem respeito ao intervalo de tempo que será utilizado durante as medições. Por fim, métodos relacionados à *receive timeout* indicam o intervalo de tempo que o servidor deve aguardar por uma resposta a uma requisição de monitoração enviada previamente antes que esta seja considerada inválida.

Um ponto interessante a ser colocado aqui é a forma como as interfaces que possuem sufixo *Listener* são especificadas. É através destas interfaces que os interessados pelas mudanças de estado/configuração são informados de tal mudança. Pode ser observada a existência de um atributo com sufixo *Event*. Estas classes de eventos encapsulam a informação necessária para que os interessados da informação tenham acesso a todo o estado do objeto responsável pelo evento.

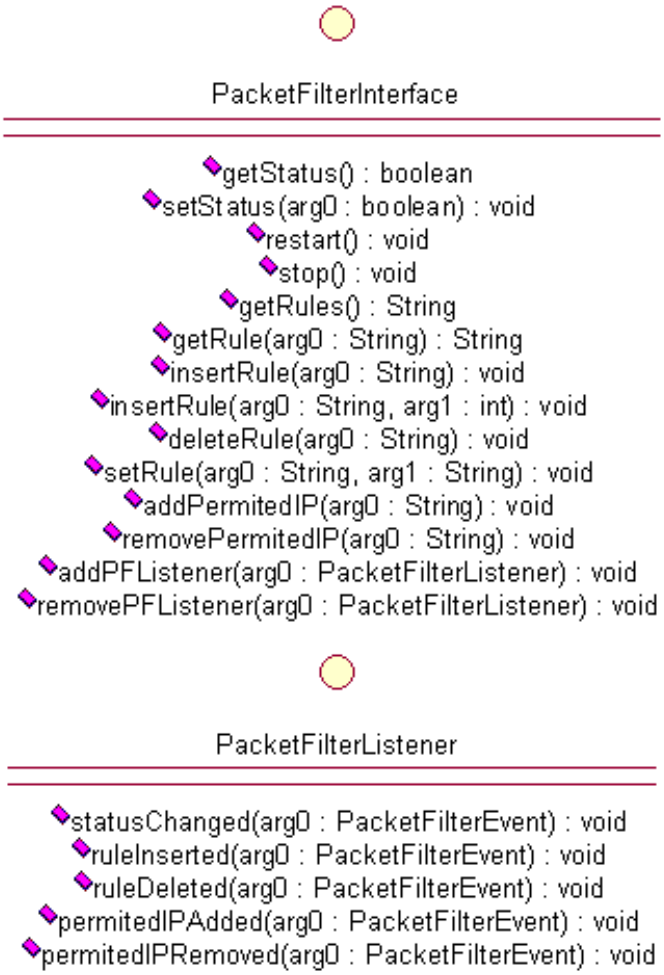

Figura 4.5: Interface PacketFilter

A Figura 4.5 mostra como interagir com um filtro de pacotes do ambiente sem fio, bem como as operações disponíveis para alterar seus parâmetros de configuração. Como pode ser observado, as regras que podem ser passadas como parâmetro para o *firewall* são apenas cadeias de caracteres. Isto se deve ao fato de que a semântica das regras diverge completamente entre os diversos filtros de pacotes disponíveis. Assim, optou-se por não condicionar a Interface de *firewall* a uma sintaxe espe-

cífica, o que permite um maior nível de flexibilidade ao *framework* proposto, não estando a Interface condicionada a uma solução particular. Futuramente é possível tentar verificar a viabilidade do uso de um mecanismo que possibilite a utilização de uma semântica única, mesmo com algumas limitações, que possa ser traduzida para os diversos modelos de *firewalls* disponíveis, sempre levando-se em consideração a restrição de manter a compatibilidade com esta interface.

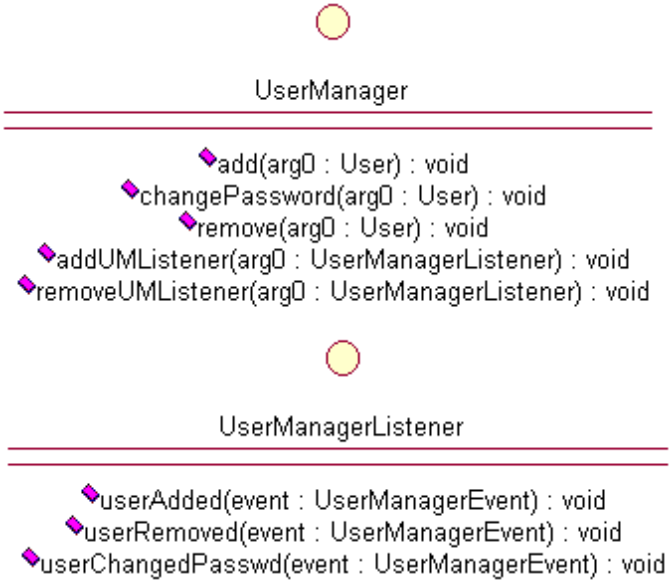

Figura 4.6: Interface UserManager

A Figura 4.6 mostra a interface de gerenciamento de usuário. Embora simples, é através dela que são cadastrados usuários no sistema de autenticação. Este cadastro de usuários pode desencadear várias outras ações, pois o atributo *UserManagerEvent* encapsula um objeto do tipo *User*. Como pode ser visto na Figura 4.7, este objeto tem vários campos que podem ser utilizados por diversas outras ferramentas de segurança. Isto pode ser exemplificado com a utilização de sistema de alarmes indicando que determinado usuário foi adicionado ao sistema. Em uma abordagem mais interessante, há também a possibilidade da alteração dos filtros de MAC dos pontos de acesso comerciais para permitir a associação e *handoff* do usuário baseados nos dispositivos clientes que ele tem permissão de utilizar.

Na Figura 4.8 são mostradas as interfaces que atuam sobre o sistema de autenticação. Embora aparentemente ela possa não demonstrar grandes funcionalidades,

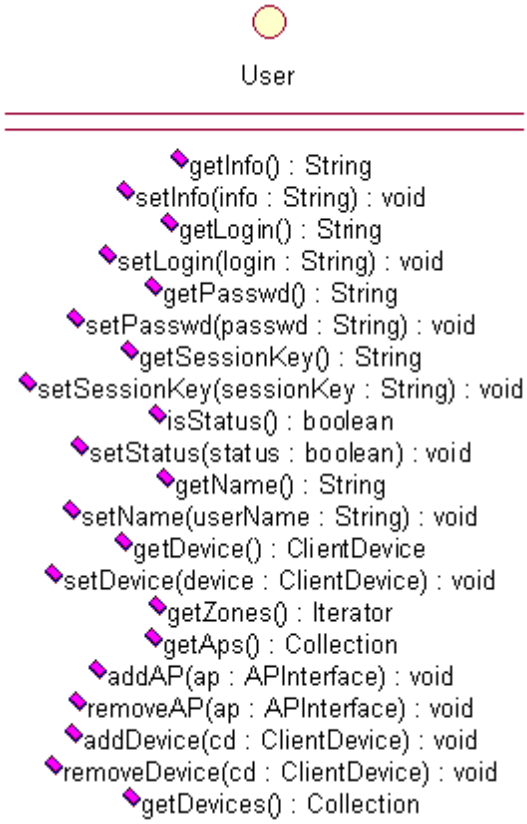

Figura 4.7: Interface User

é de extrema importância sua presença no sistema. Uma das importantes relações entre o sistema de autenticação é com o sistema de *firewall*. Através desta relação é possível liberar ou limitar o acesso do usuário aos recursos da rede. Além desta relação, outras mais também são passíveis de ocorrer, como por exemplo, ativar possíveis sistemas de contabilidade, monitorar uso do canal ou a atividade do usuário.

Já a Figura 4.9 mostra as operações disponíveis para lidar com a interface de localização. Sistemas de localização têm muitas aplicações em redes sem fio, com algumas particularmente interessantes no aspecto de segurança. Pode-se através do uso de sistemas deste tipo verificar a posição de pontos de acesso não autorizados, ou ainda de dispositivos estranhos presentes na rede. Outro bom exemplo que não é encontrado nas soluções comerciais é a própria alteração da posição de pontos de acesso autorizados. Este ponto pode ser potencialmente interessante pois usuários podem mover pontos de acesso do ambiente em que estão visando um favorecimento

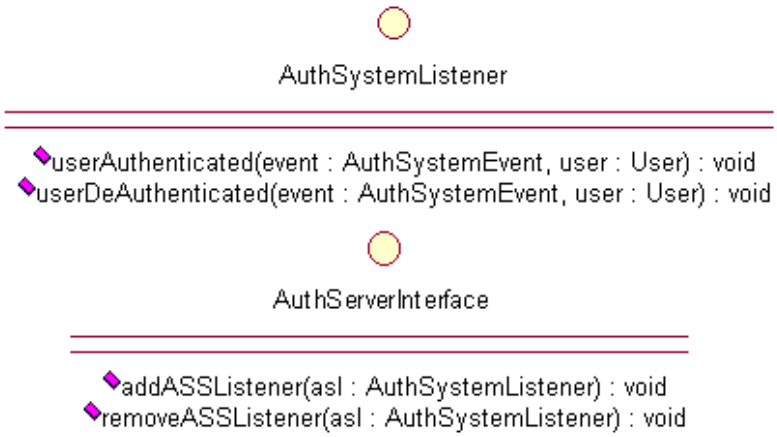

Figura 4.8: Interface Auth System

no nível de sinal de acordo com os próprios interesses. Desta maneira, ele pode estar involuntariamente disponibilizando acesso à áreas não permitidas previamente. Portanto, seria interessante que o administrador pudesse ser informado acerca de mudanças deste tipo.

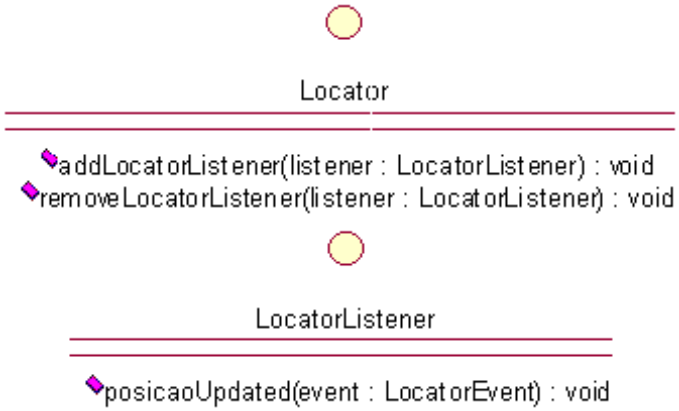

Figura 4.9: Interface Locator

A Figura 4.10 indica as operações que podem ser realizadas caso esteja disponível um sistema de detecção de intrusão no ambiente sem fio. É valido ressaltar que as operações disponíveis para estes sistemas são a de reportar atividades indevidas. Neste caso específico, reportar tentativas de intrusão. Diversas técnicas comerciais estão disponíveis para detecção de intrusão, como por exemplo a busca de assinaturas que indiquem algum ataque já conhecido. Não será discutido aqui o mérito das técnicas aplicadas, mas deve ser ressaltada a importância de tomar

alguma ação para mitigar um problema identificado. Com base nisso, encaixam-se aqui as interfaces propostas pois dado que existe um sistema de IDS na rede sem fio, possíveis interessados em tentativas de invasão podem ser avisados para que possam realizar alguma ação, que pode ser simplesmente o envio de uma mensagem para o administrador, como a desabilitação de determinado equipamento de rede(um ponto de acesso ou um switch, por exemplo).

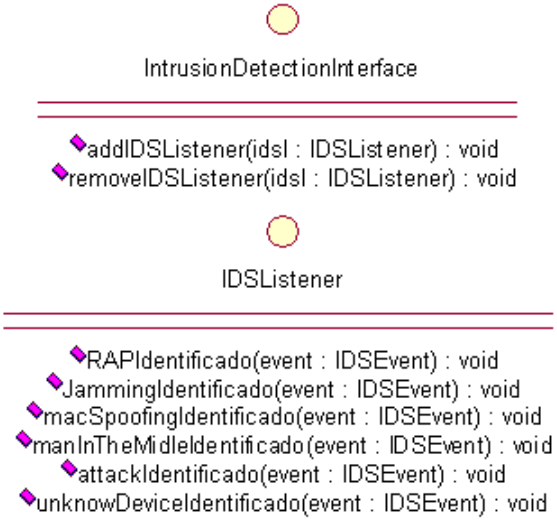

Figura 4.10: Interface IDS

A Figura 4.11 são mostradas as operações possíveis quando se tratando o mecanismo de *handoff*. É importante aqui ressaltar que o mecanismo e algoritmos envolvidos neste processo são especificados no próprio padrão do IEEE. Embora muitos trabalhos publicados em artigos sugiram métodos alternativos ou mudanças em algumas características específicas a fim de obter uma melhora no desempenho deste mecanismo, elas não foram consideradas aqui, por não serem objeto de estudo do presente trabalho. Além disso, embora sejam compatíveis entre si, fabricantes de pontos de acesso e de placas de rede sem fio eventualmente alternam a ordem que as mensagens de controle são enviadas para realização do *handoff*, dificultando um processo que seja aplicável a qualquer ambiente. Em razão do exposto, somente foram definidas as operações de adicionar ou remover a propriedade de um usuário realizar *handoff* para determinados pontos de acesso. Também foram incluídos métodos para recuperar a chave de sessão utilizada pelas partes comunicantes e a lista de pontos de acesso que determinado usuário está pré-autenticado. Esta última ope-

ração foi incluída pois algumas soluções comerciais realizam esta pré-autenticação a fim de reduzir os tempos envolvidos neste processo.

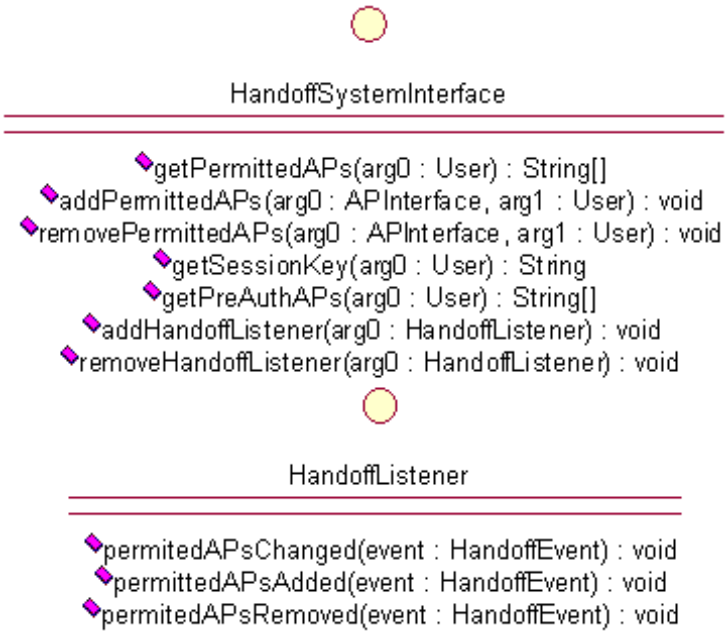

Figura 4.11: Interface Handoff

A Figura 4.12 mostra as operações que podem ser realizadas sobre um servidor VPN. Aqui vale a ressalva da existência de várias implementações diversas de servidores VPN. Neste sentido, optou-se por um conjunto reduzido de funcionalidades para manter a compatibilidade. Num momento posterior pode ser realizado um estudo para verificar que outros métodos podem ser aqui adicionados de maneira que a compatibilidade entre as soluções disponíveis não seja comprometida.

A Figura 4.13 mostra a Interface do dispositivo de WDS do sistema. Como dito anteriormente, a incorreta utilização deste mecanismo pode elevar os riscos de segurança, pois amplia a área de cobertura da rede sem fio. Sem as devidas precauções, esta pode ser uma porta para possíveis tentativas de invasão.

Na Figura 4.14 indica os possíveis eventos que podem ser reportados quando realizado o gerenciamento sobre pontos de acesso. Quando é realizada alguma alteração nas configurações do dispositivo, as entidades interessadas nestas informações são avisadas. Embora em um primeiro momento estas operações possam ser classificadas como triviais, o seu potencial de uso no sistema é enorme. Para justificar

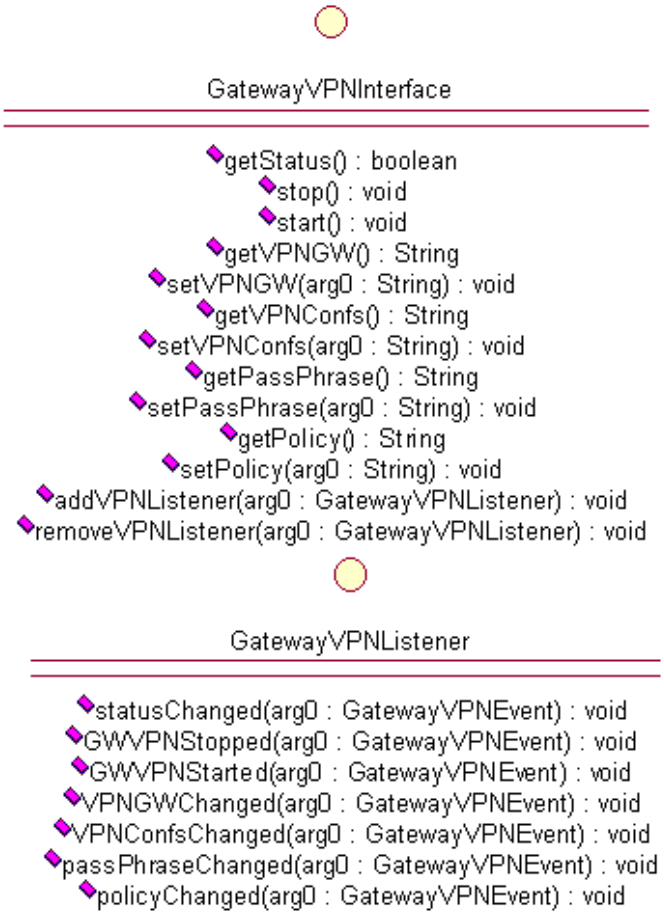

Figura 4.12: Interface VPN

esta afirmação, basta imaginar o seguinte: de maneira geral, os pontos de acesso se localizam em áreas de fácil acesso pelos usuários. Neste caso é perfeitamente factível que usuários mal intencionados pressionem o botão *reset* do equipamento a fim de configurar o equipamento com os padrões de fábrica, com senhas padrão. Assim, podem alterar as configurações do equipamento de acordo com suas necessidades, não respeitando as políticas de segurança pré-estabelecidas e colocando em risco a rede do ambiente. Os métodos desta interface associados a um sistema que monitore as configurações do equipamento são extremamente úteis para evitar tais situações que comprometem a segurança do ambiente.

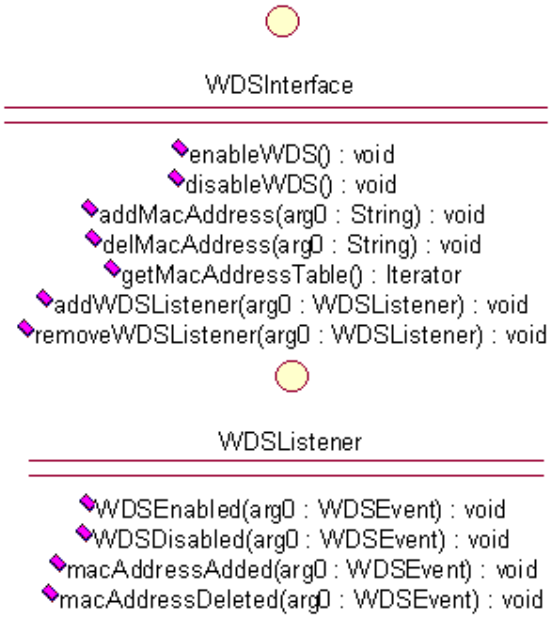

Figura 4.13: Interface WDS

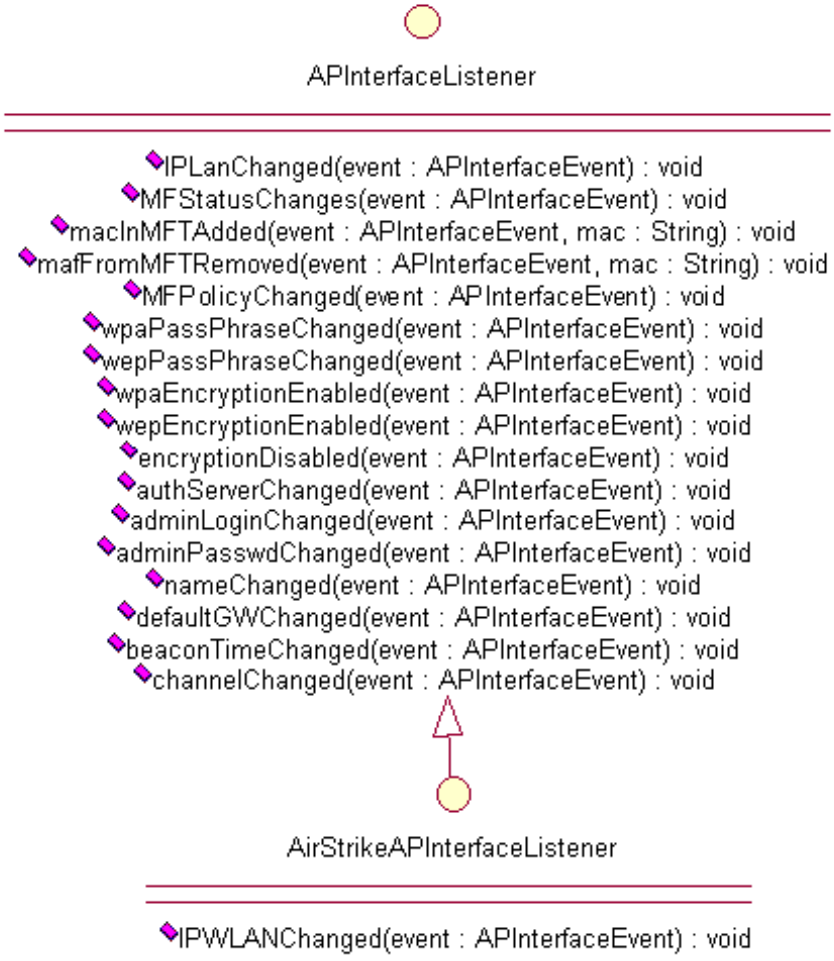

Figura 4.14: Interfaces para Listener do AP

Capítulo 5

Implementação do Framework

NESTE capítulo serão apresentados os detalhes do ambiente implementado para a validação do *framework* proposto, com a descrição das operações que foram implementadas, o ambiente de implementação e de testes, bem como os resultados obtidos.

5.1 A implementação

O objetivo de uma implementação para o *framework* proposto neste trabalho é o de validar a arquitetura apresentada, bem como os mecanismos de integração, e a escolha dos protocolos que foram utilizados. Assim, espera-se que o *framework* proposto possa ser aprimorado e utilizado posteriormente em outras aplicações e ambientes depois de demonstrada aqui sua viabilidade e eficácia.

A linguagem de programação escolhida para a implementação do protótipo para validar a arquitetura do *framework* proposto foi Java. Ela foi escolhida por uma série de fatores dentre os quais pode-se destacar o fato de ser uma linguagem orientada a objetos, o que facilita a implementação do paradigma de sistemas distribuídos adotado na arquitetura. Além disso, ela possui amplo suporte à utilização do protocolo IIOP especificado para atuar como *midlleware* de comunicação entre as entidades presentes no sistema. Com a escolha desta linguagem adquire-se uma aplicação de gerência que poderá ser executada em um grande número de arquiteturas de computador e independente de sistema operacional. Assim, mesmo que determinado mecanismo de gerência tenha como pré-requisito ser executado em determina plataforma operacional, o sistema de gerenciamento fica isento desta restrição.

Uma vez feita a escolha pela linguagem de programação, a decisão acerca de que implementação de IIOP utilizar teve início. Isto ocorreu pois Java oferece mais de um mecanismo que prevê o uso do IIOP. Dentre estes métodos podem ser destacados dois pela sua ampla utilização: CORBA e RMI-IIOP. O primeiro trata da pura implementação do padrão especificado pela OMG na linguagem Java, e o segundo, de uma implementação que busca ser um misto da programação em Java utilizando RMI com suporte ao protocolo IIOP. Neste último caso, IBM e Sun se uniram para desenvolver esta solução que busca agregar as melhores características de ambas as abordagens.

Optou-se pela utilização de RMI-IIOP por uma série de razões, dentre os quais podem ser destacados a maior facilidade de desenvolvimento, pois não existe a necessidade de aprendizado e especificação das interfaces de comunicação dos compo-

nentes através da linguagem IDL (*Interface Definition Language*), como é o caso de CORBA. No caso de RMI-IIOP, as operações dos objetos remotos são especificadas como se fossem interfaces na linguagem Java, o que facilita muito o entendimento e desenvolvimento. Outro ponto que depôs a favor da escolha do RMI-IIOP é a sua compatibilidade tanto com entidades que utilizam o protocolo IIOP para comunicação como com o RMI que utiliza o protocolo JRMP *Java Remote Method Protocol* da Sun. Mais especificamente, um servidor desenvolvido com RMI-IIOP é compatível com clientes desenvolvidos em RMI, RMI-IIOP e CORBA, o que amplia consideravelmente as alternativas possíveis para implementação dos componentes. Embora as interfaces do sistema não necessitem ser especificadas usando IDL, elas precisam estar neste formato caso seja necessária a implementação de componentes que utilizarão CORBA. Para tal, é possível gerar de maneira simples a especificação IDL das interfaces remotas através da ferramenta *rmic* com a opção *-idl*. Isto possibilita a correta implementação de componentes que por ventura venham a ser desenvolvidos utilizando CORBA.

É importante aqui indicar que a escolha pelo uso do protocolo IIOP em detrimento de outras soluções possíveis foi feita principalmente devido a sua ampla utilização e disponibilidade, o que faz com que o desenvolvimento não esteja restrito a uma única linguagem de programação. Embora estudos indiquem que, no caso específico da linguagem Java, a utilização de RMI tenha um desempenho superior sobre outras tecnologias de comunicação, foi feita a opção pela alternativa que possibilitasse maior compatibilidade possível para o desenvolvimento. Não foi realizado neste trabalho um estudo comparativo sobre a eficiência dos possíveis métodos de comunicação, mas detalhes acerca do desempenho de diversos métodos para comunicação remota usando a linguagem Java podem ser encontrados em [24].

Como já dito, a implementação do protótipo foi feita com a utilização do mecanismo de interfaces da linguagem Java. Com isto, a especificação das operações remotas que serão utilizadas no sistema tornou-se bastante simples devido à facilidade da especificação de interfaces na linguagem escolhida. Para indicar que uma interface em Java será acessível por objetos distribuídos, ela deve estender a interface *java.rmi.Remote*. Além disso, os métodos devem ser declarados para lançar

exceções do tipo *java.rmi.RemoteException* caso a operação remota não seja bem sucedida. Esta especificação de interfaces é idêntica tanto para utilização de JRMP quanto para utilização de IIOP.

Nas classes que implementam as interfaces remotas é que entram as diferenças entre a utilização do IIOP ou do JRMP para comunicação. No caso aqui apresentado, as classes devem estender *javax.rmi.PortableRemoteObject* e implementar a interface com a especificação dos métodos remotos. O procedimento então é a compilação dos componentes envolvidos, seguida da utilização da ferramenta *rmic* com a opção *-iiop* para geração das classes que serão utilizadas para a realização da comunicação com a utilização do protocolo IIOP.

Conforme dito na Seção 4.3, um servidor de nomes é necessário para o funcionamento do ambiente. Nesta implementação foi utilizado o *orbd*, ferramenta que é disponibilizada juntamente com o kit de desenvolvimento Java. Esta ferramenta provê um serviço de nomes compatível com o padrão CORBA. Uma vez definida e implementada a interface e o código do servidor, é necessário cadastrar o objeto que será acessível remotamente neste servidor de nomes. Para tal, para cada objeto remoto foi criado uma classe com sufixo *Server* que realiza a instanciação do objeto remoto e em seguida publica sua referência no servidor de nomes através do método *rebind* da interface *javax.naming.Context*.

Para fins de padronização, os nomes atribuídos às entidades seguiram o seguinte padrão: parte do nome da entidade seguido do IP da estação onde ela está. Assim, o Servidor de Autenticação (Auth System Service) foi cadastrado no serviço de nomes com a forma "auth192.168.1.1", ou seja, sua abreviação seguida do endereço IP onde ele está sendo executado. Após a publicação dos nomes dos objetos no servidor de nomes, os demais componentes do sistema podem utilizar o método *lookup* da interface *javax.naming.Context* passando como parâmetro o nome previamente cadastrado para recuperar a referência do objeto remoto. A partir deste momento, os métodos podem ser aplicados a estas referências de objetos como se estes fossem objetos locais. Em nenhum momento há a preocupação com a identificação de em que local da rede o objeto remoto está sendo executado.

Devido ao uso do mecanismo de interfaces, componentes que implementem as operações especificadas nestas interfaces podem ser acopladas posteriormente ao *framework* de maneira simples. É importante ressaltar que estes componentes não necessitam ser implementados em Java, mas em qualquer linguagem de programação que dê suporte à utilização do protocolo IIOP como *middleware* de comunicação.

Para todas as interfaces remotas do sistema existe também uma interface com sufixo "Listener", que indica as mudanças de estado ou configurações das ferramentas presentes no sistema. Estas interfaces Listener também poderão ser acionadas remotamente, pois os interessados nas informações não necessariamente devem estar na mesma máquina. Com isso, estas interfaces devem seguir os mesmos requisitos das interfaces remotas do sistema, estendendo a interface *javax.rmi.Remote* e também de *java.util.EventListener* para indicar que as classes que implementaram esta interface serão "listeners" de informação. Os métodos especificados nas interfaces Listeners contém parâmetros que tem como tipo classes que foram nomeadas com sufixo *Event*. Estes objetos encapsulam toda a informação sobre quem gerou o evento, tornando possível que o interessado na informação possa recuperar esta e outras informações que podem ser encapsuladas adicionalmente. Para tal, estas classes estendem *java.util.EventObject*.

Como pode ser visto na arquitetura descrita no Capítulo anterior, há muitas entidades lógicas envolvidas previstas para o *framework*. Desenvolver um protótipo envolvendo todas estas entidades seria de uma complexidade muito grande. Outro fator que comprometeu o desenvolvimento completo do *framework* foi o fato da inexistência de alguns dos módulos. Como exemplos, podem ser citados os módulos de WDS e IDS. Para implementar um protótipo que contasse com estas ferramentas seria necessário que estas fossem inicialmente desenvolvidas para posteriormente serem integradas ao *framework* e este não era o objetivo deste trabalho, embora alguns mecanismos de alarmes tenham sido implementados para fins de testes.

Desta forma, optou-se pelo desenvolvimento de um conjunto de funcionalidades de apenas algumas destas entidades, a saber, *firewall*, Gateway VPN, Serviço de Autenticação, Serviço de Gerenciamento de Usuário, Serviço de DPD, Sistema

de *Handoff*, Sistema de Localização e Sistema de Alarmes. O processo de escolha das funcionalidades a serem implementadas teve como critério decisivo os métodos que foram identificados de imediato como sendo preponderantes para mecanismos de integração com outras ferramentas. A partir daí, outros métodos também foram implementados, devido a sua importância subjetiva no sistema. Estes critérios subjetivos foram guiados com base no nível de segurança que a implementação de determinado método traria. Como exemplo, métodos relativos a criptografia, chaves e etc, foram implementados para os pontos de acesso.

Todas as características descritas até aqui são relativas à parte do gerenciamento distribuído. Através dele é possível ter vários componentes distintos realizando gerenciamento de componentes diversos sendo executados de maneira distribuída na rede. Para acessar estes recursos distribuídos, uma interface web simplificada foi implementada utilizando JSP. Como medida de simplificação dos testes, não foram implementados os componentes de visualização previstos inicialmente. Deste modo, as páginas JSP se comunicam diretamente com os objetos distribuídos no sistema. Para que estas páginas conseguissem acessar remotamente os componentes distribuídos, elas foram implementadas de modo a conseguir uma referência para o servidor de nomes do ambiente. Assim, as referências para os objetos distribuídos podem ser acessadas a partir do servidor web, que não necessita estar sendo executado na mesma estação de outros componentes. Um ponto interessante a ser mencionado é que o intuito final da implementação não foi o desenvolvimento de uma interface web, e sim, a comunicação, integração e comportamento automático dos sistemas de segurança implementados no ambiente.

É válido ressaltar que o conceito de "aplicações" clientes do sistema proposto é um pouco vago. Isto porque a maioria das ações do sistema é realizada automaticamente através da comunicação de eventos entre os sistemas de segurança previstos. Assim, é como se todos os componentes de segurança pudessem agir como potenciais clientes na aplicação. A interface Web também pode ser considerada um cliente do sistema, pois através dela é possível a comunicação com os sistemas de segurança previstos.

5.2 Plataforma de Testes

O ambiente utilizado para a implementação do sistema incluiu as seguintes ferramentas: a plataforma de desenvolvimento Eclipse; o banco de dados MySql e um repositório CVS. Os dois primeiros tinham uma estação de trabalho dotada do sistema operacional Slackware na sua versão mais atual (10.2). Já o repositório CVS estava disponível em uma estação Power Mac G5, habilitada com o sistema operacional OS 10. Como ferramenta adicional para auxilio do desenvolvimento foi utilizado o Apache Ant na sua versão mais recente (1.6.5). Esta última, tem funcionalidade semelhante ao já conhecido "make", mas difere deste em razão de ser baseada em XML, não dependente de sistema operacional, e com muitos recursos adicionais em relação a outras ferramentas de construção (*build tools*).

5.2.1 AirStrike

Dá-se o nome de *AirStrike* a um trabalho de mestrado desenvolvido por um aluno da UFRJ [25] que inicialmente consistia em uma proposta de ponto de acesso com diversas ferramentas de segurança. Ele é baseado em um computador pessoal de baixo poder de processamento com o sistema operacional *OpenBSD*. Várias ferramentas de segurança são instaladas e configuradas para serem executadas nesta estação. Existe o controle de acesso através do *firewall* do próprio sistema operacional (*pf - packet filter*). Através dele níveis de acesso podem ser configurados de maneira dinâmica. Além disso, todo o tráfego entre as estações sem fio do ambiente e o ponto de acesso são encapsuladas utilizando uma VPN. A proposta continha ainda um sistema de autenticação baseado no protocolo SRP (*Secure Remote Password*) [26] e um sistema de Detecção de Desligamento de Estação (uma implementação de um sistema de DPD). Mais informações podem ser obtidas em [27].

A topologia atual do AirStrike pode ser vista com mais detalhes na Figura 5.1. Através dela, é possível notar que o AirStrike passou a atuar como um servidor de segurança para a rede sem fio, atuando como agente centralizador da segurança do ambiente. Explicando melhor este ponto, a versão inicial do AirStrike poderia ser

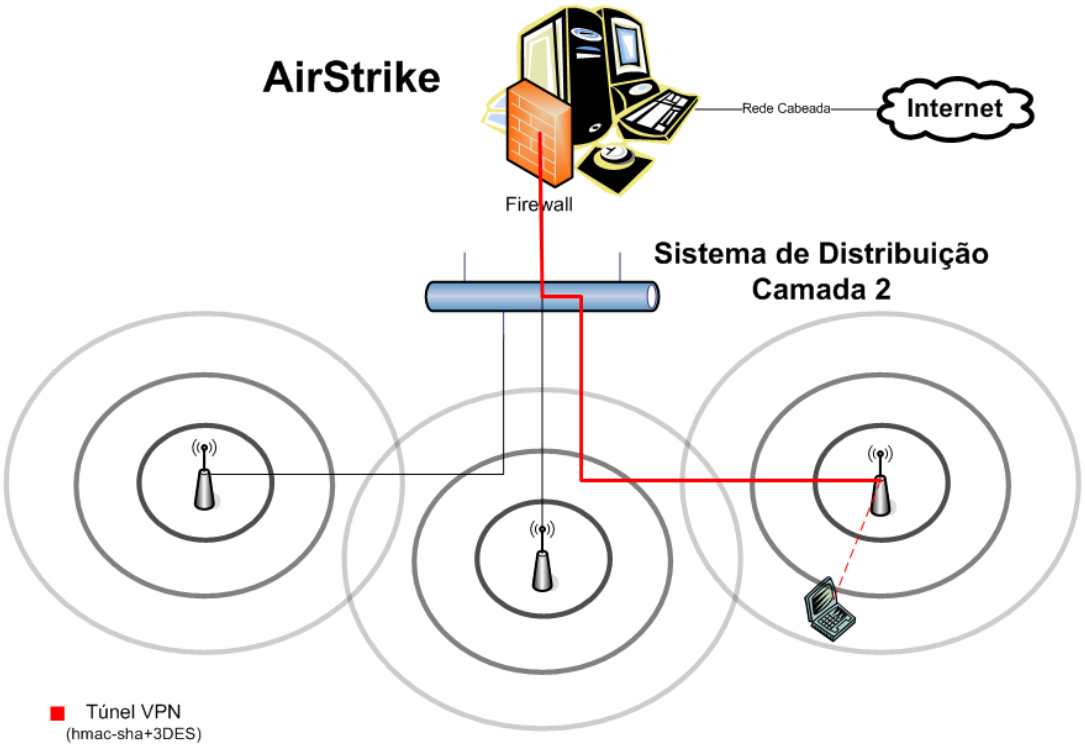

Figura 5.1: Topologia do AirStrike

compreendida como a agregação das camadas de rede e de transporte em um único dispositivo. Assim, ele ao mesmo tempo propiciava acesso à rede sem fio como tratava aspectos da camada três. Já a nova abordagem pode ser vista como a limitação de aplicação do AirStrike à camada três. Assim, o acesso sem fio é delegado a *bridges* comerciais e as aplicações de segurança que executam na camada de rede ficam concentradas do AirStrike. Esta mudança de foco ocorreu para garantir melhorias e um maior nível de aplicabilidade do sistema. Com esta nova abordagem, o AirStrike adaptou-se à utilização de pontos de acesso comerciais, um passo importante na questão de aproveitamento de legado do investimento já realizado. Além disso, o processo de *handoff* seguro de usuários entre os pontos de acesso do ambiente tornou-se possível, dentre outras vantagens.

Resumidamente, o ciclo de estados de um usuário no ambiente é o que segue: após associado com sucesso em um ponto de acesso comercial, é iniciado um processo incremental por parte do filtro de pacotes *pf* que permite apenas o tráfego DHCP (*Dynamic Host Configuration Protocol*) em um primeiro momento. Depois forma-se

um túnel *VPN* entre o servidor e o cliente. O servidor VPN que é executado no *AirStrike* é o *IPSec Isakmpd* [28]. Uma vez estabelecido este túnel a autenticação do cliente pode ser realizada. A versão atual do mecanismo de autenticação é composta por um cliente implementado em Java que utiliza o protocolo SRP.

5.2.2 Utilização de Pontos de Acesso Comerciais

Para os testes sobre o modelo proposto foram utilizados dois pontos de acesso: um *Cisco Aironet 1200* e um *3Com OfficceConnect*.

Obviamente implementar componentes para interagir com Pontos de Acesso não comerciais não é atividade trivial. Isto porque não existe uma API que indique como fazer a implementação de uma nova interface de gerenciamento para o dispositivo. Os fabricantes, em sua maioria, limitam-se a fornecer as interfaces de gerenciamento disponíveis com os respectivos manuais.

As operações implementadas para interagir com estes dispositivos foram as que tinham relativo impacto na segurança do ambiente. Assim, operações relacionadas às tabelas de filtro de endereços MAC, criptografia WEP e WPA, chaves de criptografia foram implementadas para ambos os pontos de acesso.

Para o caso do ponto de acesso 3Com foi implementado um cliente que utiliza o protocolo HTTP para gerenciar o dispositivo. Para atingir o objetivo foi necessário realizar um tipo de engenharia reversa. Foram analisados os formulários das páginas HTML de gerenciamento dos respectivos equipamentos e identificados os nomes dos campos e respectivas URLs para submissão das informações. De posse destas informações, o módulo implementado pode alterar as configurações destes dispositivos. A maneira para se atingir este objetivo foi fazer com que o programa Java que iria gerir este dispositivo conseguisse usar o protocolo HTTP para a comunicação. Assim, o programa abre uma conexão HTTP com o dispositivo e realiza a autenticação. Uma vez autenticado, ele envia requisições do tipo POST com os nomes dos campos que foram previamente identificados com os respectivos valores. Desta forma, o ponto de acesso comporta-se como se estivesse sendo acessado pela

sua interface Web, devidamente autenticado. Isso demonstra a viabilidade de se poder gerenciar uma rede heterogênea com grande diversidade de pontos de acesso diversos, bastando para isso a correta implementação dos dispositivos em questão.

No caso do ponto de acesso Cisco, o acesso via HTTP mostrou-se inviável devido à presença de *javascript* nas páginas HTML do dispositivo. Neste caso, foi encontrada uma solução alternativa: interagir com o mesmo utilizando uma conexão SSH. Neste caso, uma sessão é devidamente aberta e autenticada. Mas ao contrário do envio de métodos para o ponto de acesso como foi feito com a utilização do HTTP, neste caso foi necessário identificar quais séries de comandos deviam ser aplicados para que se atingisse o mesmo comportamento observado quando as configurações deste equipamento eram feitas com a utilização da interface web. Após um primeiro momento que apresentou um maior grau de dificuldade em relação ao gerenciamento através do HTTP, esta abordagem também se mostrou viável, bastando para sua ampla utilização a identificação dos comandos a serem aplicados na sessão SSH.

Outro método para acessar dispositivos poderia ser a utilização de telnet. Embora os equipamentos mais modernos disponham de pelo menos uma das interfaces acima descritas, talvez fosse desejável um módulo do sistema capaz de acessar pontos de acesso comerciais utilizando este protocolo para permitir o gerenciamento do maior número possível de modelos e fabricantes. Mas mesmo com a ausência de telnet, acredita-se ter chegado a um ponto onde virtualmente qualquer ponto de acesso pode ser gerenciado remotamente, seja através de HTTP, seja através de SSH, mesmo que seja necessário realizar ajustes ou novas implementações para outros fabricantes e modelos, onde o sistema proposto seria capaz de gerenciar ambientes heterogêneos, bastando para isto a utilização do componente correto.

5.2.3 Integração entre as Ferramentas

Como já visto anteriormente, vários são os módulos de segurança que podem estar presentes em um ambiente sem fio. Devido a isto, os relacionamentos entre estas ferramentas de segurança podem variar de um ambiente para outro. No estudo de

caso apresentado aqui, foram identificadas algumas relações que foram implementadas para fins de testes. A metodologia para verificação que os sistemas de segurança estavam funcionando corretamente com os respectivos relacionamentos foi a geração manual de eventos no sistema e verificação posterior se os sistemas relacionados haviam sido invocados e realizados suas atividades. A seguir, uma breve descrição dos relacionamentos entre os sistemas de segurança identificados.

O sistema de gerenciamento de usuários tem dois interessados principais nas informações de cadastro e remoção de usuários: o sistema de *handoff* e o sistema de alarmes. Ambos os casos foram implementados. No caso do *handoff*, ao cadastrar um usuário, deve ser informado que pontos de acesso e clientes sem fio o usuário está autorizado a utilizar. Partindo deste aspecto, as configurações dos pontos de acesso comerciais são alteradas para permitir que o usuário possa se associar e fazer *handoff* com os seus dispositivos cadastrados. Já um protótipo do sistema de alarmes foi configurado para enviar um e-mail para o administrador informando para alertá-lo da operação realizada.

O sistema de autenticação de usuários tem também dois interessados: o sistema de *firewall* e o sistema de alarmes. Após um usuário ser autenticado com sucesso no sistema, o serviço de *firewall* é informado e altera dinamicamente suas regras para que este usuário possa ter acesso aos recursos da rede. A situação inversa também ocorre, com a remoção da regra que libera acesso a este usuário. Em ambos os casos, o endereço IP da estação que o usuário está utilizando está disponível encapsulado no objeto "Event". Já o sistema de alarmes, ao contrário do caso anterior onde um e-mail é enviado ao administrador do sistema, simplesmente realiza uma operação de log para arquivar estas operações.

Outro ponto bastante interessante a ser colocado é a integração entre o sistema de localização e o sistema de alarmes. Neste caso, foi implementada uma classe que constantemente monitorassem o posicionamento estimado dos pontos de acesso. Caso haja uma diferença significativa da posição estimada em relação a posição cadastrada previamente, o sistema de localização informa ao sistema de alarmes. Este por sua vez envia um e-mail para o administrador relatando o fato ocorrido.

Outra integração implementada foi entre os sistemas de DPD e *firewall*. A comunicação entre os clientes autenticados e o servidor de DPD é monitorada. Quando ocorre uma falha de alguma natureza nesta comunicação é indício que o cliente foi desligado, ou afastou-se da área de cobertura, por exemplo. Nestes casos, ações como o bloqueio do endereço IP do cliente do *firewall* é uma ação que coíbe ataques de roubo de sessão.

Embora não tenham sido implementados, outros relacionamentos podem ser identificados com o ambiente disposto como aqui apresentado. Uma possibilidade seria a integração do comportamento das ferramentas de WDS com o *firewall*. Ao habilitar/desabilitar o mecanismo de WDS em pontos de acesso, talvez fossem necessárias algumas alterações nas regras de *firewall*. Exemplo similar pode ser aplicado ao servidor VPN: ao desabilitar o gateway VPN, um possível comportamento do *firewall* da rede seria liberar o tráfego não criptografado que antes seria bloqueado.

O sistema de alarmes como um todo, associado à monitoração das configurações e estado dos equipamentos da rede, também é fonte de relacionamentos possíveis no ambiente. Para tal, bastaria que fossem implementadas classes que monitorasse a configuração em execução dos equipamentos e a confrontasse com configurações válidas previamente cadastradas em um banco de dados, a exemplo do que foi feito com o sistema de alarmes de localização. Assim, alterações nas configurações ou estado dos equipamentos podem disparar alarmes no sistema indicando alterações indevidas.

Outro ponto com grande potencial de integração é quando disponível no ambiente um sistema de detecção de intrusão, pois várias ações poderiam ser tomadas após a confirmação de alguma tentativa de ataque. Além do tradicional alarme, o *firewall* poderia ser acionado para tentar conter o invasor, ou em um outro exemplo, onde este sistema de gerenciamento estaria integrado com uma plataforma mais abrangente, ocorrer a desativação de uma porta de um *switch* com o mesmo fim.

A variedade de relacionamentos entre os sistemas de segurança previstos no ambiente indica o potencial que o sistema de integração propicia ao gerenciamento de segurança do ambiente e a validade do mecanismo proposto para o fim especificado.

Estes foram apenas alguns relacionamentos aqui identificados neste caso específico. Outros mais podem também existir e apenas não foram identificados até então.

5.2.4 Desempenho do Sistema

Foram realizadas algumas medições de desempenho de algumas atividades do sistema. Não foi possível encontrar outras soluções para que pudesse ter sido realizada uma comparação, visto que estas não dispunham de um mecanismo de integração, como proposto neste trabalho. Para tais testes foi montado o seguinte ambiente:

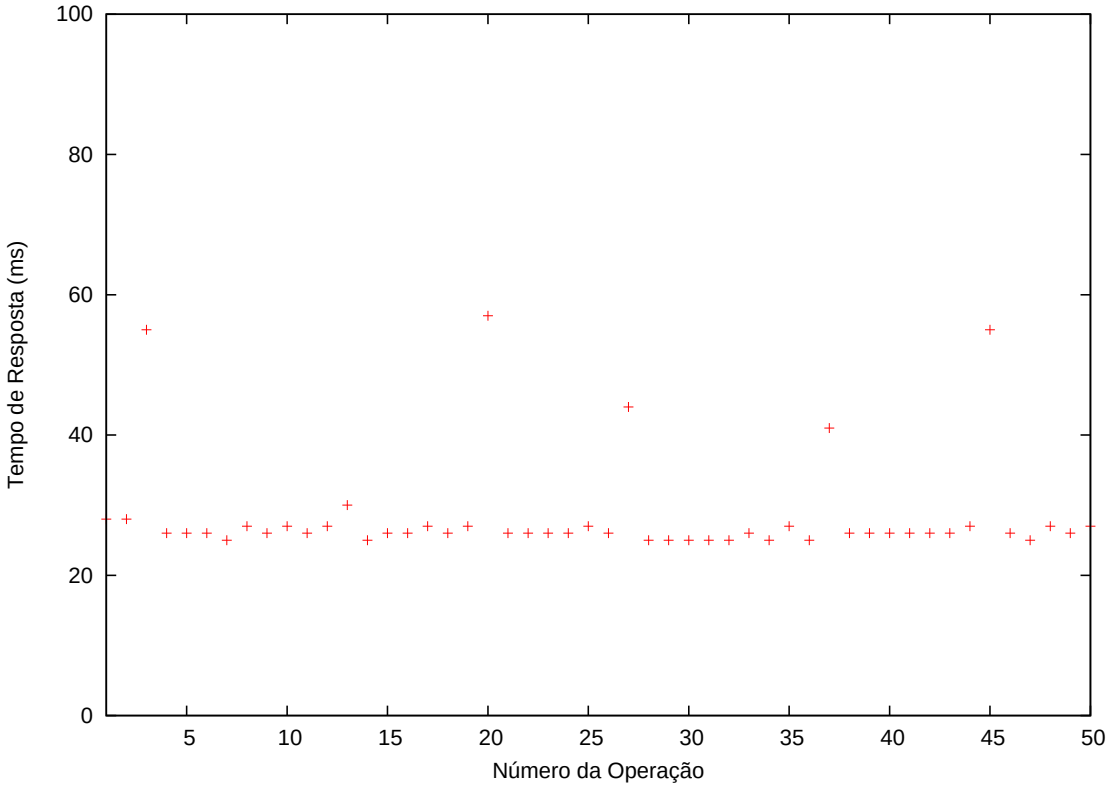

Figura 5.2: Tempo para realizar *lookup* de um objeto no Serv. de Nomes

- Uma estação de gerenciamento;
- Uma estação executando o AirStrike (*firewall* e VPN).
- Uma estação cliente do administrador;
- Dois pontos de acesso comerciais;

A estação de gerenciamento e a estação cliente do administrador consistiam em Desktops Dell Dimension 3000, Pentium IV HT 3.0 GHz, 512MB RAM com 40 GB de HD. Estas estações estavam equipadas com o sistema operacional Slackware na versão *current* e com Kernel compilado na versão 2.6.13.4 SMP.

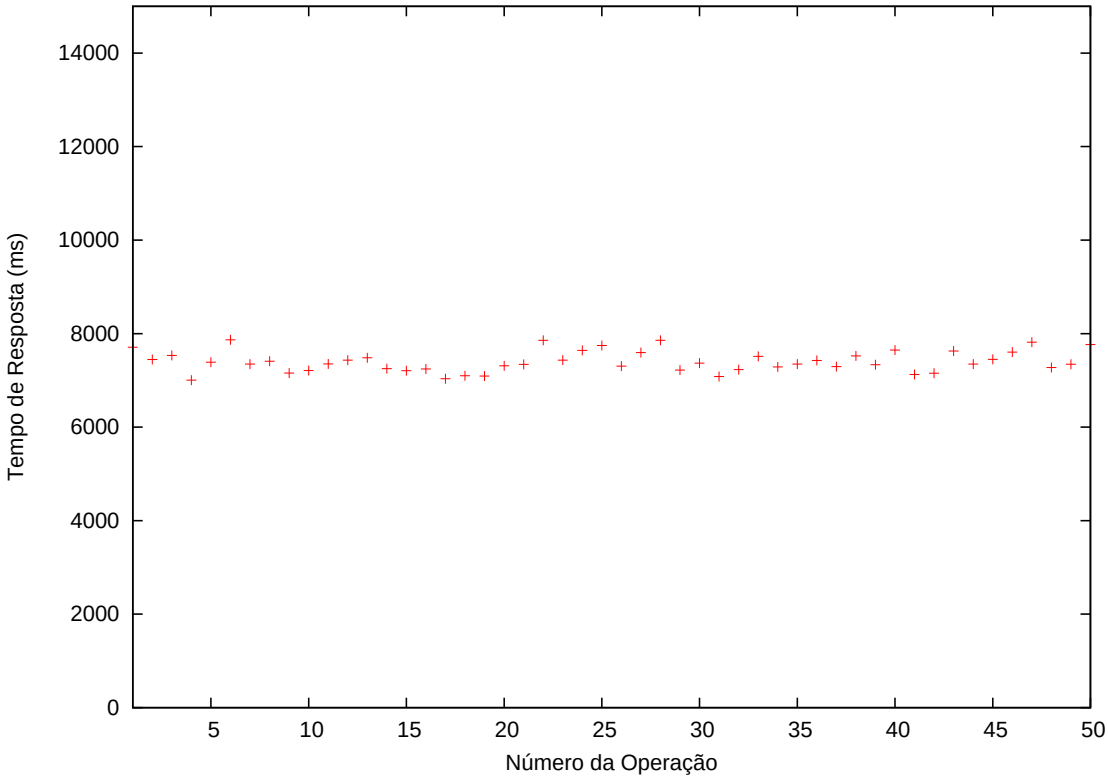

Figura 5.3: Tempo para adicionar usuário com 1 dispositivo cliente no PA Cisco

Já a estação executando o AirStrike consistia de um PC Pentium III 700 MHz, 128 MB RAM com 15 GB de HD. Esta, por sua vez, estava executando o Sistema Operacional *OpenBSD* na versão 3.8. No caso desta estação, devido a ausência de uma distribuição de Java para esta plataforma, foi necessário ativar uma emulação de Linux no sistema, baixar e compilar um pacote de Java para ser instalado no ambiente.

Os experimentos foram realizados em horário normal de expediente, onde variações de tráfego e utilização da rede não estavam sob controle. Foi feita esta opção para prover resultados que retratassem melhor o ambiente onde o servidor de gerenciamento deverá ser colocado em uso.

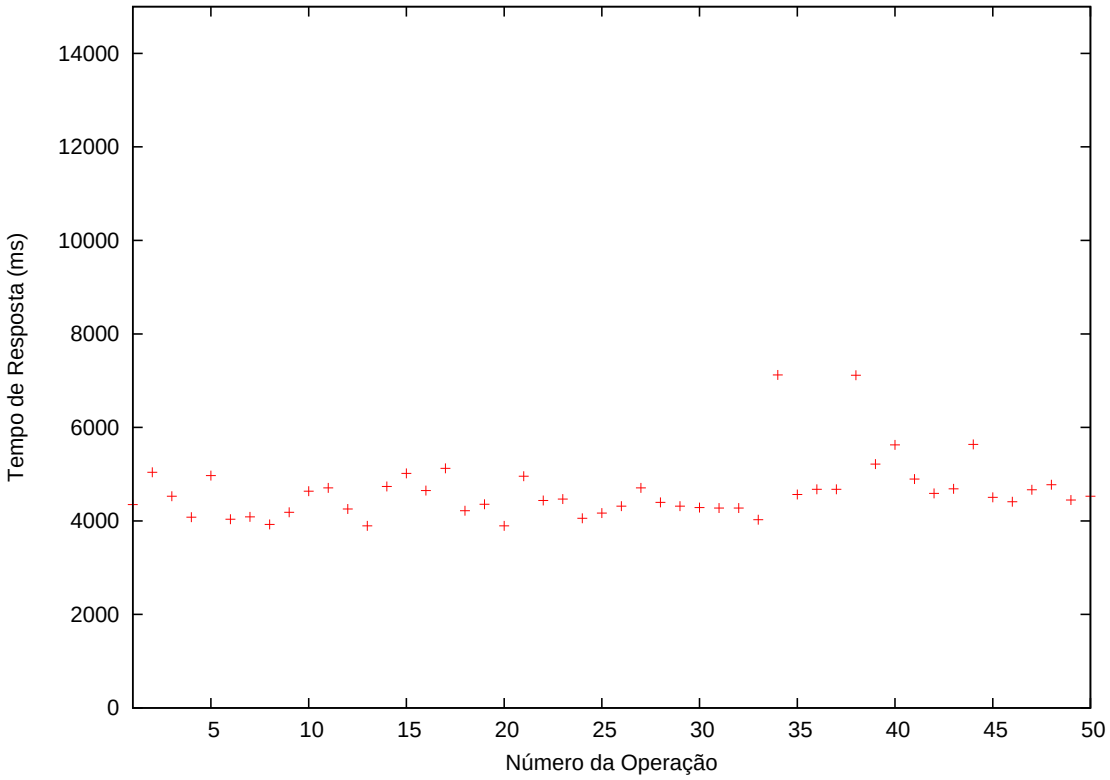

Figura 5.4: Tempo para adicionar usuário com 1 dispositivo cliente no PA 3Com

Na Figura 5.2 é mostrado o tempo decorrido da operação de *lookup* de um objeto no servidor de nomes a partir da estação cliente utilizada pelo administrador. Neste caso, foi feita esta operação para buscar a referência para o servidor de gerenciamento de usuários. Foram feitas cinqüenta operações deste tipo e pode ser observado pela Figura que os tempos para obtenção destas referências é consideravelmente baixo, na ordem de poucos milisegundos, não sendo o seu impacto decisivo para o desempenho do sistema como um todo.

Já a Figura 5.3 mostra uma operação mais complexa. O tempo que decorre para o administrador adicionar um usuário no sistema. Vale aqui lembrar que este tempo não é apenas para adicionar o usuário na base de dados do sistema, mas também de realizar as operações de integração conforme descritas na subseção 5.2.3, com exceção do envio de e-mail para o administrador.

Aqui vale a pena fazer uma suposição interessante: dado que exista um administrador em tempo integral verificando o estado do sistema, quanto tempo ele levaria

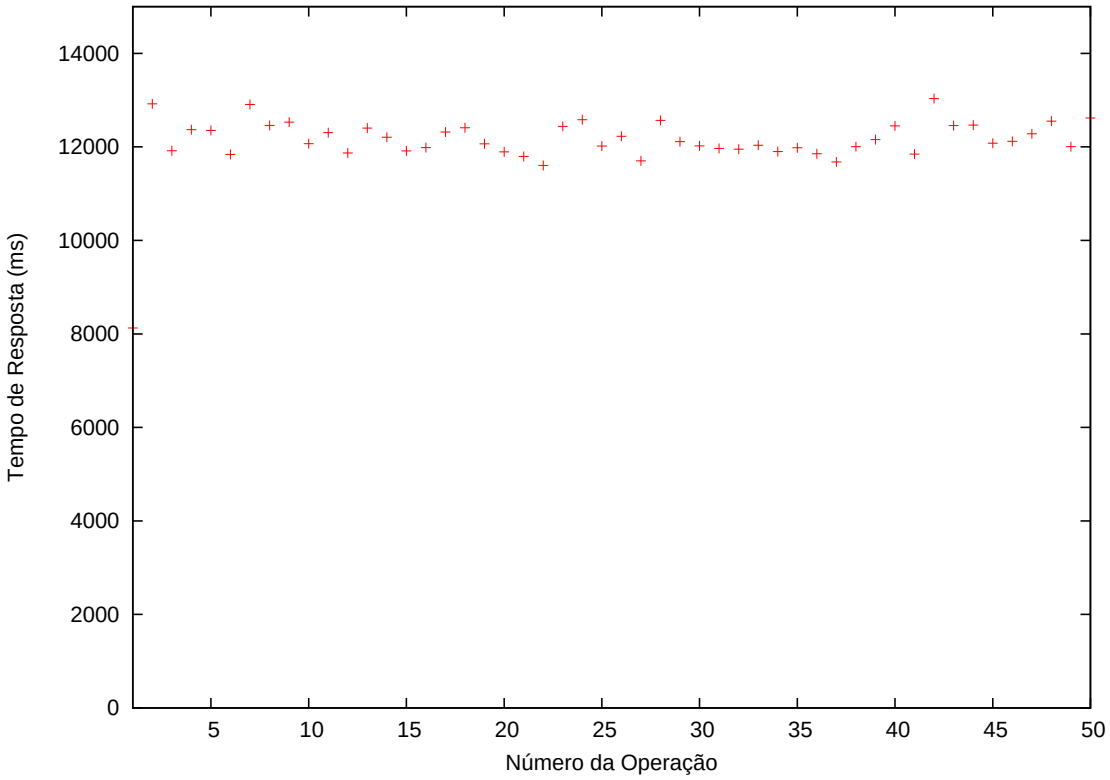

Figura 5.5: Tempo para adicionar usuário com 1 dispositivo cliente em 2 PAs

para realizar a mesma operação que foi feita automaticamente pelo sistema de gerenciamento? Testes realizados no laboratório indicaram um tempo de cerca de 30 segundos para fazer a autenticação na página do dispositivo, acessar os menus corretos, adicionar um endereço MAC (no exemplo realizado, um endereço fictício de 11:11:11:11:11:11) e salvar as alterações. Isto com o usuário que realizou o teste bastante familiarizado com a interface web do dispositivo.

Na Figura 5.4 temos os tempos da realização da mesma tarefa quando o ponto de acesso que o usuário tem permissão de usar é o 3Com. Como pode ser observado nesta figura, o tempo decorrido para a realização da mesma atividade foi menor do que com o ponto de acesso Cisco. Isto se deve basicamente às diferenças de implementação nos programas que interagem com estes dispositivos. A maneira de lidar com a tabela de MACs do equipamento Cisco é um pouco mais complicada do que com o 3Com. Além disso, é válido lembrar que os dois têm diferenças quanto ao modo de acesso utilizado. Para o Cisco foi utilizado acesso SSH e para o 3Com foi utilizado acesso via conexão HTTP. É válido ressaltar aqui também o

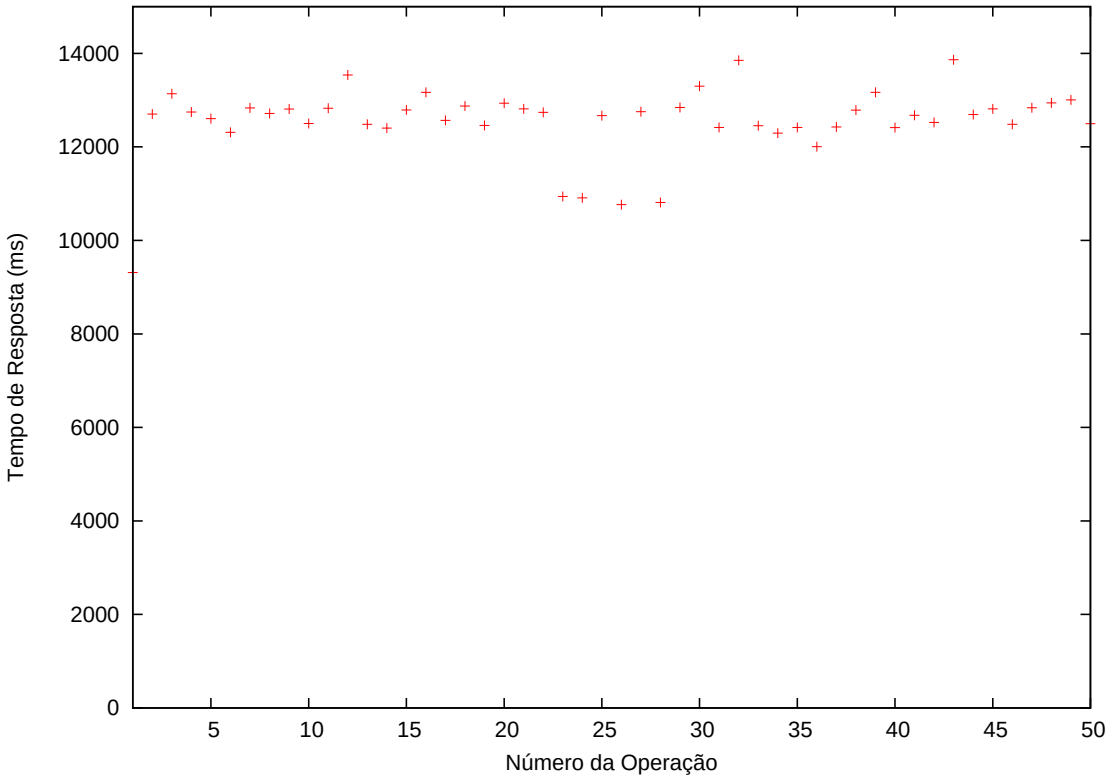

Figura 5.6: Tempo para adicionar usuário com 5 dispositivos clientes em 2 PAs

paralelo semelhante a suposição feita em relação a situação anterior. Novamente um administrador leva em todo de trinta segundos para adicionar um endereço MAC na tabela deste equipamento.

As Figuras 5.5 e 5.6 mostram os tempos quando um usuário que tem permissão de usar um e cinco clientes, respectivamente com dois pontos de acesso comerciais do ambiente é adicionado. Os tempos aqui apresentados, como eram de se esperar são maiores que os apresentados até então. Embora eles possam parecer elevados em uma primeira análise, vale lembrar que uma comparação mais justa deveria colocar estes tempos com os de acessar a interface web de dois pontos de acesso, realizar a autenticação e adicionar o referido endereço MAC. Outro ponto que deve ser ressaltado é que em nenhum momento o código destas funcionalidades foi otimizado. Este aspecto poderia significar uma melhora nos desempenhos dos gráficos apresentados. Além disso, deve se imaginar um passo além: o administrador como pessoa terá suas ações limitadas a medida que o número de dispositivos que o cliente está apto a utilizar e o número de pontos de acesso que ele tem permissão de acessar

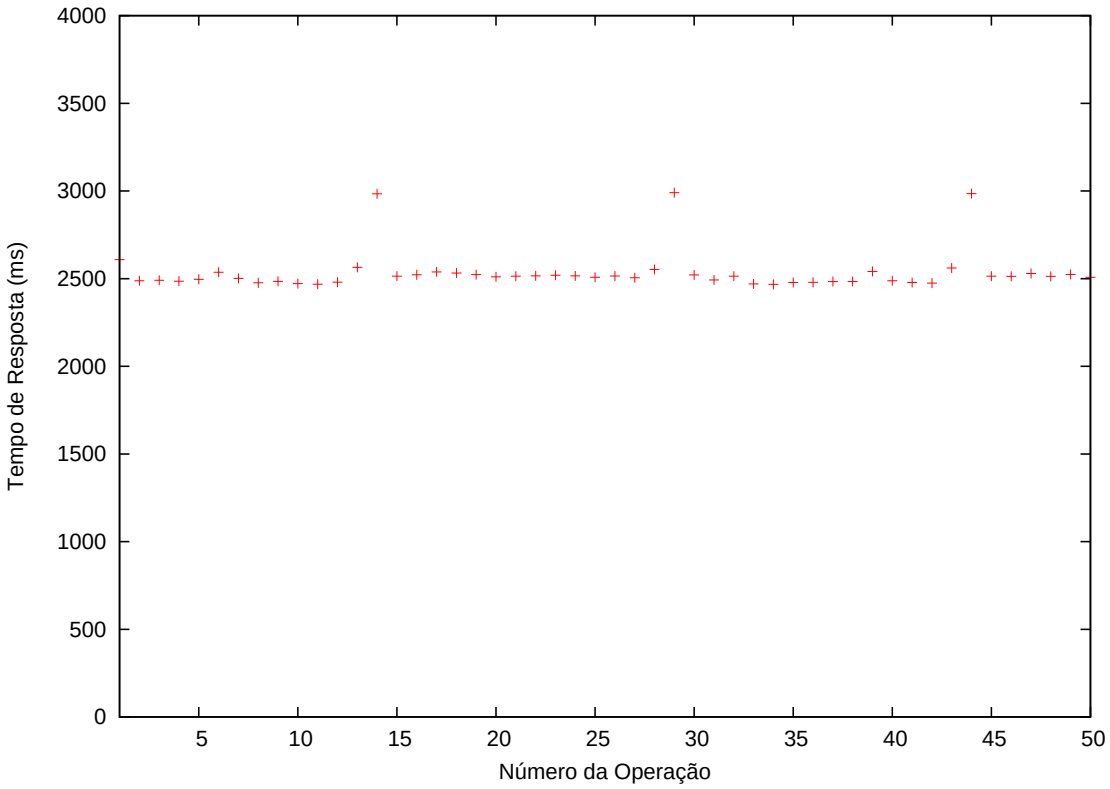

Figura 5.7: Tempo para autenticar usuário

crescem. Torna-se uma atividade não humana gerir este tipo de funcionalidade em larga escala, sendo esta mais uma justificativa para a automação destas tarefas.

A Figura 5.7 mostra os tempos do procedimento de autenticação de um usuário no sistema. Neste tempo intervalo de tempo deve ser levado em consideração o tempo a inclusão do endereço IP do cliente no *firewall* e o sistema de alarmes ser informado. É importante ressaltar que uma parcela deste tempo é devido ao próprio protocolo SRP utilizado para este fim.

Um ponto importante a ser ressaltado aqui é a análise de desempenho das operações que foram realizadas. Como mensurar se o desempenho encontrado pode ser considerado satisfatório? Aqui encontra-se uma dificuldade de análise objetiva comparativa com outras soluções, pois em nenhuma outra ferramenta existe o princípio da integração entre os sistemas de segurança. Esta integração invariavelmente leva a um incremento no tempo em que as operações são realizadas. No entanto, este aumento deve ser comparado caso não existisse o mecanismo de integração, ou

seja, caso fosse necessário alterar individualmente todos os sistemas de segurança envolvidos.

Como exemplo pode ser dito que o desempenho do sistema para adição de usuários com um tempo que, nos experimentos, variou de aproximadamente oito a doze segundos, dependendo dos parâmetros pode ser considerado bom. Esta conclusão é obtida se os dados forem confrontados com o tempo necessário para adicionar um usuário manualmente e realizar todas as operações que aqui são realizadas de maneira automática. Outro bom exemplo a ser considerado é o tempo para realização da autenticação de um usuário, que levou aproximadamente dois segundos. Este tempo, que em princípio poderia ser considerado muito longo, leva em conta todo o atraso da autenticação propriamente dita, como alteração de regras de firewall e notificação pelo sistema de alarmes, como já dito anteriormente.

5.2.5 Resultados Obtidos

A Tabela 5.1 resume um comparativo entre as principais características levantadas a respeito das ferramentas comerciais de gerenciamento de redes sem fio. É possível observar que, apesar de a solução proposta não contar com um sistema de monitoração do espectro de radiofreqüência que pode ser facilmente incluído, ela conta com o aspecto de integração entre os mecanismos de segurança do ambiente. Esta característica faz da solução proposta uma boa alternativa às soluções comerciais, pois uma idéia simples para resolver um problema interessante mostrou-se factível de ser implementada.

Na Tabela 5.2 é possível observar as métricas estabelecidas no Capítulo 3 com respectivas avaliações. Como já dito anteriormente, o objetivo deste trabalho era de apresentar um framework para o gerenciamento integrado de segurança em redes sem fio. Neste aspecto, pode-se dizer que o objetivo foi atingido, visto que apenas dois sistemas de segurança não tenham sido implementados no ambiente de testes. O sistema de WDS não foi implementado pois só havia um ponto de acesso no cenário de testes que dispunha de tal funcionalidade. O sistema de IDS não foi

	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
Proposta	OK	X	OK	X	OK	OK

Tabela 5.1: Resumo das características das ferramentas comerciais disponíveis para redes sem fio comparadas com a solução proposta

implementado pois não havia no cenário de testes nenhum IDS disponível para realização de testes. É valido ressaltar que embora estes sistemas não tenham sido implementados, a especificação das suas interfaces está muito bem definida, fazendo com que num momento futuro, caso componentes para estes sistemas de segurança venham a ser desenvolvidos, estes possam facilmente ser integrados ao framework, inclusive, com integração entre os relacionamentos que por ventura ainda não tenham sido identificados neste primeiro momento.

Requisito	Implementado	Métrica de Aceitação	OK
A solução deve contar com a utilização de sistemas de segurança que comumente são encontrados nas redes sem fio	Firewall	Implementado	OK
	VPN	Implementado	OK
	Alarmes	Implementado	OK
	Sistema de Autenticação	Implementado	OK
	IDS	Implementado	Não
Deve contar com a utilização de sistemas ligados a segurança que usualmente exclusivos de ambientes sem fio	Localização	Implementado	OK
	Handoff	Implementado	OK
	DPD	Implementado	OK
	WDS	Implementado	Não
Permitir a integração entre os sistemas de segurança do ambiente;	-	Padrão *Observer* permite esta característica	OK
Genérica	-	Especificação das funcionalidades dos sistemas de segurança não restritas à ferramentas específicas	OK
Escalável	-	Topologia baseada em clusters	OK
Flexível	-	Ações a serem tomadas de acordo com os eventos que ocorram no sistema podem ser alteradas e o funcionamento dos componentes não necessita ser alterado	OK

Tabela 5.2: Resumo dos requisitos, métricas de avaliação e cumprimento dos requisitos estabelecidos

Capítulo 6

Conclusão e trabalhos futuros

6.1 Conclusões

O uso de redes sem fio domésticas e empresariais vêm se expandido de forma bastante acentuada no decorrer dos últimos anos. Juntamente com este aumento na utilização surgiram diversas questões relacionadas à segurança neste tipo de rede. Neste aspecto, foi visto que os padrões de segurança propostos pelo IEEE são por muitas vezes falhos, o que leva a adoção e utilização de ferramentas de segurança auxiliares para aumentar o nível de segurança da rede. Foi visto também que os estudos acadêmicos e ferramentas comerciais possuem diversas lacunas no que diz respeito ao gerenciamento de segurança para este tipo de rede.

Neste contexto, neste trabalho foi apresentada a proposta de um *framework* para gerenciamento integrado de segurança para redes sem fio. Foi feita uma análise crítica das soluções disponíveis de gerenciamento de segurança para este tipo de rede.

Foi mostrado que as soluções disponíveis têm diversas lacunas que necessitam ser preenchidas, mostrando que esta é sim uma área promissora de pesquisa e desenvolvimento. Dentre estas lacunas podem ser destacadas as falhas de segurança já identificadas nos padrões, o que leva à adoção de várias ferramentas de segurança adicionais para tornar o ambiente sem fio mais confiável. Neste ponto, as configura-

ções destas ferramentas adicionais não são feitas de maneira integrada com outras ferramentas existentes no ambiente. Com base nisso, um *framework* para gerenciamento de segurança em redes sem fio foi proposto, especificado e implementado, com uma arquitetura projetada buscando ser o mais escalável e adaptável possível, permitindo que alterações possam ser feitas posteriormente ao ambiente sem que maiores problemas sejam enfrentados.

Neste sentido, foi desenvolvido um *framework* para o gerenciamento integrado do sistema de maneira distribuída. Este sistema tem como base o protocolo IIOP, que serve de base de comunicação para sistemas distribuídos que utilizam o paradigma de orientação a objetos. Além deste protocolo base, vários outros são usados no sistema, para possibilitar a comunicação entre as partes presentes no sistema. Uma API utilizando o formalismo UML foi especificada no intuito de ser um passo anterior ao desenvolvimento de um software piloto. Nesta API foram especificados os principais métodos para interagir com os equipamentos e ferramentas de segurança da rede.

Posteriormente, um protótipo foi implementado utilizando a linguagem de programação Java. Este protótipo contou com um subconjunto das funcionalidades especificadas na API, pois seu intuito era o de validar a solução proposta. Neste sentido, foram integradas as operações sobre sistema de gerenciamento de usuários, gerenciamento de autenticação, permissões de handoff, regras de *firewall*, configurações de VPN, sistema de localização, sistema de alarmes e de DPD. O mecanismo de integração entre as ferramentas de segurança foi testado exaustivamente, onde várias situações que demandavam a integração ocorreram e a comunicação entre as partes se mostrou eficaz, mesmo quando alterações não realizadas pelo administrador ocorriam e eram percebidas pelos próprios programas, que comunicavam a alteração de estado aos interessados na informação.

Atingiu-se o objetivo proposto inicialmente, pois as mudanças que ocorriam em determinadas configurações das ferramentas presentes no ambiente de testes foram automaticamente propagadas para as ferramentas cadastradas como correlatas. Este comportamento é altamente desejável, visto que automatiza as configurações das ferramentas de segurança do ambiente e o torna menos suscetível a inconsistências

que o fator humano pode incluir.

6.2 Trabalhos Futuros

Como trabalhos futuros poderiam ser colocados a implementação do framework em um ambiente que contasse com todos os mecanismos de segurança previstos, com um grande número de pontos de acesso. Assim, seria posto a prova todo o seu potencial de gerenciamento em um ambiente de grande porte. Além disso, seria extremamente interessante o desenvolvimento de outros programas para ferramentas de segurança similares. É o caso, por exemplo, do *firewall*. Embora esteja disponível a implementação para ser utilizada com o pf, do sistema operacional *OpenBSD*, seria muito interessante a implementação de outros programas para interagir com outras versões de ferramentas de segurança que podem ser encontradas em um ambiente diverso.

Seria também interessante preparar um ambiente onde estivessem disponíveis outros mecanismos de segurança que não estavam presentes no ambiente implementado, tais como o WDS e o IDS. Assim, atingir-se-ia uma solução mais completa em um ambiente de produção, para que a partir daí, novos testes pudessem ser realizados ou novos relacionamentos entre as ferramentas de segurança identificados.

Outro ponto interessante a ser colocado é o desenvolvimento de aplicações para o gerenciamento de outros pontos de acesso comerciais e testes para verificar a compatibilidade dos clientes já desenvolvidos com versões similares dos mesmos fabricantes. Desta forma, o ambiente poderia ser mais facilmente implementado em um ambiente de testes real, onde a heterogeneidade é quase sempre característica presente. Desta forma, uma maior maturidade do sistema poderia ser atingida, onde estariam disponíveis diversos componentes distintos para os mais variados ambientes, reduzindo o esforço de implementação a partir do reuso do código já implementado. Além disso, a API poderia ser consideravelmente melhorada com contribuições de terceiros a medida que fossem sendo identificadas lacunas não cobertas por este trabalho inicial.

Pode-se pensar também que este framework pode ser considerado um passo inicial para um sistema de gerenciamento mais completo, onde todo o controle da infra-estrutura da rede sem fio poderia ser de sua responsabilidade. Para isto, algumas de suas funcionalidades poderiam ser revistas, no sentido de torná-lo adequado para esta nova atribuição. Neste aspecto, o framework poderia controlar desde versões de firmware para equipamentos na rede, até a adoção de políticas de segurança pré-definidas, onde estas políticas teriam ligação direta com os relacionamentos entre os sistemas de segurança do ambiente.

Outro ponto que merece destaque é o estudo da viabilidade do modelo apresentado neste trabalho, com as devidas alterações e melhorias, ser utilizado para o gerenciamento de segurança integrado de redes *mesh*. As pesquisas neste tipo de rede tem se mostrado muito produtivas nos últimos anos, e as características que foram perseguidas neste trabalho se aplicam a um ambiente com estas características.

Bibliografia

[1] ANSI/IEEE Std, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," http://standards.ieee.org/wireless/, 2003.

[2] C. Maple, H. Jacobs, and M. Reeve, "Choosing the Right Wireless LAN Security Protocol for the Home and Business User," in *ARES '06: Proceedings of The First International Conference on Availability, Reliability and Security*. IEEE Computer Society, 2006, pp. 1025–1032.

[3] W. A. Arbaugh, N. Shankar, and Y. C. J. Wan, "Your 80211 wireless network has no clothes," *IEEE Wireless Communications*, vol. 9, pp. 44–51, dec 2002.

[4] J. R. Walker, "IEEE P802.11 wireless LANs: Unsafe at any key size; an analysis of the wep encapsulation," IEEE, Tech. Rep. IEEE 802.11-00/362, October 2000.

[5] T. D. Wu, "A real-world analysis of kerberos password security." in *NDSS*. The Internet Society, 1999. [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/99/proceedings/papers/wu.pdf, visitada em 22/10/2006

[6] W. A. Arbaugh and A. Mishra, "An initial security analysis of the IEEE 802.1x standard," http://www.cs.umd.edu/ waa/1x.pdf visitada em 22/10/2006, 2002.

[7] M. Shin, J. Ma, A. Mishra, and W. A. Arbaugh, "Wireless network security and interworking," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 455–466, Feb. 2006. [Online]. Available: http://ieeexplore.ieee.org/iel5/5/33381/01580513.pdf, visitada em 22/10/2006

[8] C. He and J. C. Mitchell, "Analysis of the 802.11i 4-way handshake," in *WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security.* New York, NY, USA: ACM Press, 2004, pp. 43–50.

[9] K. J. Hole, E. Dyrnes, and P. Thorsheim, "Securing Wi-Fi Networks," *IEEE Computer*, vol. 38, no. 7, pp. 28–34, 2005.

[10] H. Feil, "802.11 Wireless Network Policy Recommendation for Usage Within Unclassified Government Networks," *IEEE Military Communications Conference*, vol. 2, no. 7, pp. 832–838, October 2003.

[11] D. Welch and S. Lathrop, "Wireless Security Threat Taxonomy," *Proceedings of the 2003 IEEE Workshop on Information Assurance*, pp. 76–83, June 2003.

[12] F. K. L. Chan, A. H. Hoon, and B. Isaac, "Analysis of IEEE 802.11b Wireless Security for University Wireless LAN Design," *IEEE International Conference on Networks*, vol. 2, pp. 1137–1142, November 2005.

[13] C. Vrije, "Simple network management protocol (snmp) - current standards and status," http://www.iihe.ac.be/internal-report/1998/stc-98-06.ps, visitada em 22/10/2006, 1998.

[14] Y.-C. Shim, "Developing a managed system in the osi network management," in *SAC '96: Proceedings of the 1996 ACM symposium on Applied Computing.* New York, NY, USA: ACM Press, 1996, pp. 88–92.

[15] H. M. Faheem, "Multiagent-based security for the wireless LAN," *IEEE Potentials*, vol. 24, no. 2, pp. 19–22, may 2005.

[16] J. W. Branch, N. L. Petroni Junior, L. V. Doorn, and D. Safford, "Autonomic 802.11 Wireless LAN Security Auditing," *IEEE Security & Privacy Magazine*, vol. 2, pp. 56–65, may 2004.

[17] G. Corral, X. Cadenas, A. Zaballos, and M. T. Cadenas, "A Distributed Vulnerability Detection System for WLANs," in *WICON '05: Proceedings of the 1st International Conference on Wireless Internet.* IEEE Computer Society, 2005, pp. 86–93.

[18] Aruba, "Aruba Networks," http://www.arubanetworks.com, visitada em 22/10/2006, 2005.

[19] AirWave, "AirWave Wireless," http://www.airwave.com/, visitada em 22/10/2006, 2005.

[20] AirDefense, http://www.airdefense.net, visitada em 22/10/2006, 2005.

[21] B. A. A. Nunes, "Um Mecanismo Seguro de Autenticação Mútua com Detecção de Desconexão e Gerenciamento Dinâmico de Regras de Firewall," *Projeto Final de Curso, Departamento de Engenharia Eletrônica e Computação - DEL/UFRJ*, 2004.

[22] OMG, "Common Object Request Broker Architecture: Core Specification," http://www.omg.org/cgi-bin/apps/doc?formal/04-03-01.pdf, visitada em 22/10/2006, mar 2004.

[23] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, *Design patterns: elements of reusable object-oriented software*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1995.

[24] C. E. Calabrez, "Uma comparação entre diversas tecnologias de comunicação de objetos distribuídos em java," Master's thesis, Universidade Estadual de Campinas, Feb 2004.

[25] D. de Souza Diaz Carrión, "Implementação de um ponto de acesso seguro para redes 802.11b baseado no sistema operacional OpenBSD," *Simpósio Brasileiro de Redes de Computadores*, apr 2003.

[26] T. J. Wu, "The secure remote password protocol," *Proceedings of the 1998 Internet Society Symposium on Network and Distributed System Security*, pp. 97–111, mar 1998.

[27] AirStrike, "AirStrike Project," http://airstrike.ravel.ufrj.br, visitada em 22/10/2006, 2005.

[28] D. Maughan, M. Schertler, M. Schneider, and J. Turner, "Internet security association and key management protocol (isakmp)," *IETF RFC 2408*, nov 1998.