UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE ENGENHARIA
CAMPUS DE ILHA SOLTEIRA

NELCILENO VIRGÍLIO DE SOUZA ARAÚJO

KAPPA-PSO-ARTMAP FUZZY: UMA METODOLOGIA PARA DETECÇÃO DE INTRUSOS BASEADO EM SELEÇÃO DE ATRIBUTOS E OTIMIZAÇÃO DE PARÂMETROS NUMA REDE NEURAL ARTMAP FUZZY.

Ilha Solteira - SP

Junho/2013

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de Ilha Solteira

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

KAPPA-PSO-ARTMAP FUZZY: UMA METODOLOGIA PARA DETECÇÃO DE INTRUSOS BASEADO EM SELEÇÃO DE ATRIBUTOS E OTIMIZAÇÃO DE PARÂMETROS NUMA REDE NEURAL ARTMAP FUZZY.

NELCILENO VIRGÍLIO DE SOUZA ARAÚJO

Orientador: Prof. Dr. Ailton Akira Shinoda
Co-orientador: Prof. Dr. Ruy de Oliveira

Tese apresentada à Faculdade de Engenharia - UNESP - Campus de Ilha Solteira, para obtenção do título de Doutor em Engenharia Elétrica.
Área de Conhecimento: Automação.

Ilha Solteira - SP
Junho/2013

FICHA CATALOGRÁFICA

Elaborada pela Seção Técnica de Aquisição e Tratamento da Informação
Serviço Técnico de Biblioteca e Documentação da UNESP - Ilha Solteira.

A659k

Araújo, Nelcileno Virgílio de Souza.
Kappa-PSO-ARTMAP Fuzzy : uma metodologia para detecção de intrusos baseado em seleção de atributos e otimização de parâmetros numa rede neural ARTMAP Fuzzy / Nelcileno Virgílio de Souza Araújo. – Ilha Solteira: [s.n.], 2013
110 f. : il.

Tese (doutorado) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de conhecimento: Automação, 2013

Orientador: Ailton Akira Shinoda
Co-orientador: Ruy de Oliveira
Inclui bibliografia

1. Detecção de intrusos. 2. Seleção de atributos. 3. Otimização de parâmetros. 4. Classificação de padrões. 5. Rede neural ARTMAP Fuzzy. 6. Coeficiente Kappa. 7. Otimização por enxame de partículas. 8. Redes cabeadas. 9. Redes infraestruturadas sem fio.

unesp UNIVERSIDADE ESTADUAL PAULISTA
CAMPUS DE ILHA SOLTEIRA
FACULDADE DE ENGENHARIA DE ILHA SOLTEIRA

CERTIFICADO DE APROVAÇÃO

TÍTULO: KAPPA-PSO-ARTMAP FUZZY: UMA METODOLOGIA PARA DETECÇÃO DE INTRUSOS BASEADO EM SELEÇÃO DE ATRIBUTOS E OTIMIZAÇÃO DE PARÂMETROS NUMA REDE NEURAL ARTMAP FUZZY

AUTOR: NELCILENO VIRGILIO DE SOUZA ARAÚJO
ORIENTADOR: Prof. Dr. AILTON AKIRA SHINODA
CO-ORIENTADOR: Prof. Dr. RUY DE OLIVEIRA

Aprovado como parte das exigências para obtenção do Título de DOUTOR EM ENGENHARIA ELÉTRICA, Área: AUTOMAÇÃO, pela Comissão Examinadora:

Prof. Dr. AILTON AKIRA SHINODA
Departamento de Engenharia Elétrica / Faculdade de Engenharia de Ilha Solteira

Profa. Dra. CHRISTIANE MARIE SCHWEITZER
Departamento de Matemática / Faculdade de Engenharia de Ilha Solteira

Profa. Dra. MARA LÚCIA MARTINS LOPES
Departamento de Matemática / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. ANDERSON CASTRO SOARES DE OLIVEIRA
Departamento de Estatística / Universidade Federal de Mato Grosso

Prof. Dr. CARLOS DIAS MACIEL
Departamento de Engenharia Elétrica e Computação / Universidade de São Paulo

Data da realização: 28 de junho de 2013.

Dedico aos meus queridos pais, Nelci Ferreira de Araújo e Terezinha de Souza Araújo, que me educaram e me possibilitaram mais essa conquista.

AGRADECIMENTOS

A Deus e a Nossa Senhora Aparecida por toda força espiritual necessária para viver e ultrapassar os obstáculos existentes neste tipo de conquista.

À Família sempre presente nos momentos mais difíceis e a paciência por aguentar todo o minha ausência neste período.

Ao Professor Dr. Ailton Akira Shinoda, pela compreensão e por ter se mostrado um exemplo de orientador, na elaboração deste trabalho. Agradeço por sua dedicação, seus ensinamentos e por toda sua paciência no desenvolvimento da pesquisa e experimentos.

Ao Professor Dr. Ruy de Oliveira, meu co-orientador, pelas grandes contribuições ocorridas no desenvolvimento desta Tese, as quais foram essenciais para o meu amadurecimento intelectual e pessoal.

Aos Professores Dr. Valtemir Nascimento e Dr. Ed'Wilson Tavares Ferreira pela contribuição de idéias para a execução do meu trabalho.

Aos colegas Douglas Ferrari e Filipe Molina que me ajudaram na implementação dos experimentos para a construção da base de dados de detecção de intrusão.

A minha colega Juliana Fonseca Antunes pela ajuda no entendimento da rede neural ARTMAP *Fuzzy* e como melhor aplicá-la para o problema da minha Tese.

Aos meus amigos Elmha, Constantino, Jonas, Sônia, Anderson, Lia, Eveliny, Josimere, Adriana, Nádia Kunze, Einstein, Maria Eunice, Joelcio e todos aqueles que torcem pela minha vitória.

Aos meus colegas Rothschild Antunes e Lucas Ramalho, do grupo de pesquisa em redes e segurança do IFMT – Campus Cuiabá, pela ajuda profissional para a construção deste trabalho.

Ao professor Rubém, em nome de todos os docentes, discentes e técnico-administrativos do programa de pós-graduação em Engenharia Elétrica, pela ajuda, companheirismo e excelente prestação de serviços oferecida. Com certeza, o meu período vivenciado neste ambiente de pesquisa trouxe-me muitas alegrias.

Ao Instituto de Computação pelo afastamento das minhas atividades para que pudesse executar as tarefas da tese.

A Universidade Federal de Mato Grosso (UFMT) e a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo auxílio financeiro durante o afastamento para o doutorado.

À banca examinadora que analisará o conteúdo deste trabalho contribuindo com sugestões.

RESUMO

Nos últimos anos têm-se percebido um forte crescimento no uso da tecnologia sem fio 802.11 (*Wireless Local Area Network* - WLAN) e os mecanismos de segurança implementados pelas emendas IEEE 802.11i e IEEE 802.11w têm se mostrado pouco eficazes no combate a ataques contra a disponibilidade dos serviços da WLAN. Os sistemas detectores de intrusão surgem como uma forma de auxiliar as redes de computadores neste combate contra a indisponibilização dos serviços. Nesta tese é proposto um modelo de detecção de intrusos chamado Kappa-PSO-ARTMAP *Fuzzy*, onde primeiramente a base de dados original é pré-processada, por meio de uma técnica de seleção de atributos baseada em rede neural ARTMAP *Fuzzy* e coeficiente Kappa, para reduzir a quantidade de atributos, deixando apenas as características mais representativas. A seguir, aplica-se a técnica de otimização por enxame de partículas (*particle optimization swarm* – PSO) na seleção de um conjunto de critérios (parâmetro de escolha, parâmetro de vigilância do módulo ART_a, taxa de treinamento e acréscimo do parâmetro de vigilância do módulo ART_a) empregados no treinamento do classificador de ataques, de forma a maximizar a identificação correta de amostras classificadas. O algoritmo de detecção de intrusos empregado no classificador de ataques é a rede neural ARTMAP *Fuzzy*. O desempenho desta nova estratégia é avaliado sobre três bases de dados coletadas respectivamente de uma rede simulada cabeada, uma rede infraestruturada sem fio com criptografia WEP (*Wired Equivalent Privacy*) e WPA (*WiFi Protected Access*) habilitadas e uma rede infraestruturada sem fio com criptografia WPA2 (*WiFi Protected Access version 2*) habilitada. Os resultados obtidos na avaliação da metodologia Kappa-PSO-ARTMAP *Fuzzy* demonstram a diminuição do custo computacional do IDS sem acarretar piora na capacidade de reconhecimento e possuem uma abrangência de aplicação sobre redes WLAN e redes cabeadas.

Palavras-chave: Detecção de intrusos. Seleção de atributos. Otimização de parâmetros. Classificação de padrões. Rede neural ARTMAP *Fuzzy*. Coeficiente Kappa. Otimização por enxame de partículas. Redes cabeadas. Redes infraestruturadas sem fio.

ABSTRACT

In the last years have seen a strong increase in the 802.11 wireless local area network (WLAN) technologies use, and the security mechanisms implemented by amendments IEEE 802.11i and IEEE 802.11w have proven not very effective in combating attacks against availability of WLAN services. Intrusion detection systems emerge as a way to help computer networks in this combat against the deny of services. In this thesis it's proposed a model of intrusion detection called Kappa-PSO-Fuzzy ARTMAP, where initially the original database is pre-processed through a feature selection technique based on ARTMAP Fuzzy neural network and Kappa coefficient for reduce the amount of attributes, leaving only the most representative features. Then, apply the particle swarm optimization (PSO) technique in searching a set of criteria (choice parameter, ART_a module vigilance parameter, training rate and increase in the ART_a module vigilance paramater) employees in training attacks classifier, in order to maximize the accurate identification of classified samples. The intrusion detection algorithm used in the attacks classifier is the ARTMAP Fuzzy neural network. The performance of this new strategy is evaluated over three colleted databases respectively in a simulated wired network, infrastructured wireless network with WEP (Wired Equivalent Privacy) and WPA (WiFi Protected Access) encryption enabled and infrastructured wireless network with WPA2 (WiFi Protected Access version 2) encryption enabled. The obtained results in the Kappa-PSO-ARTMAP Fuzzy methodology demonstrate the IDS computational cost reduction without causing deterioration in the recognize capacity and have a scope of application over wireless and wired local area networks.

Keywords: Intrusion detection. Feature selection. Paramater optimization. Pattern classification. Fuzzy ARTMAP neural network. Kappa coefficient. Particle swarm optimization. Wired networks. Wireless networks.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ACK	*Acknowledgment*
AES	*Advanced Encryption Standard*
AP	*Access Point* (Ponto de acesso)
ART	*Adaptative Ressonance Theory*
AS	*Authenticator Server*
BIP	*Broadcast/Multicast Integrity Protocol*
BSS	*Basic Service Set* (Grupo de Serviço Básico)
BSSID	*Basic Service Set Identity*
CBC-MAC	*Cipher Block Chaining Message Authentication Code*
CCM	*Counter-Mode/Cipher Block Chaining Message Authentication Code*
CCMP	*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*
CFP	*Contention-Free Period*
CMAC	*Block Cipher based Message Authentication Code*
CP	*Contention Period*
CRC	*Cyclic Redundancy Code*
CSMA/CA	*Carrier Sense Multiple Access/Collision Avoidance*
CTR	*Counter Mode*
CTS	*Clear-to-Send*
CW	*Content Window*
DCF	*Distributed Coordination Function*
DIFS	*DCF Inter-frame Space*
DoS	*Denial of Service* (Negação de Serviço)

DS	*Distribution System* (Sistema de Distribuição)
EAP	*Extensible Authentication Protocol*
EAPoL	*EAP over LAN*
EIFS	*Extended Inter-frame Space*
ESS	*Extended Service Set*
FAM	Rede Neural ARTMAP *Fuzzy*
FCS	*Frame Check Sequence*
GTK	*Group Temporal Key*
HIDS	*Host based Intrusion Detection System*
IC	Inteligência Computacional
ICV	*Integrity Check Value*
IDS	*Intrusion Detection System* (Sistema Detector de Intrusão)
IEEE	*Institute of Eletrical and Eletronics Engineers*
IGR	Taxa de Ganho de Informação
IGTK	*Integrity GTK*
IPN	*IGTK Packet Number*
IV	*Initialization Vector*
KDD99	*Knowledge Discovery and Data Mining*
LAN	*Local Area Network*
MAC	*Media Access Control*
MFP	*Management Frame Protection*
MFPC	*Management Frame Protection Capable*
MFPR	*Management Frame Protection Required*
MIC	*Message Integrity Code*

MITE	*Man-in-the-Middle*
MMIE	*Management MIC Information Element*
MPDU	*MAC Protocol Data Unit*
MSK	*Master Session Key*
NAV	*Network Allocation Vector*
NIDS	*Network Intrusion Detection System*
PCF	*Point Coordination Function*
PHY	*Camada Física*
PIFS	*PCF Interframe Space*
PLCP	*Physical Layer Convergence Protocol*
PMK	*Pairwise Master Key*
PSK	*Pre-Shared Key*
PSO	*Particle Swarm Optimization* (Otimização por Enxame de Partículas)
PS-Poll	*Power Save-Poll*
PTK	*Pairwise Transient Key*
RC4	*Rivest Cipher 4*
RM	*Robust Management Frame*
RNA	Rede Neural Artificial
RSN	*Robust Security Network*
RSNA	*Robust Security Network Association*
RTS	*Request-to-Send*
RSN IE	*RSN Information Element*
R2L	Remoto para Usuário
SA	*Security Association*

SA Query	*Security Association Query*
SFS	*Sequential Forward Search*
SIFS	*Short Interframe Space*
SSID	*Service Set Identity*
STA	*Wireless Station* (Estação)
TCP	*Transmission Control Protocol*
TKIP	*Temporal Key Integrity Protocol*
U2R	Usuário para Superusuário
VPN	*Virtual Private Network*
WLAN	*Wireless Local Area Network*
WEP	*Wired Equivalent Privacy*
WPA	*WiFi Protected Access*
WPA2	*WiFi Protected Access version 2*
WM	*Wireless Medium* (Meio sem fio)

SUMÁRIO

1 INTRODUÇÃO

As redes sem fio 802.11 já podem ser consideradas uma tecnologia de redes de computadores bem difundida, como pode ser visto nos números apresentados pela IDC Brasil, onde 57,4% dos computadores vendidos em 2012 foram *notebooks*/*netbooks/ultrabooks* e as vendas de *smartphones* e *tablets* em 2012 cresceram, respectivamente, 78% e 171% com relação ao ano anterior (IDC BRASIL, 2013a; 2013b; 2013c). Isso se deve, principalmente, à sua instalação simplificada, mobilidade, alcançar regiões onde a rede confinada chega com dificuldade, barateamento dos dispositivos de comunicação sem fio e a possibilidade de atingir altas taxas de transferências compatíveis com as redes cabeadas.

Devido a essa ampla utilização da tecnologia *wireless*, estas redes sem fio tem amadurecido muito desde o surgimento do primeiro padrão 802.11 em 1997 (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS - IEEE, 1999). A partir desse momento, diversas emendas foram realizadas sobre o texto original, das quais a maioria trata do aumento da vazão e velocidade operacional na camada física da WLAN (*Wireless Local Area Network*). Contudo, em 2004 foi ratificada a emenda 802.11i (IEEE, 2004) cuja função principal é tratar as ameaças relacionadas à confidencialidade, integridade e controle de acesso numa WLAN. Com a implantação do padrão 802.11i nos adaptadores de redes sem fio, muito das preocupações de segurança que cercavam a tecnologia WLAN foram resolvidas.

Os mecanismos de segurança fornecidos pelo padrão original 802.11 sofriam de inúmeras falhas e podiam facilmente ser corrompidos. Até a ratificação do padrão 802.11i, mecanismos de segurança da camada de rede, tais como VPNs (*Virtual Private Networks*), foram empregados para garantir acesso seguro numa WLAN. O padrão 802.11i introduziu o conceito *robust security network* - RSN (IEEE, 2004), onde se provê confidencialidade e integridade ao tráfego da WLAN por meio de protocolos e algoritmos criptográficos fortes e o controle de acesso é implementado pelo *framework* 802.1X (IEEE, 2001). O *framework Extensible Authentication Protocol* - EAP (ABOBA et al., 2004) é utilizado para autenticar os pontos da WLAN.

Apesar dos avanços em segurança trazidos pelo padrão 802.11i, a proteção estava focada apenas nos quadros de dados. Os quadros de gerenciamento e controle continuavam sem nenhuma salvaguarda, e com as alterações implantadas pelas emendas 802.11r/k/v, novas informações relevantes sobre as redes sem fio foram introduzidas nos quadros de gerenciamento (AHMAD; TADAKAMADLA, 2011).

Neste sentido foi ratificada em 2009 a emenda 802.11w (IEEE, 2009), que assegurou à rede as seguintes propriedades de segurança: autenticidade da origem dos dados, detecção de *replay* e proteção ao quadro de gerenciamento.

No entanto, apenas poucos quadros de gerenciamento (*Deauthentication*, *Diassociation* e *Action*) estão protegidos e os quadros de controle continuam sem mecanismo de proteção. A tecnologia WLAN continua carente com relação à questão de segurança, principalmente, quando se trata da disponibilidade dos serviços da rede, pois tanto os quadros de gerenciamento quanto os quadros de controle são bastante empregados em ataques para indisponibilizar os recursos da rede para usuários legítimos, popularmente conhecidos como ataque de Negação de Serviço (*denial of service* - DoS) (BICAKCI; TAVLI, 2009).

Uma forma de amenizar os ataques de DoS nas redes 802.11 é implantar ferramentas de segurança que monitorem o comportamento do tráfego WLAN de modo que sempre que ocorrer interrupções ocasionadas por dispositivos maliciosos ou não-autorizados, tais ferramentas acionem alertas de ataque para que ações defensivas próprias sejam executadas para impedir ou minimizar os danos.

Uma técnica de segurança que se enquadra nesse conceito são os sistemas detectores de intrusão (*intrusion detection system* - IDS). O IDS pode analisar o tráfego monitorado a partir de um conjunto de assinaturas de ataques (detecção baseada em assinaturas) ou pela definição de um perfil esperado para um dispositivo pertencente à rede (detecção baseada em anomalia). A principal deficiência do IDS baseado em assinaturas acontece quando surgem novos ataques, pois este IDS não consegue reconhecer eventos inéditos. Com relação ao IDS baseado em anomalia, a dificuldade está relacionada à definição desse perfil de bom comportamento do dispositivo (SOBH, 2006; WU; BANZHAF, 2010).

Os sistemas detectores de intrusão têm sofrido grandes mudanças desde o aparecimento do primeiro modelo baseado em sistemas especialistas e dados estatísticos até o uso de inteligência artificial e aprendizado de máquina nos modelos mais atuais. Embora, na atualidade, os IDSs estejam enfrentado muitos problemas, tais como: grandes volumes de tráfego das redes, distribuição de dados altamente desbalanceada, dificuldade em determinar o limite entre comportamento normal e anômalo, necessidade de adaptação contínua para ambientes altamente dinâmicos (WU; BANZHAF, 2010).

A inteligência computacional busca oferecer uma boa resposta para as restrições enfrentadas pelos IDSs, por meio do desenvolvimento de sistemas inteligentes que imitam aspectos do comportamento humano, tais como: aprendizado, percepção, raciocínio, evolução e adaptação (WU; BANZHAF, 2010).

Os principais métodos de inteligência computacional aplicados nos sistemas de detecção de intrusão são redes neurais artificiais, sistemas *Fuzzy*, computação evolucionária, sistemas imuno-artificiais, inteligência de enxame e *soft computing* (WU; BANZHAF, 2010).

1.1 Contribuições do trabalho

O presente trabalho busca contribuir através dos seguintes tópicos:

- **Utilização do coeficiente Kappa como métrica de desempenho na avaliação de IDS**: normalmente, os trabalhos relacionados na avaliação de IDS empregam a exatidão global como medida de desempenho, mas esta unidade mostra problemas quando aplicada em bases de dados desbalanceadas. Por isso, uma das grandes contribuições do trabalho é o uso do coeficiente Kappa como função de avaliação para o problema de detecção de intrusos.
- **Construção de bases de dados coletadas em redes infraestruturada sem fio com criptografia WEP, WPA e WPA2 habilitadas**: a falta de bases de dados representativas ao ambiente de rede WLAN com suporte aos mecanismos de segurança WEP, WPA e WPA2 nos leva a implementação de *testbeds* com esses cenários e a construção de bases de dados para posterior avaliação da metodologia de IDS proposta neste trabalho.
- **Avaliação dos campos do cabeçalho MAC na definição de perfis de comportamento de tráfego**: Outra oportunidade surgida na construção das bases de dados WEP-WPA e WPA2 é avaliar os campos do cabeçalho MAC como atributos na definição de perfis de comportamento, pois muitos trabalhos acabam empregando campos das camadas superiores (aplicação, transporte e rede) na montagem da base de treinamento.
- **Aplicação da técnica de otimização por enxame de partículas (*particle swarm optimization* – PSO) para selecionar parâmetros ótimos para o treinamento do IDS**: A configuração da rede neural ARTMAP *Fuzzy* em sistemas detectores de intrusão é realizado por um ajuste padrão ou aplicam-se técnicas de otimização computacional para definir um formato que maximize a função de avaliação do IDS, na metodologia Kappa-PSO-ARTMAP *Fuzzy* aplica-se a técnica de otimização PSO para buscar esta configuração ótima.

- **Pré-processamento da base de dados para reduzir o custo computacional do IDS**: A alta dimensionalidade das bases de dados é um dos grandes obstáculos para diminuir o custo computacional de um IDS, que torna necessário o uso de pré-processamento na base original de forma reduzí-la a uma dimensão que atenua o custo computacional e mantenha a capacidade de identificação de amostras. Sendo assim, no Kappa-PSO-ARTMAP *Fuzzy* é introduzido um módulo de seleção de atributos que avalia os subconjuntos candidatos por meio do classificador ARTMAP *Fuzzy* e utiliza o coeficiente Kappa no cálculo da função de avaliação do subconjunto.

1.2 Objetivos

O objetivo principal deste trabalho é desenvolver metodologias de detecção de intrusos que não seja atenta apenas em aumentar a taxa de detecção e diminuir a taxa de falsos alarmes, mas também em reduzir o custo computacional originado destas soluções, bem como poder aplicá-las sobre bases de dados coletadas tanto em redes cabeadas quanto em redes sem fio. Sendo assim, é proposto um IDS com os seguintes objetivos específicos:

- Aplicar a rede neural ARTMAP Fuzzy como o classificador de ataques;
- Utilizar seleção de atributos no pré-processamento de dados para extrair os atributos mais representativos da base original e gerar um subconjunto ótimo a ser utilizado no IDS;
- Empregar a técnica de otimização por enxame de partículas na seleção dos parâmetros de escolha (α), vigilância (ρ), treinamento (β) e acréscimo do parâmetro de vigilância (δ) para treinamento do classificador ARTMAP Fuzzy;
- Construir bases de dados coletadas em redes infraestruturadas sem fio com criptografia WEP, WPA e WPA2 habilitadas;
- Avaliar o coeficiente Kappa como métrica de desempenho de IDS.

1.3 Organização do trabalho

Este trabalho está organizado em seis capítulos como segue:

- Capítulo 1: Introdução, objetivos e contribuições para o presente trabalho.

- Capítulo 2: Embasamento teórico sobre as redes sem fio padrão IEEE 802.11, suas operações, mecanismos de segurança existentes e as vulnerabilidades ainda persistentes na WLAN.
- Capítulo 3: Revisão conceitual sobre os sistemas detectores de intrusão, apresentando sua taxonomia quanto ao tipo de intrusão, comportamento de detecção, abordagem de detecção e tipo de sistemas monitorados. A seguir, apresentam-se os critérios de avaliação para sistemas detectores de intrusão e, por último, é realizado uma análise dos principais trabalhos relacionados à metodologia de detecção de intrusos associado a redes infraestruturadas sem fio.
- Capítulo 4: Apresentação da metodologia Kappa-PSO-ARTMAP *Fuzzy* e os conceitos teóricos (seleção de atributos, coeficiente Kappa, rede neural ARTMAP *Fuzzy* e otimização por enxame de partículas) envolvidos nesta técnica.
- Capítulo 5: Investigação do desempenho do IDS Kappa-PSO-ARTMAP *Fuzzy* sobre três bases de conhecimento que representam redes cabeadas e redes infraestruturadas sem fio.
- Capítulo 6: Considerações finais e perspectivas para trabalhos futuros.

2 SEGURANÇA EM REDES LOCAIS SEM FIO PADRÃO IEEE 802.11

Com o crescimento do uso da tecnologia WLAN IEEE 802.11 por todo tipo de organização, a segurança tem se tornado uma questão muito importante. Na última década surgiram muitas propostas de protocolos de segurança e mecanismos de troca de chaves para as redes IEEE 802.11.

Neste Capítulo serão apresentadas as operações existentes numa WLAN e uma revisão sobre a evolução dos mecanismos de segurança nas emendas sobre o padrão IEEE 802.11.

2.1 Topologias de uma rede IEEE 802.11

Uma arquitetura WLAN 802.11 possui múltiplos componentes de rede que pode ser organizadas em duas topologias básicas: infraestruturado e *adhoc*. Antes de especificar melhor estas arquiteturas, é interessante definir os quatro componentes principais em funcionamento nestes modelos (IEEE, 1999):

- Meio sem Fio (*Wireless Medium* - WM) – O meio utilizado para transferir quadros entre os nós da rede WLAN 802.11.

- Sistema de Distribuição (*Distribution System* - DS) – Componente lógico empregado para encaminhar quadros entre estações pertencentes a diferente *base stations* e uma rede local cabeada (*Local Area Network* - LAN).

- Estação (*Station* - STA) – Qualquer dispositivo que acesse o meio sem fio é essencialmente uma estação.

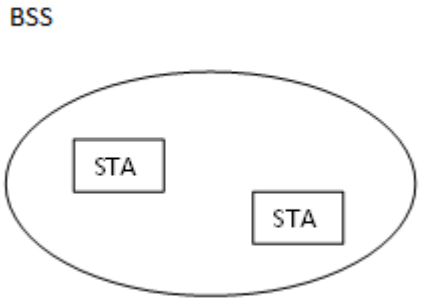
- Ponto de acesso (*Acess Point* - AP) – Um AP é uma estação (STA) especializada que fornece conectividade entre vários STAs e entre STAs e DS.

A Figura 1 apresenta o bloco de construção básico de uma arquitetura 802.11 WLAN, cuja denominação é grupo de serviço básico ou *basic service set* - BSS. Um simples BSS representa um grupo de estações que podem se comunicar e sua cobertura é definida por meio das características de propagação no WM. Cada BSS está associado a um BSSID (*Basic Service Set Identity*), que é um identificador binário com 48 bits, cuja função é criar uma assinatura única para cada BSS.

A topologia na qual os BSSs se organizam, ilustrado na Figura 2, acontece por meio do modo infraestruturado ou *adhoc*. No modo infraestruturado, o AP tem o papel de gerenciar a troca de informações entre as estações pertencentes ao mesmo BSS e a BSSs diferentes, por

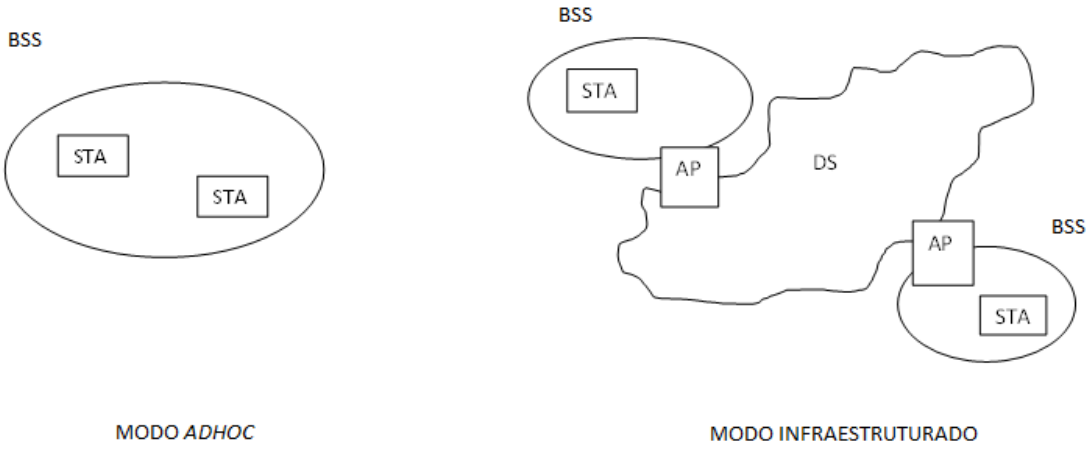
meio do DS. Enquanto no modo *adhoc*, não há entidade de gerenciamento central, tal como o AP, e assim a comunicação dar-se-á de forma direta entre as estações.

Figura 1 - Representação gráfica de um BSS.



Fonte: Adaptado de IEEE (1999).

Figura 2 - Topologias de redes numa arquitetura WLAN.



Fonte: Adaptado de IEEE (1999).

Enquanto o modo ad-hoc, geralmente, é utilizado para transferência de arquivos entre STAs numa rede pequena, o modo infraestruturado é aplicado como uma extensão de uma rede local (LAN) convencional, fazendo parte da infraestrutura de redes da organização. O padrão 802.11 ainda permite que um conjunto de BSSs infraestruturadas seja conectado por meio de um DS, formando um grupo de serviço extendido ou *extended service set* - ESS. Os componentes do ESS são apenas as BSSs infraestruturadas, o DS trata apenas de interligá-las.

2.2 Operações básicas de uma rede IEEE 802.11

O padrão 802.11 define um endereço MAC (*Media Access Control*) de 48 bits para cada nó (estações ou ponto de acesso) da WLAN e os quadros são encaminhados baseados nesses endereços MAC. Nesta seção relatam-se como é gerenciado o acesso ao meio sem fio na WLAN e como as STA's estabelecem uma associação com o AP para a comunicação de dados.

2.2.1 Subcamada MAC

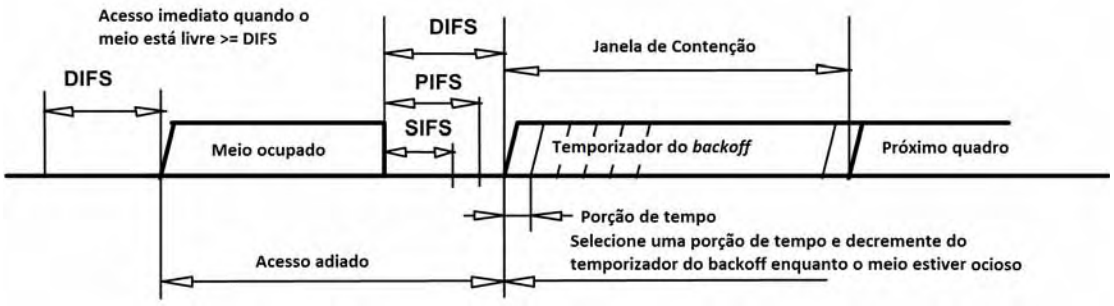
Para disciplinar o acesso ao meio de transmissão sem fio, a WLAN emprega a técnica CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), cujo objetivo principal é evitar que ocorram colisões entre os quadros durante o processo de transmissão de dados. Esta técnica é empregada devido às colisões no meio sem fio terem um custo muito alto na disponibilidade da capacidade de transmissão da WLAN.

O padrão 802.11 especifica dois mecanismos de controle, DCF (*Distributed Coordination Function*) e PCF (*Point Coordination Function*), para a resolução de disputas entre as STA's para acesso ao meio sem fio. A seguir, relatam-se os princípios de cada técnica.

O método DCF, representado na Figura 3, utiliza um contador aleatório (*backoff*) para resolver as disputas entre as STA's para acessar o canal de transmissão. Todos os quadros recebidos devem enviar um ACK (*Acknowledgment*) positivo da STA destino. Antes de transmitir, a STA observa o canal para garantir que o meio não esteja ocupado. Se o meio estiver ocupado, a STA adia seu acesso até o canal encontrar-se ocioso por um período de tempo igual ao DIFS (*DCF Inter-frame Space*) quando o último quadro detectado no meio for recebido corretamente, ou depois do meio sem fio ficar ocioso por um período de tempo igual ao EIFS (*Extended Inter-frame Space*) quando o último quadro detectado no meio não for recebido corretamente. Após o tempo de ociosidade, a STA seleciona um valor aletório de *backoff* que pode variar de 0 a CW, onde o tempo de contenção (*content window* - CW) é um valor mantido por cada STA. O temporizador do *backoff* é decrementado uma porção de tempo a cada observação que o canal está ocioso e quando o meio sem fio torna-se novamente ocupado, o valor existente no temporizador é congelado. A STA pode acessar o canal para transmissão quando o temporizador for decrementado à zero (IEEE, 1999).

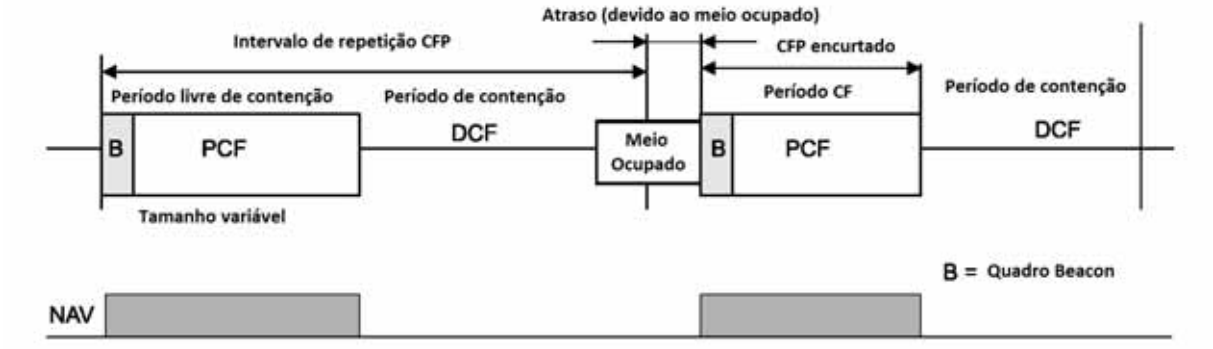
PCF disciplina o acesso das STA's ao canal de transmissão por meio de um ponto central de gerenciamento (AP), exatamente por isso só pode ser utilizado no modo infraestruturado da WLAN. O ponto central de gerenciamento garante que o meio esteja disponível para transmissão entre as STA's durante um período de tempo chamado período livre de contenção (*contention-free period* - CFP), sem a necessidade da disputa pelo canal. Isto é seguido por um período de contenção (*contention period* - CP), onde as STA's comunicam-se diretamente sobre o controle do modo DCF, o qual será explicado a seguir. A Figura 4 mostra como no modo PCF a transferência de quadros livre de contenção controlado pelo AP alterna com a transferência baseada em contenção, a qual está sujeita as regras do DCF. A frequência na qual o CFP ocorre é determinada pelo intervalo de repetição PCF, um parâmetro controlado pelo AP (IEEE, 1999).

Figura 3 - Funcionamento do mecanismo de acesso ao meio DCF.



Fonte: Adaptado de IEEE (1999).

Figura 4- Alternância entre períodos livres de contenção e com contenção.



Fonte: Adaptado de IEEE (1999).

Em ambos os métodos de acesso existem parâmetros para regular o tempo necessário de espera antes de liberar o acesso ao meio para uma STA, uma vez que o meio pode estar ocupado com a transmissão de quadros de dados, quadros de controle ou ainda estar disponível, para que alguma estação possa tomar o meio de transmissão.

Para garantir a atomicidade das operações na WLAN, o padrão 802.11 requer duas propriedades. A primeira propriedade define que todo quadro transmitido com sucesso deve gerar um ACK positivo por parte da STA destino para a STA origem. Nenhuma operação é permitida enquanto esta transação estiver ocorrendo. Se o quadro ou o ACK é perdido, a STA origem deve retransmitir o quadro. A segunda propriedade procura garantir que nenhuma STA obtenha o controle do canal de transmissão durante o tempo que o meio estiver ocupado. Ela faz isso por meio de um mecanismo de detecção virtual de portadora implementado na subcamada MAC, onde cada STA tem um vetor de alocação de recursos (*network allocation vector* - NAV) que determina quanto tempo em microssegundos o meio vai estar reservado para este elemento. A definição do tempo de reserva alocado no NAV é realizada por meio do campo *duration* no cabeçalho do quadro MAC. O valor a ser fornecido para a reserva depende do tempo gasto para o quadro ser transmitido e o recebimento do ACK. Todas as STAs que detectam quadros *unicast* no meio sem fio configuram seus valores NAV com o valor do campo *duration* do quadro detectado. O mecanismo de detecção virtual de portadora considera o canal ocupado quando o valor do NAV é maior que zero e decrementa-o, repetidamente, uma porção de tempo até atingir zero, para assim considerar o meio ocioso.

Juntamente com o NAV, o espaçamento interquadros também é utilizado para garantir a atomicidade das operações numa WLAN. Há quatro tipos de espaçamento interquadros aplicados no DCF e PCF (GILL, 2009; IEEE, 1999):

- DIFS (*DCF Inter-frame Space*): é o tempo mínimo de ociosidade onde as STA's devem esperar antes de acessar o meio para uma transmissão.

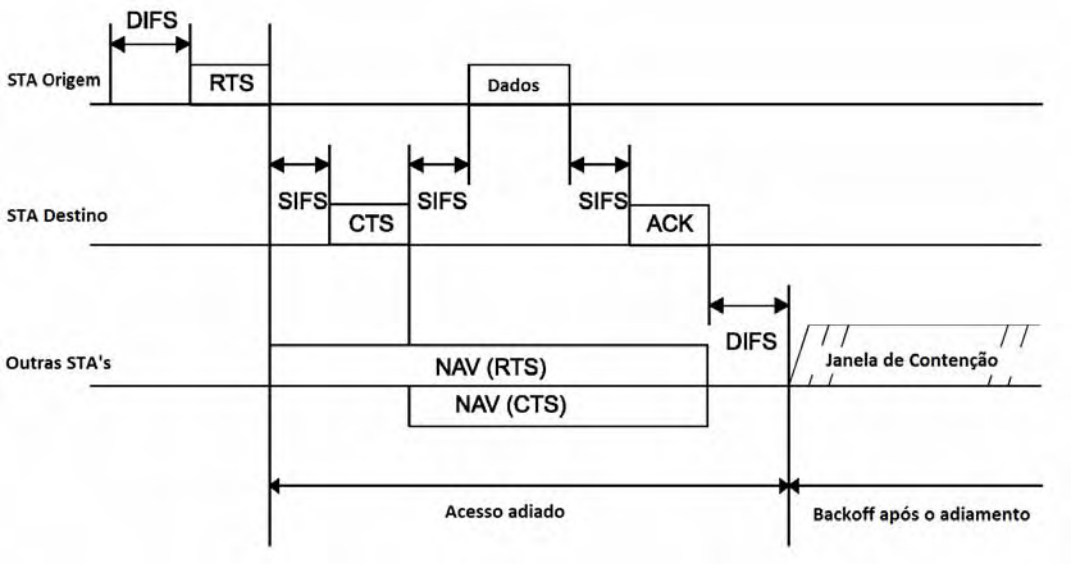
- SIFS (*Short Interframe Space*): é menor que o DIFS e aplica-se este espaçamento em transmissões de alta prioridade, tais como os quadros ACK, RTS (*Request-to-Send*) e CTS (*Clear-to-Send*). STA's com transmissões de alta prioridade têm que esperar somente o tempo SIFS antes de acessar o meio sem fio e assim acabam tendo prioridade sobre outras STA's, as quais terão que esperar um tempo DIFS.

- PIFS (*PCF Interframe Space*): deve ser utilizado somente em STA's executando sobre o PCF, para garantir prioridade no acesso ao meio no início do período livre de contenção ou para uma STA transmitir o quadro *Channel Switch Announcement*.

- EIFS (*Extended Inter-frame Space*): é maior que o DIFS e aplica-se este espaçamento quando há um erro na transmissão do quadro.

Além de utilizar o campo *duration* dos quadros *unicast* para atualizar o NAV, o padrão 802.11 também leva em consideração um tipo especial de *handshake* para reservar o canal antes de iniciar a transmissão. Este mecanismo é chamado *handshake* RTS-CTS, ilustrado na Figura 5. Quando uma STA ganha acesso ao meio, ela adota os quadros *Request-to-Send* (RTS) e *Clear-to-Send* (CTS) para reservar o acesso ao canal durante sua transmissão. A STA origem envia um quadro RTS para a STA destino, a qual responde com o quadro CTS posteriormente a um espaçamento SIFS. O campo *duration* nos cabeçalhos MAC dos quadros RTS e CTS determinam o tempo de duração proposto para a transmissão dos dados. Se alguma STA ouvir por acaso os quadros RTS e CTS, atualiza o seu NAV e retarda sua entrada ao meio pelo período definido na variável. Logo após o *handshake* RTS-CTS, as STA's origem e destino podem comunicar-se sem a interferência de outra estação da WLAN pelo período destinado a transmissão de dados (GILL, 2009; IEEE, 1999).

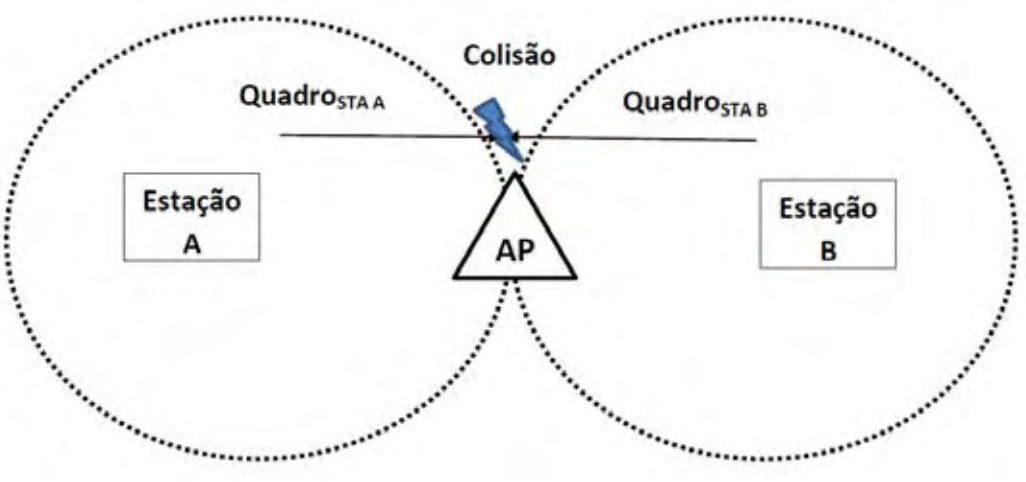
Figura 5 - *Handshake* RTS-CTS.



Fonte: Adaptado de IEEE (1999).

O mecanismo handshake RTS-CTS é extremamente útil para minimizar o problema do terminal escondido. A Figura 6 mostra este problema onde o AP escuta dois terminais A e B, mas ambas STA's não detectam uma a outra e por isso estão vulneráveis a ocorrer colisões de quadros no processo de transmissão.

Figura 6 - Problema do terminal escondido.

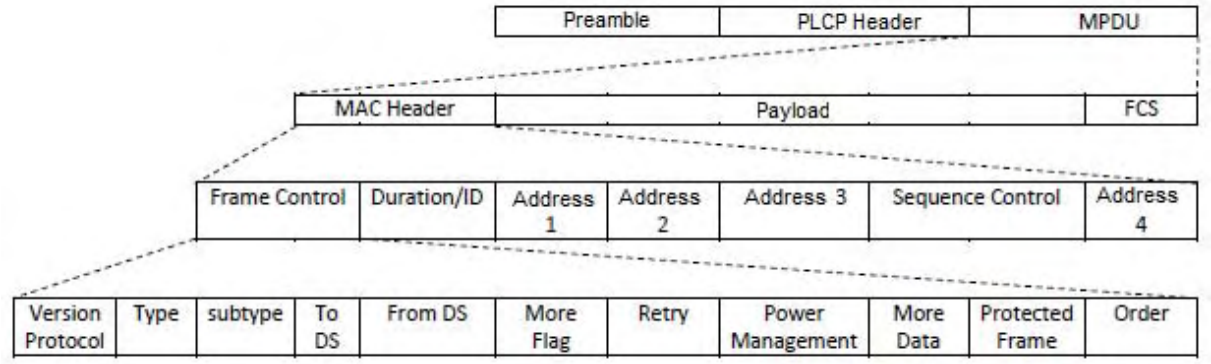


Fonte: Elaboração do próprio autor.

2.2.2 Estrutura de quadros

A estrutura de quadros definida pelo padrão 802.11 é um pouco mais complexa que o padrão ETHERNET, pois existem vários níveis de encapsulamentos. A Figura 7 descreve a organização do formato do quadro 802.11. No nível mais alto encontram-se três campos: preâmbulo, cabeçalho PLCP (*Physical Layer Convergence Protocol*) e MPDU (*MAC Protocol Data Unit*). O campo MPDU contém os dados transmitidos e nele há um segundo nível de encapsulamento formado pelos campos: MAC *Header* (cabeçalho), *frame body* (corpo do quadro) e FCS (*Frame Check Sequence*). O terceiro nível de encapsulamento ocorre no campo MAC *Header*, o qual é constituído pelos campos: *frame control*, *duration/ID*, endereço 1, endereço 2, endereço 3, *control sequence* e endereço 4. No último nível de encapsulamento, o campo *frame control* acomoda os seguintes campos na sua constituição: *Protocol Version*, *Type*, *Subtype*, *To DS*, *From DS*, *More Fragments*, *Retry*, *Power Management*, *More Data*, *Protected Frame*, and *Order*.

Figura 7 - Organização do formato do quadro 802.11.



Fonte: Adaptado de IEEE (1999).

O foco desta tese é no *MAC Header*, por isso a seguir será detalhada a função de cada campo existente nos segundo, terceiro e quarto nível de encapsulamento do quadro 802.11.

- *Frame Control* – Esse quadro contém informações de controle usado para definir o tipo de quadro 802.11. A estrutura desse campo é composta por onze subcampos:
  - *Protocol Version* - indica a versão corrente do protocolo 802.11 utilizado. As estações receptoras usam esse valor para determinar se a versão do protocolo do quadro recebido é suportada.
  - *Type* e *Subtype* - determina a função do quadro. Há três diferentes tipos de quadro: controle, dados e gerenciamento. Há múltiplos subtipos para cada tipo de quadro. Cada subtipo determina uma função específica desempenhada com o seu tipo de quadro associado, por exemplo, RTS ou CTS.
  - *To* DS (Para Sistema de Distribuição) e *From* DS (Do Sistema de Distribuição) - indica se a informação será enviada para um sistema de distribuição ou se foi originada em um sistema de distribuição. Esses campos somente são utilizados em um quadro de dados transmitidos por estações conectadas a um ponto de acesso.
  - *More Fragments* - campo utilizado para informar se existem mais fragmentos do quadro, seja de dados ou de gerenciamento, que devem ser encaminhados.
  - *Retry* - indica se a informação (dados ou gerenciamento) está ou não sendo retransmitida.

  - *Power Management* - é usado pelo ponto de acesso para deixar ou retirar o receptor do estado de espera.
  - *More Data* - indica que a STA transmissora tem quadros adicionais para a STA receptora.
  - *Protected Frame* - indica ou não se está sendo usado no quadro o processo de criptografia e autenticação. Isso pode ser configurado para todos os quadros de dados e gerenciamento que têm o subtipo configurado para autenticação.
  - *Order* - indica se todos os quadros de dados recebidos devem ser processados em ordem.

- *Duration/ID* – Quando usado como campo *duration* determina o tempo, em microssegundos, onde o meio estará alocado para transmissão com sucesso do quadro 802.11. Este campo é empregado para atualizar o NAV das estações WLAN. Em certos quadros de controle, este campo atua como um identificador de conexão.
- Endereços – A quantidade de campos *endereços* e seus significados dependem do contexto do tipo e subtipo do quadro 802.11. O campo endereço pode assumir um dos seguintes tipos: BSSID, endereço origem, endereço destino, endereço da estação transmissora e endereço da estação receptora.
- *Sequence Control* – Inclui um número de sequência com 12 bits, o qual enumera os quadros transmitidos entre uma STA transmissora e uma STA receptora, e um número de fragmento com 4 bits, que é aplicado para fragmentação e remontagem. Este campo está presente apenas nos quadros de gerenciamento e dados.
- *Frame Body* – o corpo do quadro é variável no tamanho e específico ao quadro transmitido.
- *Frame Check Sequence* – a estação transmissora do quadro aplica um CRC (*Cyclic Redundancy Code*)-32 sobre todos os campos do MAC *Header* e sobre o corpo do quadro para gerar o FCS. Assim é possível que a estação receptora do quadro através do CRC-32 analise se o valor recebido no campo FCS é o mesmo recebido, possibilitando a verificação de possíveis erros durante a transmissão.

Os tipos de quadros numa rede 802.11 pertencem a três categorias: 1) gerenciamento - responsável pelo gerenciamento da rede e o controle de admissão; 2) controle – ajuda no controle de acesso e na entrega dos quadros de dados; 3) dados – transportam os dados a serem transmitidos.

Os quadros de gerenciamento podem ser subcategorizados em:

- *Association Request* – Este quadro é enviado de uma STA para um AP, solicitando associação com o AP e contém as informações de capacidade da STA.
- *Association Response* – Este quadro é enviado do AP para a STA como resposta ao quadro *Association Request*, anunciando se aceita ou não a solicitação da STA.
- *Reassociation Request* – Enviado para o AP por meio da STA, quando a STA muda de um BSS para outro BSS, de modo que o novo AP possa negociar com o antigo AP o encaminhamento dos quadros armazenados. Este quadro também pode ser utilizado para atualizar os atributos de associação enquanto a STA permanecer associada ao mesmo AP.
- *Reassociation Response* – Este quadro é a resposta do AP a solicitação realizada pela STA por meio do quadro *Reassociation Request*.
- *Probe Request* – Este quadro é enviado pela STA para conseguir informações sobre o AP ao qual a STA tem interesse em associar-se. Geralmente, é utilizado para localizar um BSS.
- *Probe Response* – Este quadro contém as informações sobre o AP solicitadas pela STA por meio do quadro *Probe Request*.
- *Beacon* – O AP divulga sua presença e suas características para as STA's por meio da transmissão periódica do *beacon*. Este quadro ajuda as STA's na localização do BSS.
- *Disassociation* – Este quadro é empregado para terminar a associação entre a STA e o AP. O quadro *Disassociation* pode ser enviado de qualquer estação WLAN (STA ou AP).
- *Authentication* – Estes quadros são trocados entre a STA e o AP para autenticar um ao outro durante o estabelecimento de uma associação.

- *Deauthentication* – Este quadro é utilizado para terminar a autenticação (por consequência, a associação) entre a STA e o AP. O quadro *Deauthentication* pode ser enviado de qualquer estação WLAN (STA ou AP).

Os quadros de controle podem ser subcategorizados em:

- *Power save-poll (PS-Poll)* – Este quadro solicita ao AP para enviar os quadros armazenados para uma STA que acabou de acordar do modo *power-save*.
- *Request-to-Send (RTS)* – Este quadro é empregado no mecanismo *handshake* RTS-CTS por uma estação para alertar ao destinatário e as outras STA's na faixa de cobertura que tem a intenção de transmitir um quadro para o destinatário.
- *Clear-to-Send (CTS)* – Este é o segundo quadro no mecanismo *handshake* RTS-CTS. O quadro CTS é enviado da STA destino para a STA remetente, funciona como um consentimento do quadro RTS e concede a permissão para a STA remetente enviar os quadros de dados.
- *Acknowledgment (ACK)* – Este quadro é enviado do destinatário para o remetente e sua principal função é anunciar ao remetente que o quadro foi recebido com sucesso.

Os quadros de dados podem ser subcategorizados em:

- *Data* – Este quadro executa atualmente o encapsulamento dos dados recebidos das camadas superiores da rede sem fio.
- *Null Function* – Este quadro não transporta qualquer informação do usuário e é utilizado para gerenciamento de energia.

2.2.3 Funcionamento da rede

Toda estação WLAN mantém duas variáveis de estados para cada estação que se comunica sobre o meio sem fio. Estas variáveis são referenciadas como *Authentication State* e *Association State*. Os valores para a variável *Authentication State* são autenticado e não autenticado. Os valores para a variável *Association State* são associado e não associado. Estas variáveis criam três estados, nativamente, sobre a STA para cada estação remota, com a qual se comunica:

- **Estado 1** – estado inicial, não autenticado e não associado.
- **Estado 2** – autenticado e não associado.

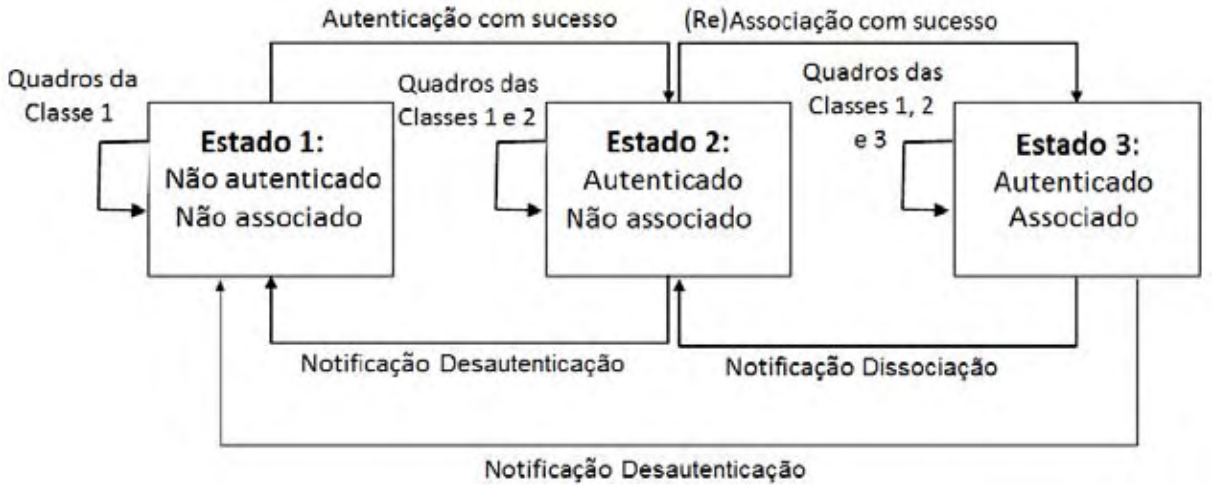
- **Estado 3** – autenticado e associado.

O estado corrente entre uma estação origem e uma estação destino determina qual tipo de quadro pode ser trocado entre as STA's. Os quadros permitidos são agrupados dentro de classes, as quais correspondem aos estados. As classes de quadros são definidas da seguinte forma:

- Classe 1 – Quadros pertencente à classe 1 são permitidos nos estados 1, 2 e 3. Esta classe de quadros permite as STAs buscar uma WLAN e autenticar-se com ela. Os quadros referente à classe 1 são: os quadros de controle RTS, CTS e ACK; os quadros de gerenciamento *Probe Request/Response*, *Beacon*, *Authentication* e *Deauthentication*; e os quadros de dados com os subcampos *To DS* e *From DS* do campo *frame control* estabelecido com zero.
- Classe 2 – Quadros da classe 2 são permitidos apenas nos estados 2 e 3. Estes quadros coordenam associações entre as STA's e os AP's e somente podem ser transmitidos após a autenticação com sucesso da STA na rede. Os quadros relativos à classe 2 são os quadros de gerenciamento *Association Request/Response*, *Reassociation Request/Response* e *Diassociation*. Se um AP recebe um quadro de classe 2 originado de uma STA não autenticada, a sua resposta é um quadro *Deauthentication*, o qual retorna a STA para ao estado 1.
- Classe 3 – Quadros de classe 3 são permitidos apenas no estado 3, ou seja, quando a STA completou com sucesso a autenticação e associação com o AP. Quadros referente à classe 3 são o quadro de controle PS-Poll, o quadro de gerenciamento *Deauthentication* e qualquer quadro de dados. Se um AP recebe um quadro de classe 3 originado de uma STA não associada, a sua resposta é um quadro *Diassociation*, que regressa a STA para o estado 2. Se a STA não for autenticada, o AP responde com o quadro *Deauthentication* e leva a STA de volta para o estado 1.

A Figura 8 ilustra as transições dos nós WLAN num diagrama de classes dos quadros 802.11.

Figura 8 - Diagrama de Estados 802.11



Fonte: Adaptado de Gill (2009).

2.3 Princípios de segurança numa rede IEEE 802.11

Devido à natureza compartilhada do meio sem fio, os mecanismos de segurança numa WLAN são singularmente diferentes daqueles existentes numa rede cabeada. No entanto, há semelhanças entre os princípios de segurança numa WLAN com aqueles encontrados nas redes LAN, bem como em outros tipos de redes sem fio. Estes princípios são descritos a seguir (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST, 2007):

- Confidencialidade – A WLAN deve impedir que nenhuma entidade não autorizada possa ler os dados transmitidos entre duas estações comunicantes.
- Integridade – A WLAN deve ser capaz de detectar qualquer mudança que ocorra no tráfego da rede, independente se é intencional ou não. Isto inclui detecção de retransmissão e proteção contra ataques *replay*.
- Disponibilidade – A WLAN deve impedir ou pelo menos minimizar ataques contra a funcionalidade da rede, tal como ataques de negação de serviço (DoS).
- Controle de Acesso – A WLAN deve limitar os direitos de acesso à rede e seus recursos pelos dispositivos e seus usuários. Políticas de controle de acesso e autenticação devem ser empregadas de modo que obrige as STA's criarem uma identidade na WLAN e, assim, definir os recursos pertencente a cada elemento da rede.

Contudo, os desafios de segurança de uma WLAN são muito maiores que os existentes numa rede cabeada, devido às características inerentes do meio sem fio. Ao contrário das

redes confinadas, onde o acesso ocorre por meio de um ponto de rede, no meio sem fio qualquer dispositivo que esteja na área de cobertura da rede pode acessá-la. Para lançar um ataque ou injetar um tráfego numa rede cabeada, o atacante deve primeiramente obter o acesso físico à rede ou comprometer remotamente o sistema. No caso de uma WLAN, basta que o atacante esteja na área de cobertura da rede alvo.

No próximo tópico serão relatadas as ameaças enfrentadas pela WLAN devido às especificidades relativa aos protocolos da camada MAC e PHY.

2.4 Ameaças à segurança numa rede IEEE 802.11

As principais categorias referentes às ameaças de segurança numa WLAN podem ser divididas da seguinte forma (NIST, 2007; WELCH; LANTHROP, 2003):

- Análise de tráfego – Esta ameça refere-se às técnicas aplicadas por um adversário para monitorar o tamanho e a frequência das comunicações numa WLAN para coletar informações sobre as transmissões da rede. Para uma WLAN, este tipo de ameaça é muito real, pois um adaptador de rede WLAN no modo promíscuo pode coletar todo tipo de informação trafegada na rede. Mesmo que o tráfego da rede esteja criptografado outras informações relevantes podem ser coletadas da WLAN, tais como: a quantidade de STA's, os períodos de alta atividade, a topologia e os protocolos empregados.
- Interceptação passiva – A natureza aberta do meio sem fio permite ao adversário, passivamente, coletar todo o tráfego da WLAN, sem a necessidade de associar-se a rede ou transmitir dados para a mesma.
- Modificação, remoção e interceptação da mensagem – Com o acesso garantido ao meio WLAN, o adversário pode alterar a mensagem executando as seguintes ações: remoção, inserção, reordenamento e modificação.
- Injeção da mensagem e Interceptação Ativa – Neste tipo de ameaça, o adversário não monitora apenas o tráfego WLAN, mas também introduz tráfego dentro da rede por meio da injeção de mensagem. A injeção de mensagem pode ser aplicada tanto para a falsificação de quadros quanto para a inserção de quadros repetidos dentro da WLAN. Um adversário pode enviar quadros com um endereço MAC fonte, BSSID e SSID (*Service Set Identity*) falsificados de um AP legítimo e, assim, atrair STA's desavisadas para

associar-se a ele. Além disso, o adversário pode colher informações mais especializadas da WLAN por meio da injeção de quadros customizados.

- Acesso não autorizado – Neste tipo de ameaça, o adversário tenta driblar os mecanismos de controle de acesso e autenticação para conseguir associar-se a WLAN. A ameaça do acesso não autorizado é muito mais perigosa na WLAN devido ao fato que os seus dispositivos podem facilmente mudar de identidade (endereço MAC) na rede. Se a checagem do controle de acesso é baseada apenas na filtragem do endereço MAC, o adversário pode facilmente obter acesso não autorizado pela interceptação do tráfego da rede, criar uma lista de endereços MAC autorizados a acessar WLAN e, em seguida, falsificá-los.
- *Man-in-the-Middle (MITE)* – Apesar dos esforços realizados pela emenda 802.11w, ainda persistem problemas de segurança nos quadros de gerenciamento responsáveis pela associação entre as estações e o AP. Dessa forma, um adversário pode utilizar quadros de gerenciamento falsificados para desconectar uma STA legítima da rede e assumir suas conexões com AP por meio da falsificação do seu endereço MAC. A partir daí, o atacante receberá todos os quadros enviados para a STA falsificada e responderá em nome dela. A mesma situação pode ocorrer se o adversário obtiver o SSID de um AP legítimo, as estações conectadas ao falso AP terão suas informações transparentes para o atacante exceto se os dados estiverem criptografados. Ao contrário da interceptação da mensagem, a ameaça MITE necessita de uma participação direta do atacante na comunicação.
- Roubo de sessão – Este tipo de ameaça é semelhante ao MITE, contudo depois de derrubar a conexão da STA legítima e assumir suas conexões com o AP, o atacante certifica-se de que a STA desconectada não seja reassociada ao AP. Logo, o adversário utiliza esta sessão roubada muito tempo depois de tê-la usurpado da rede.
- Repetição de mensagem – Se não há proteção contra repetição de mensagem, um atacante pode monitorar passivamente o tráfego da WLAN e retransmitir determinadas mensagens interceptadas um tempo depois.
- Negação de Serviço (DoS) – Ataques DoS impedem a execução normal ou o gerenciamento da rede e seus recursos. Um atacante pode empregar dispositivos de bloqueio de rádio-frequência para causar interferência nos

canais de comunicação ou, simplesmente, utilizar os quadros de gerenciamento do tipo *Deauthentication* e *Diassociation* para obrigar estações legítimas a interromperem suas associações com a rede.

2.5 Evolução dos padrões de segurança numa rede IEEE 802.11

Antes das emendas IEEE 802.11i (onde se introduziu o *framework* Rede com Segurança Forte) e IEEE 802.11w (que assegurou para os quadros de gerenciamento *Deauthentication, Disassociation* e *Action* as propriedades de autenticidade da origem dos dados, detecção de *replay* e proteção), o padrão IEEE 802.11 sofria de sérios problemas de segurança. Esta Seção relatará os defeitos das WLAN's Pré-RSN (*robust security network* - RSN)e como as emendas IEEE 802.11i e IEEE 802.11w ajudaram a minimizar os problemas com segurança na rede IEEE 802.11.

2.5.1 Segurança Pré-RSN numa rede IEEE 802.11

Para satisfazer os princípios de segurança e combater as ameaças descritas, anteriormente, nesse trabalho, a especificação original IEEE 802.11 desenvolveu diversos mecanismos de segurança.

Confidencialidade dos dados

O protocolo WEP (*Wired Equivalent Privacy*) é utilizado para resguardar a confidencialidade nas redes IEEE 802.11 Pré-RSN. A proteção dos quadros de dados é realizada no WEP por meio do algoritmo criptográfico *Rivest Cipher* 4 - RC4 (SCHNEIDER, 1996), que gera uma chave de fluxo a partir de uma chave compartilhada de 40 bits e um vetor de inicialização (*initialization vector* - IV) de 24 bits. Infelizmente, esta técnica criptográfica apresentou-se muito vulnerável a ataques de força bruta devido ao tamanho reduzido da chave compartilhada (GILL, 2009). Mesmo o uso de chaves maiores não previne o resuso da chave de fluxo gerado por causa do tamanho pequeno do IV e da chave compartilhada ser estática (WALKER, 2000).

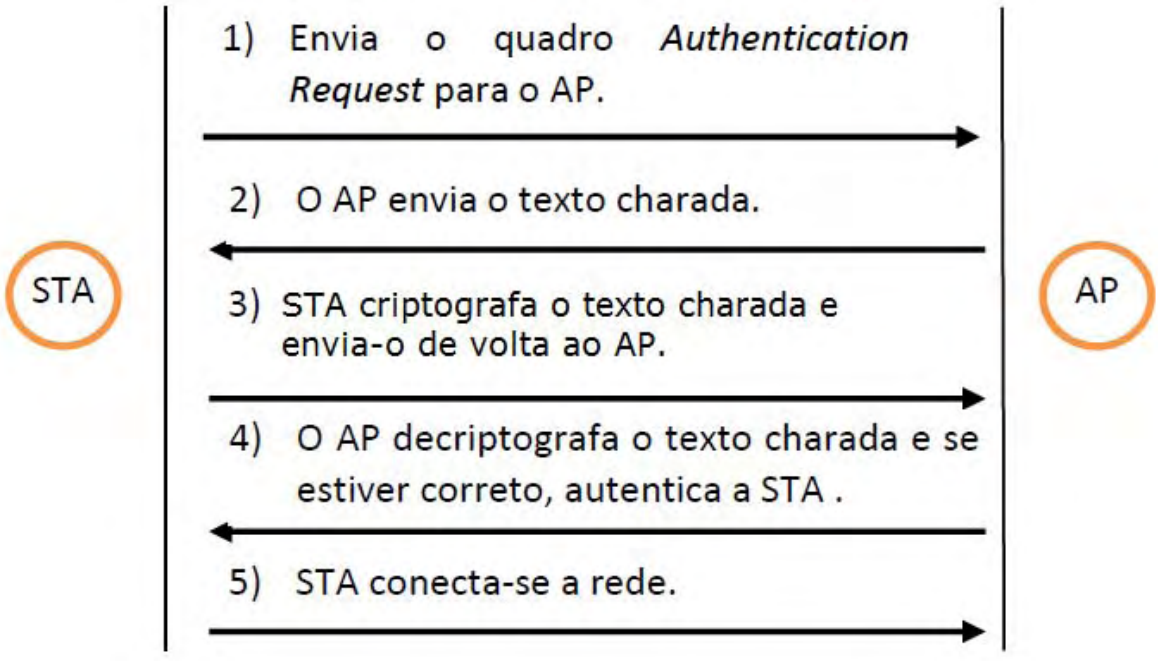
O protocolo WEP também não possui proteção contra ataques de repetição, uma vez que não há nenhum mecanismo de contador, *timestamp* ou outra informação temporal que possa ajudar na detecção de quadros repetidos (GILL, 2009). A falta de proteção contra repetição de mensagem contribui para interceptar dados de uma rede protegida em um período

mais curto de tempo. Portanto, é evidente que a proteção de confidencialidade oferecida pelo protocolo WEP é falha e não deve ser confiável.

Controle de acesso e autenticação

As redes IEEE 802.11 Pré-RSN aplicam dois métodos para autenticar as identidades dos dispositivos WLANs: *Open System Authentication* e *Shared Key Authentication*. O método *Open System Authentication* é obrigatório numa WLAN, enquanto o método *Shared Key Authentication* é opcional. Definitivamente, *Open System Authentication* é uma designação incorreta para esse método de autenticação, já que nenhuma verificação de identidade é realizada no processo de registro na rede por nenhuma das partes comunicantes. A Figura 9 mostra o funcionamento do método *Shared Key Authentication*, o qual se baseia num mecanismo de troca de respostas unilateral e utiliza a criptografia WEP para calcular a resposta. Embora este método de autenticação pareça ser mais seguro que o *Open System Authentication*, atualmente encontra-se em desuso devido às suas fragilidades.

Figura 9 - Funcionamento do método de autenticação *Shared Key Authentication*



Fonte: Adaptado de NETGEAR (2012).

Os mecanismos de controle de acesso aplicados nas redes IEEE 802.11 Pré-RSN estão limitados ao reconhecimento do SSID e ao uso de listas de filtragem com endereços MAC permitidos. Ambas as soluções são consideradas falhas e podem ser facilmente vencidas, já

que o SSID pode ser coletado livremente no tráfego da WLAN e a maioria dos adaptadores de rede WLAN podem ter seus endereços MAC trocados. Portanto, é apenas necessário roubar uma sessão legítima de uma STA pertencente a WLAN, fingir-se por ela e o mecanismo de controle de acesso fracassa (BITTAU; HANDLEY; LACKEY, 2006; GILL, 2009).

Integridade dos dados

O protocolo WEP utiliza um campo, chamado Valor de Checagem de Integridade (*integrity check value* - ICV), para proteger a integridade do quadro de dados durante a transmissão (IEEE, 1999). Este ICV é um valor criptografado (com RC4) resultante do método de checagem CRC-32 executado sobre o quadro a ser enviado. Infelizmente, o ICV está sujeito a ataques de *bit-flopping* (troca de bits) onde o atacante pode modificar um pacote sem detecção ou falsificar um quadro com ICV válido, sem o conhecimento da cifra de fluxo (GILL, 2009).

Disponibilidade

As redes IEEE 802.11 Pré-RSN não desenvolvem nenhuma operação contra ataques de DoS nas camadas PHY e MAC. O atacante pode causar interferência na camada PHY para tornar indisponíveis frequências na WLAN. A interferência também pode ser causada de forma não intencional quando dispositivos não-WLAN funcionam na mesma faixa de frequência. Na camada MAC, o atacante pode causar uma inundação na rede sem fio por meio da injeção de quadros falsificados, causando um DoS, ou empregar quadros de gerenciamento falsificados para deteriorar as associações seguras das estações WLAN (GILL, 2009).

2.5.2 WiFi Protected Access *(WPA)*

O protocolo WPA surgiu como um reforço temporário de segurança enquanto a emenda de segurança IEEE 802.11i fosse terminada, apesar disso este paliativo demonstrou-se tão ineficiente quanto o protocolo WEP.

Confidencialidade dos dados

Para prover confidencialidade, o WPA emprega um mecanismo denominado TKIP (*Temporal Key Integrity Protocol*), o qual utiliza também a cifra criptográfica RC4 (SCHNEIDER, 1996). Os principais avanços em comparação com o WEP são a inclusão de um espaço extendido no IV e uma função de embaralhamento de chave para construir chaves

por pacotes. Apesar disso, o algoritmo aplicado no embaralhamento de chave sofre do mesmo problema encontrado no WEP, o tamanho reduzido de chaves geradas pelo RC4, que acaba tornando muito vulnerável a ataques de força bruta (GILL, 2009; LASHKARI; MANSOOR; DANESH, 2009).

Integridade dos dados

O princípio da integridade é aplicado no WPA por meio de uma mensagem de verificação de integridade (*message integrity code* - MIC) onde se utiliza o algoritmo *Michael*. O protocolo WPA também implementa proteção contra ataques de repetição utilizando um sequenciamento de números por pacotes (LASHKARI; MANSOOR; DANESH, 2009).

Controle de acesso e autenticação

Dois mecanismos de autenticação são oferecidos pelo WPA. No primeiro método, a posse de uma chave pré-compartilhada (*pre-shared key* - PSK) é aplicada para autenticar os pontos e uma chave criptográfica de 128 bits e uma chave MIC de 64 bits também são derivadas da PSK para fornecer confidencialidade e integridade ao protocolo. No segundo método, os mecanismos IEEE 802.1X e *Extensible Authentication Protocol* (EAP) são usados para fornecer autenticação forte para os pontos e um mecanismo de rechaveamento fornece chaves dinâmicas de integridade e criptográficas como forma de combater as ameaças de ataques decorrentes do reuso de chaves. No entanto, a escolha por um método de autenticação mútua e criptografia forte são essenciais para proteger a autenticação IEEE 802.1X EAP de ataques de roubo de sessão e *man in the middle* - MITE (GILL, 2009).

Disponibilidade

Como no protocolo WEP, não há nenhum mecanismo de segurança para proteção de disponibilidade a WLAN oferecido pelo WPA. Ao contrário, a proteção de integridade proporcionada pela técnica MIC pode causar ataques de DoS na rede, relatada na situação onde:

> quando dois erros de MIC são detectados em menos de um minuto o AP cancela a conexão por 60 segundos e altera a chave de integridade. Portanto, com uma simples injeção de pacotes mal formados é possível fazer um ataque de negação de serviço (LINHARES; GONÇALVES, 2006, p. 12).

Além disso, o WPA também não oferece nenhuma proteção aos quadros de gerenciamento permitindo ataques de DoS a infraestrutura da rede.

2.5.3 Segurança RSN

A emenda IEEE 802.11i (IEEE, 2004), lançada em 2004, foi criada para solucionar os graves problemas existentes de confidencialidade e integridade nos mecanismos de segurança fornecidos pelo padrão original das redes WLAN. A principal inovação desta especificação é o conceito de Rede com Segurança Forte (RSN), que condiciona o acesso à rede WLAN apenas por meio de Associações de Rede com Segurança Forte (*robust security network association* - RSNA). A RSNA é uma conexão lógica entre duas entidades IEEE 802.11 estabelecida usando o esquema de gerenciamento de chaves *Four-way Handshake*.

Confidencialidade e integridade de dados

A mudança no algoritmo criptográfico é uma das grandes inovações introduzidas na emenda IEEE 802.11i, a partir dessa especificação utiliza-se o protocolo CCMP (*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*) para oferecer proteção de confidencialidade e integridade de dados, autenticação e contra ataques de repetição. O CCMP é baseado no algoritmo criptográfico AES (*Advanced Encryption Standard*) (NIST, 2001), o qual aplica o modo de operação CCM (*Counter with CBC-MAC*) (WHITING; HOUSLEY; FERGUSON, 2012) onde combina o método contador (*counter* - CTR) para fornecer confidencialidade de dados e o método de autenticação de mensagem CBC-MAC (*Cipher Block Chaining Message Authentication Code*) para prover integridade e autenticação. No protocolo CCMP é aplicado o conceito de chaves temporárias, semelhante ao TKIP, onde há uma hierarquia de chaves que derivam de uma chave mestra PMK (*Pairwise Master Key*). Além disso, o CCMP implementa um *nonce* único para cada quadro protegido por uma chave temporária para prevenir ataques de repetição. Este *nonce* é gerado a partir do número do pacote a ser criptografado (GILL, 2009).

Controle de acesso e autenticação

A emenda IEEE 802.11i utiliza o framework IEEE 802.1X (IEEE, 2001) para prover autenticação mútua e executar o controle de acesso numa WLAN. A autenticação IEEE 802.1X é composta de três componentes principais: um suplicante, um autenticador e um servidor de autenticação (*autentication server* - AS). Na WLAN, o suplicante são as estações,

o autenticador é o AP e um servidor RADIUS (RIGNEY; WILLENS, 2000) é utilizado como o servidor de autenticação. O autenticador meramente encaminha o tráfego de autenticação entre o suplicante e o AS. IEEE 802.1X emprega um controle de acesso baseado em porta para controlar o fluxo de dados entre o DS e as STAs. A autenticação EAP (ABOBA et al., 2004) ocorre por meio de porta não-controlada pelo autenticador e os quadros de dados não-EAP são submetidos na porta controlada IEEE 802.1X. Ao tráfego não-EAP somente é permitido ser encaminhado pela porta controlada se o solicitante tiver obtido sucesso no processo de autenticação com o AS. Assim, usando este modelo, o IEEE 802.1X bloqueia acesso não autorizado à WLAN. O protocolo EAP sobre LAN (EAPoL) é aplicado para encaminhar mensagens EAP entre o suplicante e o autenticador pelo meio sem fio, e o protocolo RADIUS (RIGNEY; WILLENS, 2000) é mais comumente utilizado na troca de mensagens EAP entre o autenticador e o AS. No término da autenticação EAP, a porta controlada do AP permanece bloqueada. Mesmo que a autenticação tenha sido um sucesso, a porta controlada somente é desbloqueada quando as chaves temporárias tenham sido negociadas e instaladas sobre a STA e o AP usando o esquema *Four-way handshake*.

A especificação IEEE 802.11i também permite autenticação empregando PSK. Se a chave pré-compartilhada está sendo utilizada a autenticação EAP não ocorre. Apesar disso, a técnica de gerenciamento de chaves *Four-way handshake* continua negociando as chaves temporárias e desbloqueia a porta controlada do AP.

Disponibilidade

Como nos protocolos WEP e WPA, a emenda IEEE 802.11i não possui nenhuma medida para minimizar ataques de DoS nas camadas MAC e PHY. Os quadros de controle e gerenciamento permanecem desprotegidos e para agravar a situação do problema mesmo quadros EAP e EAPoL não possuem proteção, podendo ser utilizados para lançar ataques de DoS contra a WLAN.

Gerenciamento de chaves e operações numa WLAN RSN

O estabelecimento de uma RSNA pode ser dividido em cinco fases distintas:

- **Fase 1 – Descoberta da rede**: Durante esta fase o AP anuncia seus serviços e política de segurança usando o elemento de informação RSN (RSN IE) em seus quadros *Beacon* e *Probe Response*. A STA utiliza essa informação para selecionar um AP com o qual deseja estabelecer uma associação segura. Durante esta fase, a STA e o AP negociam os protocolos de confidencialidade

e integridade para proteger o tráfego *unicast*, um método de autenticação mútua entre o AP e o AS, um esquema de gerenciamento de chave criptográfica e serviços de pré-autenticação.

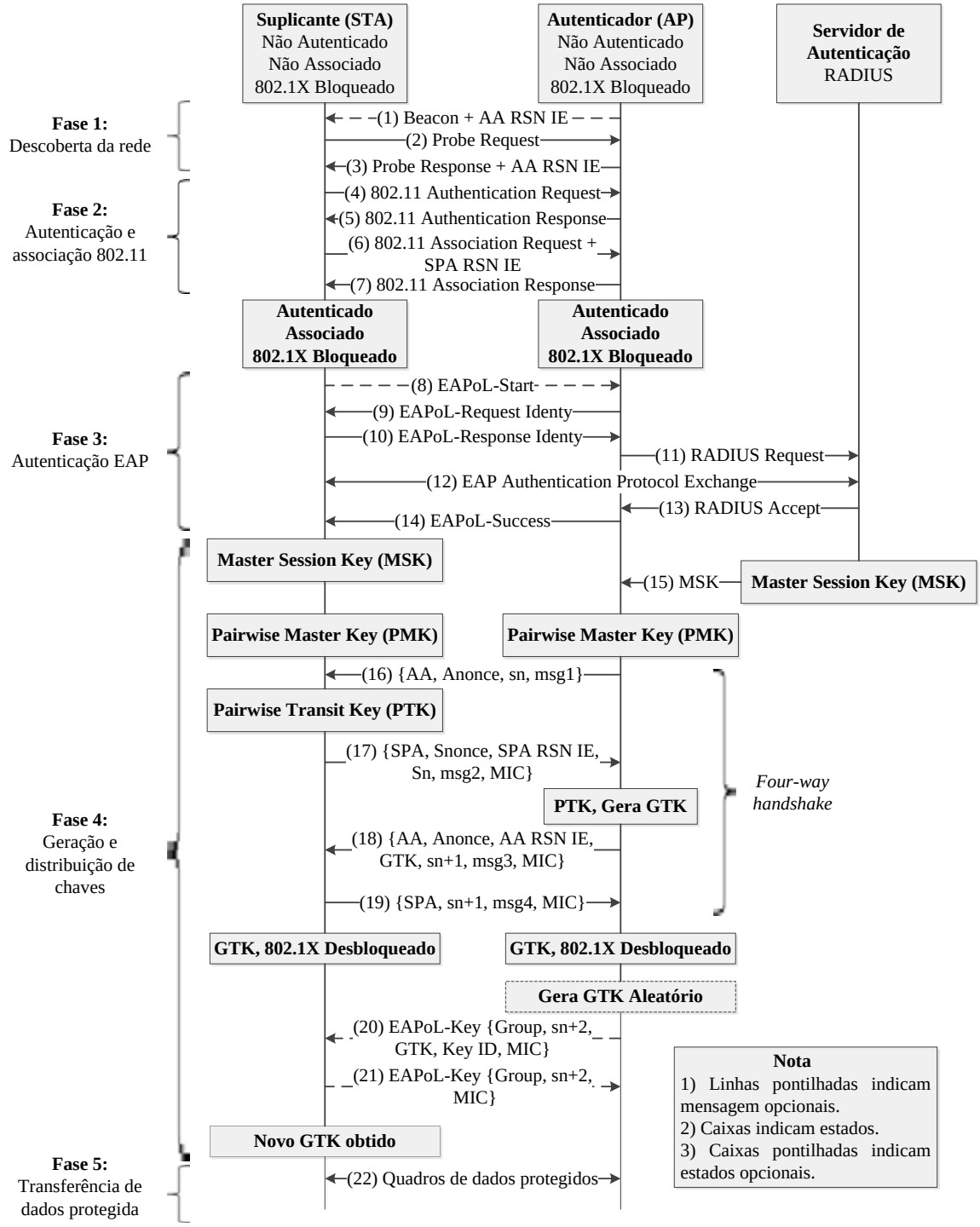
- **Fase 2 – Autenticação e Associação 802.11**: Para manter compatibilidade com as versões anteriores de hardware, o passo *open system authentication* é mantido antes da execução do *framework* de autenticação IEEE 802.1X.
- **Fase 3 – Autenticação EAP:** Durante esta fase, a STA e o AS fornecem suas identidades um ao outro. Durante a sessão EAP, o autenticador (AP) não participa da sua própria autenticação, ele meramente repassa as mensagens entre STA e AS.
- **Fase 4 – Geração e distribuição de chaves:** Durante esta fase, o AP e a STA executam diversar operações para criar e instalar chaves criptográficas sobre eles, exatamente por isso que as mensagens são trocadas apenas entre o AP e a STA.
- **Fase 5 – Transferência de dados protegida:** Todos os quadros de dados encaminhados entre o AP e a STA são criptograficamente protegidos empregando um grupo de cifras negociado na fase de descoberta da rede.

A Figura 10 descreve os passos desenvolvidos no estabelecimento de uma RSNA. Mensagens (1), (2) e (3) são relativas à fase de descoberta da rede, onde o AP anuncia periodicamente as suas informações de segurança nos quadros *beacon* ou responde quadros de *probe request* originados nas estações. As mensagens de (4) a (15) fazem parte das fases de autenticação e associação 802.11 e autenticação EAP. Antes da autenticação EAP, a STA tem que submeter-se ao estabelecimento de autenticação e associação simplificada com o autenticador (AP), representado pelas mensagens (4) e (7). Após a STA estar autenticada e associada, a autenticação EAP inicia a troca de mensagens entre a STA e o AS. O AP desempenha um papel secundário no processo de autenticação, pois apenas encaminha as mensagens de autenticação entre a estação e o AS. A autenticação pode ser iniciada pelo suplicante (aplicando o quadro *EAPoL-Start* – mensagem (8)) ou pelo AS (aplicando o quadro *EAP-Request Identity* – mensagem (9)). Depois que a autenticação EAP (mensagens (8) a (14)) tenha sido realizada com sucesso (usando o quadro *EAPoL-Success* – mensagem (14)) , a STA e o AS compartilham em comum um segredo chamado chave mestra de sessão (*master session key* - MSK). A estação utiliza esta MSK para gerar uma chave mestra pareada (*pairwise master key* - PMK) para comunicar-se de forma segura com o AP. Do outro lado, o

AS repassa sua MSK para o AP (mensagem (15)), a qual recebe esse segredo para gerar a mesma PMK criada pela estação. A autenticação EAP não ocorre se uma chave pré-compartilhada estática é empregada pela PMK.

As mensagens (16) a (21) são referentes à fase de geração e distribuição de chaves representada pelo esquema *four-way handshake*. Independente de o PMK ser gerado usando a autenticação EAP ou de uma PSK, o esquema *four-way handshake* (mensagens (16) a (19)) tem que ser executado para que o estabelecimento de uma RSNA seja considerado com sucesso. Este modelo de gerenciamento de chaves é empregado para confirmar a existência de uma PMK, confirmar a seleção de um conjunto de cifras criando e instalando uma chave temporária (*pairwise transit key* - PTK) para proteger a confidencialidade e integridade dos dados transferidos entre a STA e o AP. O autenticador também distribui um segredo conhecido como chave temporária de grupo (*group temporal key* - GTK) na mensagem (18) durante o *four-way handshake*. Após a fase de geração e distribuição de chaves, o AP e a STA compartilham uma chave temporária *unicast* PTK e uma chave temporária de grupo GTK, e a porta controlada IEEE 802.1X é desbloqueada para a transferência dos dados. Depois disso, no caso de aplicações *multicast*, o autenticador irá criar uma chave temporária de grupo GTK para distribuir entre os suplicantes da WLAN (mensagens (20) e (21)). Isto não ocorre apenas quando uma chave temporária GTK já tiver sido distribuída pelo *four-way handshake* na mensagem (18).

Figura 10 - Estabelecimento RSNA



Fonte: Adaptado de Gill (2009)

2.5.4 Emenda IEEE 802.11w

Os mecanismos de segurança apresentados nas emendas do padrão IEEE 802.11 relatados anteriormente são focados apenas em proteger os quadros de dados. Os quadros de controle e gerenciamento continuam desprotegidos e oferecendo para o atacante uma brecha para ataques contra a disponibilidade dos serviços de rede da WLAN. Junte-se a isso, a introdução de novas emendas (802.11r, 802.11k e 802.11v) que acrescentam aos quadros de gerenciamento novas informações relevantes sobre a rede sem fio. Com esse intuito foi ratificada, em 2009, a emenda IEEE 802.11w (IEEE, 2009), onde o principal objetivo é proteger os quadros de gerenciamento para que as informações relevantes sobre a rede sem fio contidas nesses quadros, não sejam empregadas em ataques contra a disponibilidade da WLAN.

A emenda IEEE 802.11w introduz o conceito de quadro de gerenciamento seguro (*robust management frame* - RM), que agrega os seguintes princípios de segurança na WLAN (AHMAD; TADAKAMADLA, 2011; IEEE, 2009):

- Autenticidade da origem dos dados – Mecanismo pelo qual uma STA receptora de um quadro RM, é capaz de identificar qual é a STA transmissora desse quadro. Esta propriedade é necessária para prevenir que um atacante se apresente como uma estação legítima. A autenticidade da origem dos dados é aplicada apenas em quadros RM *unicast*.
- Detecção de repetição – Este princípio determina uma forma pela qual uma estação receptora de quadro RM verifica se este quadro é repetido ou não.
- Proteção do quadro de gerenciamento (*management frame protection* - MFP) – Este mecanismo é solicitado numa associação segura (RSNA) para proteger os quadros RM contra falsificação e interceptação de dados. Regras MFP são empregadas somente depois que a chave PTK para proteção de quadros *unicast* seja estabelecida. No caso de quadros *broadcast/multicast*, as regras são aplicadas apenas depois que a chave de grupo IGTK (*Integrity Group Temporal Key*) seja instalada. A chave IGTK tem como função principal proteger a integridade da mensagem dos quadros RM endereçados a um grupo de estações. Quadros RM transmitidos ou recebidos por uma estação, antes da instalação das chaves temporárias, estão desprotegidos.

RM é um conjunto de quadros de gerenciamento que podem ser protegidos pelo serviço de MFP. Os quadros de gerenciamento *Deauthentication*, *Diassociation* e *Action* representam os quadros RM numa WLAN.

Confidencialidade e integridade de dados

Na emenda IEEE 802.11w, a proteção de confidencialidade e integridade de dados também emprega o modelo de hierarquia de chaves desenvolvido na emenda IEEE 802.11i. Quadros RM *unicast* são criptografados empregando a chave temporária PTK. A primeira inovação introduzida pela emenda 802.11w é a geração de uma nova chave temporária IGTK, responsável pela verificação da integridade e detecção de repetição em quadros RM *broadcast/multicast*.

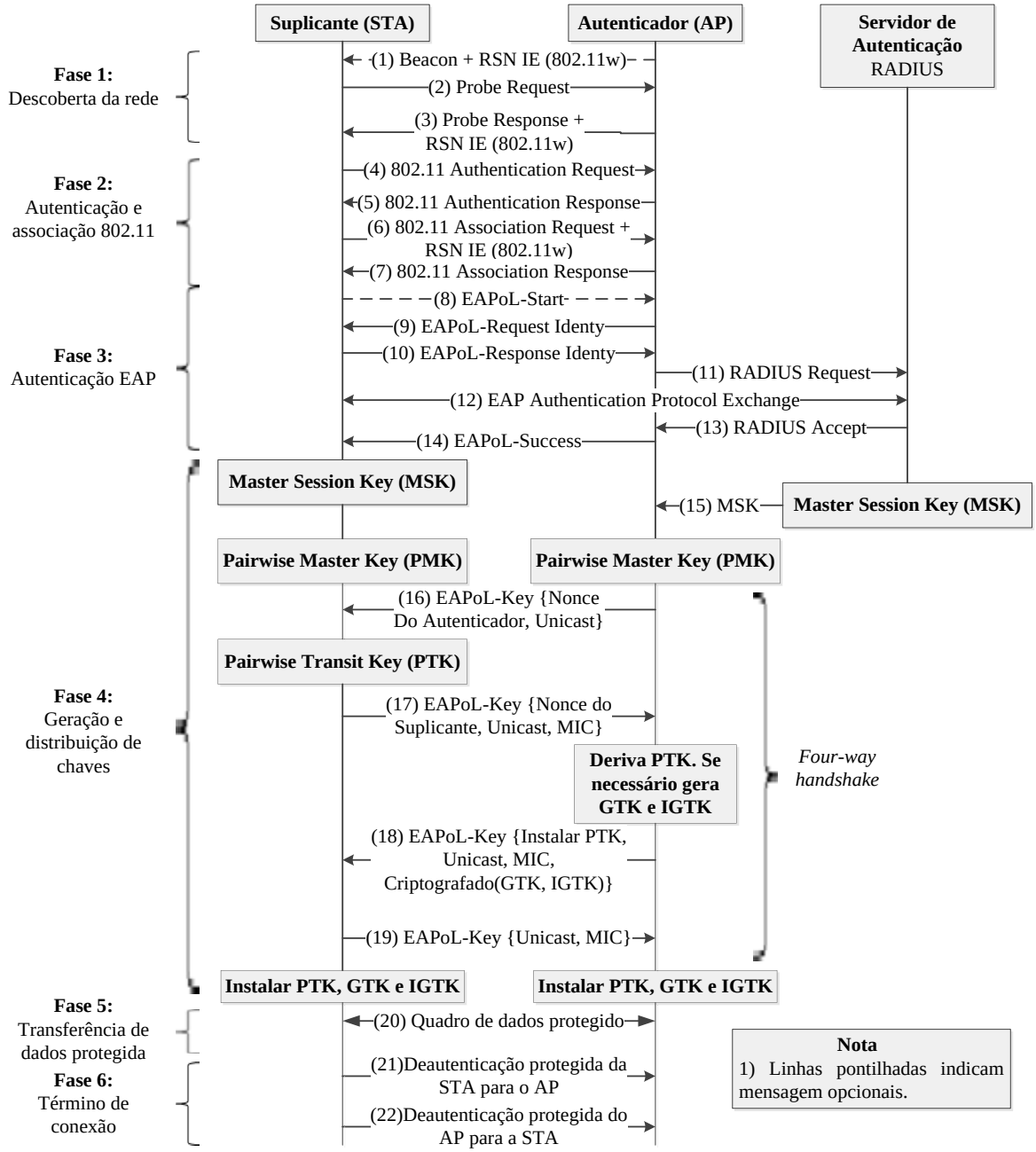
A chave IGTK é baseada no protocolo *Broadcast/Multicast Integrity Protocol* - BIP (IEEE, 2009), onde o algoritmo criptográfico AES-128bits no modo de operação CMAC (*Block Cipher based Message Authentication Code*) é aplicado para prover verificação de integridade e detecção de repetição para os quadros RM enviados para os suplicantes associados ao AP. Todas as estações associadas a um AP, que suporta a emenda IEEE 802.11w, recebem incluso no corpo do quadro RM *broadcast/multicast* um campo conhecido como MMIE (*Management MIC Information Element*), contendo os subcampos IGTK, número do pacote IGTK (*IGTK packet number* - IPN) e o MIC.

Autenticação e controle de acesso

O estabelecimento de uma associação segura entre dispositivos habilitados com a emenda IEEE 802.11w é muito semelhante com o que ocorre no RNSA, exceto por algumas alterações realizadas na máquina de estados. A Figura 11 mostra o estabelecimento e término RSNA numa rede WLAN com suporte à emenda IEEE 802.11w. A primeira mudança a ser comentada é a introdução de dois campos, MFPR (*Management Frame Protection Required*) e MFPC (*Management Frame Protection Capable*), no campo RSN IE para anunciar se o dispositivo (STA ou AP) exige ou não o suporte à emenda IEEE 802.11w para o estabelecimento de uma associação segura. Os quadros *beacon* e *probe response* transmitidos pelo AP são utilizados para informar as estações se a associação a ser estabelecida deve suportar a emenda 802.11w. A estação anuncia sua compatibilidade com a emenda 802.11w usando o quadro *(Re)Association Request* na fase de autenticação e associação 802.11. Todas as mensagens restantes trocadas são semelhantes ao estabelecimento RSNA, apresentado na Figura 10, exceto pela mensagem (18) na qual o AP envia o GTK junto com o IGTK para a

STA e pelas mensagens (21) e (22) onde o término da conexão é realizado usando quadros RM protegidos, as quais são mensagens específicas (ilustradas na Figura 11) numa rede WLAN com suporte a emenda IEEE 802.11w.

Figura 11 - Estabelecimento e término RSNA numa rede WLAN com suporte a emenda IEEE 802.11w.



Fonte: Adaptado de Ahmad e Tadakamadla (2011).

Disponibilidade

A emenda 802.11w introduz um procedimento de verificação de estado de segurança (*Security Association Query – SA Query*) para solucionar uma falha no término da associação segura existente nas redes WLAN RSN, que leva a problemas de disponibilidade na rede sem fio. O procedimento *SA Query* insere dois novos quadros RM: *SA query request* e *SA query response*.

SA query request é enviado por uma AP sempre que há necessidade de sincronizar o estado de SA com uma estação associada. Um AP envia um quadro *SA query request* após ter recebido um quadro *(Re)association request* de um cliente cujo estado SA está presente no AP. Se a estação está ativa e seu estado de SA ainda é válido, então a estação decriptografa o quadro utilizando seu PTK e transmite o quadro *AS query response* para o AP. Isto ajuda o AP em dois cenários. No primeiro cenário onde um atacante tenta remover um estado de SA de um cliente legítimo pelo envio de quadros *(Re)association request* falsificados. No segundo cenário, o cliente sem fio reinicializa e tenta reestabelecer uma nova associação segura com o AP.

Outra inovação introduzida pela emenda IEEE 802.11w é a inserção do campo TIE (*Time Element Information*) no quadro de gerenciamento *(Re)association response*. O TIE tem o propósito de informar a estação comunicante que o AP encontra-se ocupado no momento para completar o procedimento SA query e depois de quanto tempo o AP vai estar pronto para aceitar a solicitação de associação desta estação comunicante. Isto é feito por meio de um subcampo chamado valor de intervalo de *timeout* (*timeout interval value* - TIV) ou tempo de regresso.

Apesar de todo avanço empregado pela emenda IEEE 802.11w na proteção dos quadros de gerenciamento, os quadros de controle continuam desprotegidos. Deixando assim, uma porta aberta para um atacante lançar um ataque de DoS contra a disponibilidade da rede sem fio. Além disso, a proteção de disponibilidade na emenda IEEE 802.11w está restrita num pequeno grupo de quadros de gerenciamento (*deauthentication*, *diassociation* e *action*) e vinculada à geração e instalação das chaves temporárias PTK e IGTK (AHMAD; TADAKAMADLA, 2011).

2.6 Conclusões

A evolução das emendas de segurança (IEEE 802.11, IEEE 802.11i e IEEE 802.11w) propostas para uma rede WLAN demonstra todo o esforço realizado pela comunidade

científica para fornecer num ambiente sem fio os princípios de segurança existentes numa rede confinada. Contudo, ainda persistem vulnerabilidades que colocam em risco a segurança de uma rede WLAN, principalmente com relação à disponibilidade dos serviços.

Uma das principais vulnerabilidades referente ao princípio da disponibilidade numa rede WLAN refere-se ao fato de os mecanismos de segurança implantados pelas emendas IEEE 802.11i e IEEE 802.11w apenas entrarem em execução após a geração e instalação das chaves temporárias PTK e IGTK, deixando assim desprotegidos os quadros de gerenciamento envolvidos nas fases anteriores de uma associação segura (AHMAD; TADAKAMADLA, 2011).

Desta forma, surge a necessidade de se empregar outras ferramentas de segurança que auxiliem na proteção dos serviços de rede oferecidos pela WLAN aos seus usuários legítimos. Apresenta-se no próximo Capítulo o referencial teórico de um instrumento auxiliar na proteção da disponibilidade de uma rede IEEE 802.11, que são os sistemas detectores de intrusão.

3 VISÃO GERAL DE SISTEMAS DETECTORES DE INTRUSÃO

Como foi discutido no Capítulo 2, apesar de todas as medidas de segurança implantadas pelas emendas IEEE 802.11i e IEEE 802.11w, a WLAN ainda sofre de várias vulnerabilidades e ataques. Assim, torna-se imperativo o uso de sistemas detectores de intrusão que monitorem constantemente as ondas de rádio, de forma a detectar possíveis explorações destas vulnerabilidades. O IDS pode agir como uma segunda camada de defesa em mecanismos de segurança numa WLAN e ajudar a garantir que nenhum tráfego malicioso ou atividade não autorizada venha ocorrer na rede.

Neste Capítulo apresenta-se o referencial teórico sobre IDS, descrevendo-se os seguintes temas: conceituação de um IDS, componentes relacionados a ele, classificação segundo o tipo de intrusão, comportamento da detecção, abordagem da detecção e tipo de sistemas monitorados. A seguir, relata-se a metodologia para avaliação de um IDS e por último, os principais trabalhos relacionados de IDS's empregados em redes sem fio infraestruturadas (IEEE 802.11).

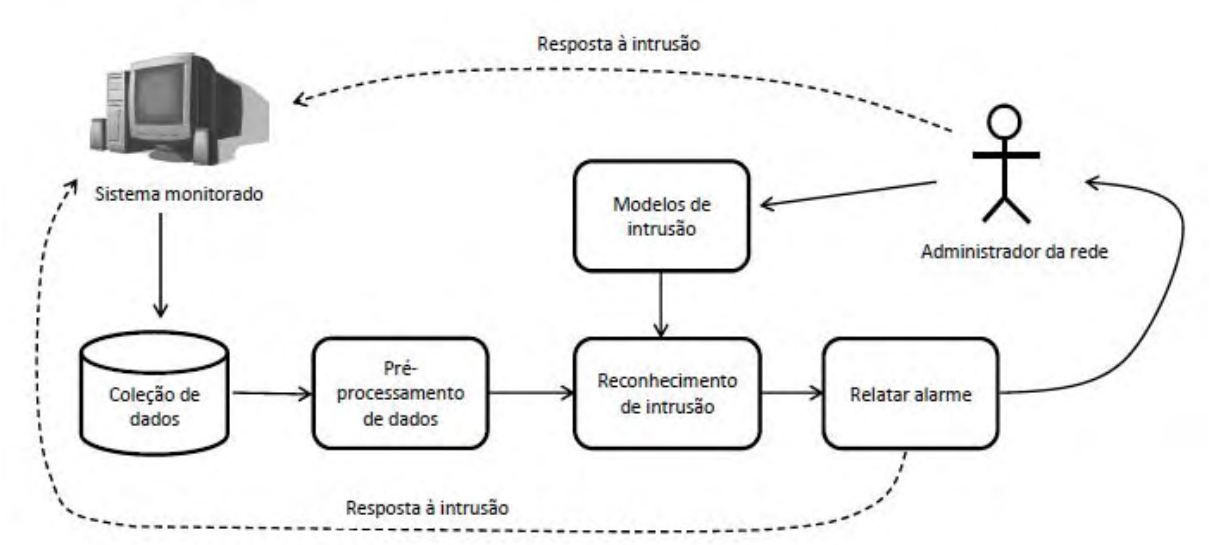
3.1 Conceitos básicos de um IDS

IDS é o processo de detecção e identificação de atividade não autorizada ou imprópria no sistema (SOBH, 2006). O objetivo de um IDS é identificar ocorrências decorrentes de brechas na segurança capazes de comprometer a integridade dos recursos ou serviços (SOBH, 2006).

Um IDS monitora constantemente os eventos que se sucedem num sistema, e decide se estes eventos são sintomas de um ataque ou constituem o uso legítimo do sistema (WU; BANZHAF, 2010).

A Figura 12 descreve a organização de um IDS, onde se ilustra duas fases bem distintas. Na primeira fase, dados são coletados no sistema monitorado, que logo após são tratados no componente de pré-processamento de dados, para que os registros compartilhem um mesmo padrão de instâncias a serem analisadas posteriormente na fase de reconhecimento de intrusão. Na segunda fase, os registros coletados e tratados são comparados a modelos de intrusão gerados a partir de assinaturas de ataques bem conhecidos ou de um perfil de comportamento normal ou esperado do sistema monitorado, que gera um relatório para o administrador de rede com os registros que possuem comportamento intrusivo.

Figura 12 - Organização de um sistema detector de intrusão generalizado.



Fonte: Adaptado de Wu e Banzhaf (2010).

3.2 Classificação de sistemas detectores de intrusão

Um IDS pode ser classificado conforme os seguintes critérios: tipos de intrusão, comportamento da detecção, metodologia da detecção e tipos de sistemas monitorados (SOBH, 2006).

Com relação ao tipo de intrusão, o IDS pode ser classificado em intrusão externa, em que o ataque parte de um elemento externo a rede alvo, e intrusão interna, em que o ataque tem origem a partir de um nó pertencente à própria rede alvo.

O comportamento da detecção reconhecida por um IDS pode ser classificado nas seguintes categorias: tentativa de invasão, ataques de personificação, penetração do sistema de controle de segurança, perdas, negação de serviço e uso malicioso.

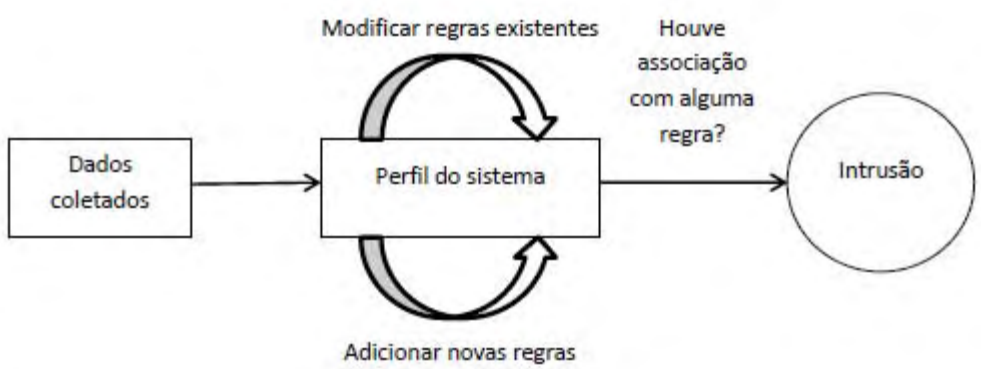
O IDS pode ser dividido em duas categorias baseado na fonte dos dados utilizada para a detecção de intrusão: *Network Intrusion Detection System* (NIDS) – analisa eventos de rede para detecção de intrusão e *Host based Intrusion Detection System* (HIDS) – utiliza eventos produzidos pela estação para detecção de intrusão (SOBH, 2006).

Em geral, os IDSs enquadram-se em duas classes, de acordo com o método de detecção utilizado, denominadas: detecção por assinaturas e detecção por anomalia.

A primeira abordagem (detecção por assinaturas), ilustrada na Figura 13, reconhece intrusos pela associação entre os registros auditados e descrições pré-definidas de comportamento intruso. Por isso, intrusões bem especificadas podem ser eficientemente

detectadas com uma taxa de falso alarme muito baixa. Por essa razão, esta abordagem é amplamente utilizada na maioria dos sistemas comerciais (WU; BANZHAF, 2010). Contudo, o comportamento intruso geralmente é mutável e evolui continuamente. A detecção por assinaturas falha facilmente quando submetida a reconhecer intrusões não especificadas na sua base de conhecimento. Uma forma de solucionar é regularmente atualizar a base de conhecimento, mas isso é uma tarefa cara e trabalhosa devido à necessidade de se criar especificações que englobem uma grande variação de ataques e, ao mesmo tempo, não sejam associadas a nenhuma atividade não intrusiva (SOBH, 2006).

Figura 13 - Um mecanismo típico de detecção por assinaturas.



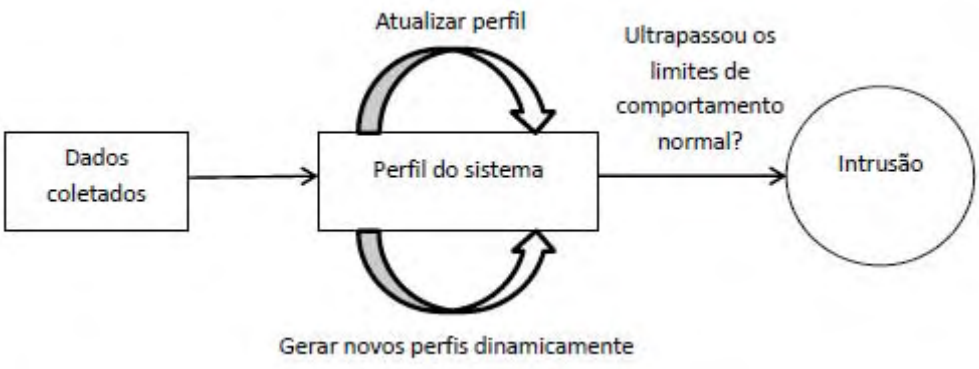
Fonte: Adaptado de Sobh (2006).

As assinaturas são derivadas a partir de ataques conhecidos ou vulnerabilidades e representam características de atividade intrusiva presente no ataque. Estas assinaturas podem ser fornecidas ao IDS para detecção de intrusão, de duas formas (GILL, 2009):

- Assinaturas simples – as atividades intrusivas podem ser especificadas por meio de padrões de bits ou expressões regulares que representam unicamente as propriedades bem conhecidas de ataques.
- Modelos de transição de estado – o ataque é especificado por meio de uma máquina de estados, onde cada estado representa uma característica única da intrusão, que ao atingir o estado final indica a existência de atividade intrusiva.

A Figura 14 apresenta o mecanismo de detecção por anomalia, o qual parte do princípio de que o comportamento anômalo é raro e diferente do comportamento normal. Assim, o IDS constrói modelos para comportamento normal e caracteriza como atividade intrusiva todo tráfego observado que desvia destes modelos.

Figura 14 - Um mecanismo típico de detecção por anomalia.



Fonte: Adaptado de Sobh (2006).

Os eventos de interesse para um IDS baseado em anomalia são os desvios de uma especificação de comportamento normal ou esperado, e podem ser definidos das seguintes formas (GILL, 2009):

- Modelos estatísticos – a abordagem de modelagem estatística é amplamente empregada em eventos de interesse para IDS baseado em anomalia. Variáveis e características são medidas sobre certos períodos de tempo pelo IDS e agrupada estatisticamente para gerar uma base de referência do comportamento normal ou esperado do *host* ou da rede monitorada. Se o desvio da base de referência exceder um limite pré-definido, o IDS lançará um alerta sobre a possível ocorrência de atividade intrusiva. Esta abordagem requer um período de treinamento pelo IDS para que este possa aprender qual é o comportamento não intrusivo definido pela entidade monitorada. A presença de eventos de intrusão na fase de treinamento pode levar o IDS a tratar comportamento anômalo como comportamento normal e, por consequência, aumentar o número de falsos negativos. A escolha das variáveis e características corretas para gerar a base de referência é, geralmente, uma tarefa árdua, e selecionar atributos errados pode ocasionar alta taxa de falsos positivos.
- Modelos baseados em especificação – detecção por anomalia baseada em especificação não depende de uma fase de treinamento nem de coletar dados que representem o comportamento não intrusivo de um sistema monitorado. Nesta abordagem, especificações implementadas pela política de segurança da instituição descrevem o comportamento de atividades legítimas para a rede. Como este método é baseado em comportamento legítimo, não gera falsos

alarmes quando uma atividade excepcional (mas legítima) ocorre na rede, tal como: quando algum aplicativo tem suas requisições hibernadas por um determinado período e depois retornam a trafegar. Dessa forma, os ataques são detectados como desvios desta conduta esperada pelos programas em execução na rede.

A principal vantagem da detecção por anomalia é a capacidade de reconhecer novos ataques. Contudo, a definição do limite entre um comportamento normal e anômalo é uma das maiores dificuldades no uso deste tipo de IDS devido à deficiência de amostras anômalas na fase de treinamento (WU; BANZHAF, 2010). Outra dificuldade é adaptar-se a uma constante mudança no comportamento normal, ainda mais quando se tem uma detecção por anomalia dinâmica. Por isso, pode ocorrer um alto custo computacional devido ao rastreamento do tráfego e a atualização dos limites de intrusão.

3.3 Avaliação de IDS

Para avaliar a eficiência de uma metodologia de IDS é necessário, primeiramente, calcular uma estrutura de dados conhecida como matriz de confusão (WU; BANZHAF, 2010), que apresenta informações sobre as classificações corretas e previstas realizadas pelo módulo de reconhecimento de intrusão. O desempenho do IDS, normalmente, é avaliado usando os dados contidos nesta matriz. A Tabela 1 é uma representação da matriz de confusão do problema de detecção de intrusos.

Tabela 1 - Matriz de confusão do problema de detecção de intrusos

		Classe prevista	
		Classe negativa (Normal)	Classe positiva (Anomalia)
Classe real	Classe negativa (Normal)	Verdadeiro Negativo (TN)	Falso Positivo (FP)
	Classe positiva (Anomalia)	Falso Negativo (FN)	Verdadeiro Positivo (TP)

Fonte: Adaptado de Wu e Banzhaf (2010).

As entradas da matriz de confusão possuem os seguintes significados no contexto do nosso estudo: Verdadeiro Positivo (TP) - identifica uma atividade intrusiva corretamente; Verdadeiro Negativo (TN) - identifica uma atividade não-intrusiva corretamente; Falso

Positivo (FP): identifica uma ação não-intrusiva como sendo intrusiva; Falso Negativo (FN): identifica uma atividade intrusiva como sendo não-intrusiva.

Para avaliar o desempenho do IDS, diversas métricas têm sido calculadas a partir das entradas oferecidas pela matriz de confusão, entre as mais empregadas pode-se citar (WU; BANZHAF, 2010):

- Taxa de detecção ($\frac{TP}{FN+TP}$) - proporção de atividades intrusas classificadas corretamente;
- Taxa de falsos alarmes ($\frac{FP}{TN+FP}$) - proporção de atividades normais classificadas incorretamente como intrusas;
- Exatidão global ($\frac{TN+TP}{N}$) – proporção da quantidade de previsões que foram classificadas corretamente;
- Precisão ($\frac{TP}{FP+TP}$) – proporção de atividades intrusas previstas que foram corretamente identificadas.

3.4 Trabalhos relacionados

Com relação aos modelos de detecção de intrusos aplicados em redes locais sem fio, há vários tipos de abordagens relatadas na literatura. Khoshgoftaar, Nath, Zhong e Seliya (2005) utilizam uma abordagem que aplica o algoritmo de agrupamento *k-means* para reunir os registros coletados por meio de SNMP numa rede WLAN real em *clusters*. A seguir, analisa-se a distância entre o *cluster* com a maior quantidade de registros e o restante dos clusters. Define-se uma distância de corte ao maior *cluster*, e aqueles grupos que estão antes desse limite são considerados atividade normal. Caso contrário, é atividade intrusa. Outra técnica de detecção de intrusos, apresentada em Gill, Smith e Clark (2006), utiliza uma máquina de transição de estados e um conjunto de restrições para identificar intrusão e monitorar o cumprimento das políticas de segurança numa rede WLAN. De forma similar, Fayssal, Hariri e Al-Nashif (2007) apresentam uma proposta de detecção de intrusos que avalia atividade anômala a partir de medidas da rede sem fio relacionadas ao canal utilizado, a potência do sinal e as informações do pacote, empregando técnicas de mineração de dados (análise multivariada).

É apresentada por Tang, Sun e Kong (2009) uma proposta de detecção de intrusos que identifica e defende-se contra ataques de homem ao meio e inundação TCP SYN pela análise dos canais e da informação do pacote.

Os artigos publicados por Mar, Yeh e Hsiao (2010) e Makanju, LaRoche e Zincir-Heywood (2007) abordam a detecção por assinaturas voltada para ataques ocasionados por deautenticação na subcamada MAC de uma rede WLAN. Em Mar, Yeh e Hsiao (2010) é utilizado um sistema de inferência neuro-*Fuzzy* adaptativo como mecanismo de aprendizagem. E Makanju, LaRoche e Zincir-Heywood (2007) utilizam a programação genética para o reconhecimento dos ataques.

Os autores Haddadi e Sarram (2010) apresentam uma estratégia de IDS híbrida e multi-agente que monitora os canais de comunicação e implementam três máquinas para detectar diferentes tipos de intrusão. Danzinger e Neto (2010) também relatam uma proposta de IDS híbrida e multi-agente, com o diferencial no mecanismo de aprendizagem, que utiliza sistemas imuno-artificiais e um classificador bayseano como componentes de detecção.

A proposta de Liu, Tian e Li (2006) aplica redes neurais de crescimento dinâmico para a detecção de atividades anômalas numa rede WLAN.

El-Khatib (2010) mostra que a otimização do conjunto de atributos de uma rede WLAN tem um impacto significativo na eficiência e precisão de um IDS.

O IDS proposto nesta tese aplica na fase de pré-processamento de dados, uma técnica de seleção de atributos baseada no coeficiente Kappa e na rede neural ARTMAP *Fuzzy*, para extrair os atributos mais significativos da base de treinamento e gerar um subconjunto ótimo de atributos que será empregado para treinar o módulo de reconhecimento de intrusão do IDS. A rede neural ARTMAP *Fuzzy* é utilizada como o algoritmo de detecção de intrusos, onde primeiramente aplica-se uma metaheurística de otimização por enxame de partículas para determinar uma configuração de parâmetros ótima que maximize a identificação de ataques de negação de serviço numa rede WLAN real com suporte a emenda de segurança IEEE 802.11i.

3.5 Conclusões

Os métodos de detecção num IDS têm suas vantagens e desvantagens, que torna a definição por um modelo uma tarefa complicada. A detecção por assinatura possui na rapidez sua grande prerrogativa, pois as especificações dos ataques são previamente conhecidas, mas uma pequena alteração nesta assinatura apreendida prejudica a identificação de atividades intrusivas. Por outro lado, a detecção por anomalia possui seu ponto forte na caracterização do comportamento normal esperado, pois o sucesso da classificação correta não fica ligado às assinaturas previamentes conhecidas, tornando-a mais abrangente quando novos tipos de

ataques surgirem, mas a definição do comportamento esperado pelos programas em execução numa rede não é tão simples de ser modelado devido à dinamicidade dos eventos.

No próximo Capítulo serão apresentados o embasamento teórico utilizado na metodologia de IDS proposta nesta tese (seleção de atributos, coeficiente Kappa, otimização por enxame de partículas, rede neural ARTMAP *Fuzzy*) e uma descrição sucinta do mecanismo de funcionamento desta nova arquitetura.

4 KAPPA-PSO-ARTMAP FUZZY: UMA METODOLOGIA PARA DETECÇÃO DE INTRUSOS EM REDES DE COMPUTADORES

Neste Capítulo são apresentados, primeiramente, os pilares teóricos (seleção de atributos, coeficiente Kappa, redes neurais ARTMAP *Fuzzy* e otimização por enxame de partículas) que fundamentam a metodologia de IDS proposta neste trabalho. A seguir, descreve-se uma visão geral desta sugestão de arquitetura, apresentando como os referenciais teóricos são aplicados neste sistema de detecção de intrusos.

4.1 Seleção de atributos

Em domínios mais complexos de classificação de padrões, algumas características podem ser redundantes, visto que a informação contida nelas podem já existir em outros atributos. Esta redundância de informação pode aumentar o custo computacional do IDS, uma vez que a quantidade de atributos existentes na base de treinamento influencia o número de processamentos necessários para executá-la (TSAI et al., 2009). A seleção de atributos enfrenta este problema, buscando um subconjunto de atributos que melhor representa os padrões de comportamento existente na base de treinamento.

A Figura 15 ilustra o fluxograma de um algoritmo de seleção de atributos, que normalmente é composto de três componentes (LIU; YU, 2005):

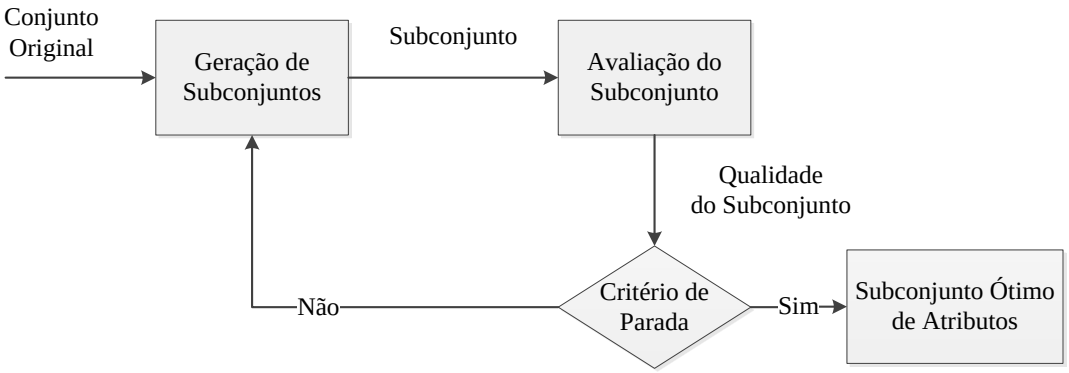
• Geração de subconjunto - responsável por gerar os subconjuntos candidatos para a avaliação. O mecanismo de geração pode começar: sem nenhum atributo, com todos os atributos, ou com um subconjunto aleatório de atributos. Nas duas primeiras situações, os atributos são adicionados e removidos sequencialmente, enquanto no último caso, os atributos podem ser tanto adicionados ou removidos sequencialmente quanto gerados aleatoriamente.

• Avaliação de subconjunto – calcula a qualidade do subconjunto produzido pelo módulo de geração e compara esta medida computada com o melhor valor obtido por um subconjunto candidato. Se a resposta for afirmativa então o novo subconjunto gerado torna-se o melhor valor pessoal dos subconjuntos candidatos.

• Critério de parada – determina quando o processo de seleção de atributos deve terminar. Esta condição pode ocorrer: quando a busca se encerra; ao alcançar um limite predeterminado (quantidade mínima de atributos, quantidade máxima de iterações); ao

adicionar ou remover algum atributo que não produz uma melhora na qualidade do subconjunto candidato; e o subconjunto gerado possui uma taxa de erro considerada boa para uma determinada tarefa.

Figura 15 - Fluxograma de um algoritmo de seleção de atributos.



Fonte: Adaptado de Liu e Yu (2005).

Há três formas de implementação de seleção de atributos: filtro, que depende das características gerais dos dados para avaliar e selecionar subconjuntos de atributos; envoltório, que adota algoritmos de aprendizagem de máquina e utiliza métricas de desempenho (precisão, exatidão global, coeficiente Kappa) destes classificadores como função de avaliação para medir a importância de um ou vários atributos, com o objetivo de construir um subconjunto ótimo; e híbrida, que procura levantar as melhores características dos métodos filtro e envoltório, explorando-as em diferentes critérios de avaliação no processo de busca pelo subconjunto ótimo (GUYON; ELISSEEFF, 2003; LIU; YU, 2005).

4.1.1 Geração de subconjunto

A geração de subconjunto é essencialmente uma busca heurística, pois especifica em cada estado do espaço solução da pesquisa um subconjunto candidato para avaliação (LIU; YU, 2005). A natureza deste processo é determinada por dois princípios básicos. O primeiro princípio define o ponto (ou pontos) de partida da investigação que por sua vez determina a direção da pesquisa. Definido o ponto de partida, deve-se escolher a estratégia de busca a ser utilizada para percorrer o espaço solução.

Uma busca exaustiva no espaço solução desencadeia um processamento exponencialmente proibitivo para o IDS, pois o custo computacional de uma base de treinamento com N atributos (mesmo N assumindo um valor médio) é $O(2^N)$. Devido a isso,

métodos de busca mais sofisticados têm sido desenvolvidos para tratar este problema. Eles podem ser categorizados em (LIU; YU, 2005):

- Completa – garante encontrar um subconjunto ótimo de acordo com a função de avaliação aplicada. Apesar da busca completa possuir um espaço solução na ordem de $O(2^N)$, a quantidade de subconjuntos candidatos avaliados é mais reduzida pois utiliza métodos heurísticos para reduzir este espaço solução, sem que isto comprometa a qualidade da busca pelo subconjunto ótimo. As principais implementações de busca completa aplicadas em seleção de atributos são: *branch and bound* e *beam search*.
- Sequencial - a cada iteração deste tipo de busca, a geração de subconjuntos dar-se-á incrementalmente (adicionando ou removendo atributos). Os algoritmos de busca heurística são de fácil implementação e velozes em gerar resultados, devido a isso a ordem do espaço solução é $O(N^2)$ ou menor. As principais implementações de busca heurística aplicadas em seleção de atributos são: *sequential forward selection*, *sequential backward selection*, *plus-l minus-e selection*, busca bidirecional, *sequential floating selection*.
- Aleatória - emprega a aleatoriedade para fugir de ótimos locais no espaço solução e a otimalidade do subconjunto selecionado depende dos recursos disponíveis no IDS. A ordem do espaço solução na busca aleatória é $O(2^N)$, apesar da complexidade exponencial, o uso de técnicas de obtenção de soluções aproximadas produzem uma redução na quantidade de subconjuntos avaliados. As principais implementações de busca aleatória aplicadas em seleção de atributos são: *random generation plus sequential selection*, algoritmos genéticos e *simulated annealing*.

4.1.2 Avaliação do subconjunto

A cada nova geração de um subconjunto candidato deve ser realizada uma apreciação por meio de uma função de avaliação. A qualidade deste subconjunto sempre é definida por um determinado critério, que pode ser categorizado segundo sua dependência em algoritmos de aprendizagem. Os critérios de avaliação podem ser enquadrados em (LIU; YU, 2005):

- Independente – avalia a qualidade de um subconjunto candidato ou atributo pela exploração das características intrínsecas da base de treinamento, sem

envolver qualquer algoritmo de aprendizagem. Este tipo de critério de avaliação é aplicado em métodos com filtros. Os principais critérios de avaliação independente são medidas baseadas em distância, informação, dependência e consistência.

- Dependente – requer um ou mais algoritmos de aprendizagem no processo de avaliação dos subconjuntos candidatos e determina a qualidade destes subconjuntos por meio de uma métrica de desempenho do classificador, tais como: precisão, exatidão geral, coeficiente Kappa. O método envoltório utiliza o critério dependente nas suas avaliações de subconjunto.

4.2 Coeficiente Kappa

O coeficiente Kappa é uma métrica de concordância introduzida, primeiramente, entre observadores da área de psicologia (COHEN, 1960). A intenção original de Kappa era medir o nível de concordância ou discordância de um grupo de pessoas observando um mesmo fenômeno (COHEN, 1960).

O cálculo do coeficiente Kappa é realizado a partir das entradas da matriz de confusão, mostrada na Tabela 2, gerada pelo classificador de padrões.

Tabela 2 - Matriz de confusão para o cálculo do coeficiente Kappa

		Classe prevista		**Total**
		Classe negativa (Normal)	Classe positiva (Anomalia)	
Classe real	Classe negativa (Normal)	Verdadeiro Negativo (TN)	Falso Positivo (FP)	L_1 = TN+FP
	Classe positiva (Anomalia)	Falso Negativo (FN)	Verdadeiro Positivo (TP)	L_2 = FN+TP
Total		C_1 = TN+FN	C_2 = FP+TP	N = TN+TP+FN+FP

Fonte: Elaboração do próprio autor.

Para o problema da detecção de intrusos, o coeficiente Kappa (*k*) mede a proporção de concordância observada (P_o) entre as classes de comportamentos existentes (classe real) e calculadas (classe prevista) sobre a base de treinamento após ser removida a proporção de concordância devido ao acaso (P_a), representada pelas Equações (1), (2) e (3).

$$k = \frac{P_o - P_a}{1 - P_a} \quad (1)$$

$$P_o = \frac{TN+TP}{N} \quad (2)$$

$$P_a = \frac{(C_1 * L_1)+(C_2 * L_2)}{N^2} \quad (3)$$

Onde:

TN – quantidade de amostras não-intrusivas identificadas corretamente

TP – quantidade de amostras intrusivas identificadas corretamente

C_1 – quantidade de amostras não-intrusivas e intrusivas reais identificadas como atividade não-intrusiva

C_2 - quantidade de amostras não-intrusivas e intrusivas reais identificadas como intrusiva

L_1- quantidade de amostras não-intrusivas reais identificadas como não-intrusiva ou intrusiva

L_2 – quantidade de amostras intrusivas reais identificadas como não-intrusiva ou intrusiva

N – Quantidade total de amostras classificadas

A interpretação do valor calculado *k* dar-se-á da seguinte forma: quanto mais próximo de zero for *k*, significa que as unidades classificadas ocorreram ao mero acaso, por outro lado quando *k* aproxima-se de 1, a concordância entre as classes corretas e previstas tende ao "exato" (COHEN, 1960).

A escolha pelo coeficiente Kappa como métrica para selecionar os atributos mais relevantes da base de treinamento e para avaliar a qualidade da classificação do IDS deve-se as métricas, exatidão global e precisão, serem inapropriadas em aplicações onde as classes são desigualmente representadas na base de treinamento (KUBAT; HOLTE; MATWIN, 1998).

4.3 Redes neurais ARTMAP *Fuzzy*

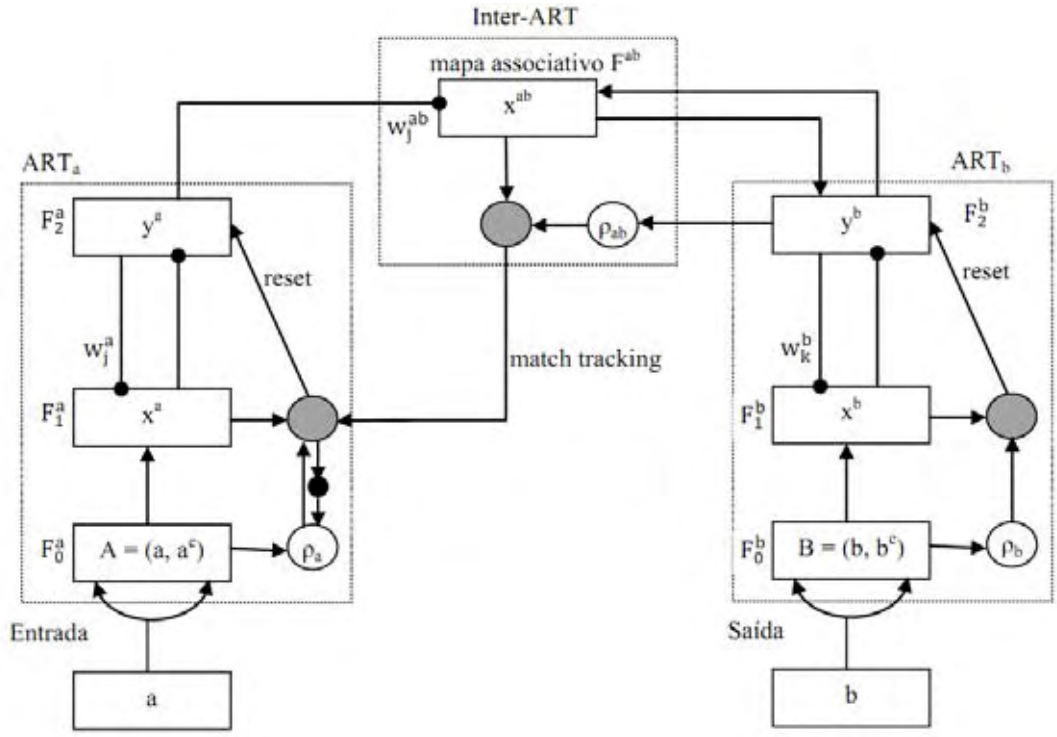
A arquitetura ARTMAP *Fuzzy* possui um sistema de aprendizado auto-organizado, que preserva os padrões de entrada assimilados e aprende novos padrões de entrada não-conhecidos (CARPENTER et al., 1992). Este tipo de sistema pertence a família das redes neurais baseada em teoria da ressonância adaptativa (*adaptive ressonance theory* – ART) e possui treinamento supervisionado.

A Figura 16, baseada na topologia original desenvolvida por (CARPENTER et al., 1992), apresenta a arquitetura da rede neural ARTMAP *Fuzzy*. Esta rede neural é composta por dois módulos (ART_a e ART_b) que seguem a estrutura de uma rede ART *Fuzzy*

(CARPENTER; GROSSBERG; ROSEN, 1991b). Cada módulo é responsável por associar uma sequência arbitrária de padrões de entrada (a e b) com as suas respectivas categorias de reconhecimento. Durante o processo de aprendizagem supervisionada, a rede ART_a recebe um determinado padrão de entrada (a) e a rede ART_b recebe outro padrão de entrada (b), onde a entrada da rede ART_b é a previsão desejada para a entrada da rede ART_a. Os módulos ART_a e ART_b são interligados por um módulo conhecido como inter-ART que controla o treinamento de um mapa associativo de categorias de reconhecimento da ART_a para categorias de reconhecimento da ART_b.

O inter-ART aplica um acréscimo no parâmetro de vigilância da rede ART_a quando a previsão da categoria de reconhecimento ativada pela rede ART_a não é confirmada pela rede ART_b. Este processo é conhecido como *match tracking* e acarreta num procedimento de busca na rede ART_a para ativar uma outra categoria de reconhecimento que possua associação na rede ART_b ou criar uma nova categoria de reconhecimento (CARPENTER et al., 1992). Devido a estas características, o *match tracking* tem como objetivos: maximizar a generalização das categorias de reconhecimento da rede ART_a e minimizar o erro de previsão da rede (CARPENTER et al., 1992).

Figura 16 - Arquitetura da rede neural ARTMAP *Fuzzy*



Fonte: Adaptado de Carpenter et al. (1992).

Na Tabela 3 é apresentado os vetores de atividades dos módulos envolvidos na rede neural ARTMAP *Fuzzy*. Sendo M_a e M_b, a quantidade de vetores de entrada na camada de comparação (F_1) e, N_a e N_b, a quantidade de vetores de entrada na camada de reconhecimento (F_2) dos módulos ART_a e ART_b, respectivamente.

Tabela 3 - Vetores dos módulos ART_a, ART_b e inter-ART

ART_a	ART_b	inter-ART
$\boldsymbol{x^a} = \left[x_1^a \dots x_{2M_a}^a\right]$	$\boldsymbol{x^b} = \left[x_1^b \dots x_{2M_b}^b\right]$	$\boldsymbol{x^{ab}} = \left[x_1^{ab} \dots x_{N_b}^{ab}\right]$
$\boldsymbol{y^a} = \left[y_1^a \dots y_{2N_a}^a\right]$	$\boldsymbol{y^b} = \left[y_1^b \dots y_{2N_b}^b\right]$	-
$\boldsymbol{w_j^a} = \left[w_{j1}^a \dots w_{j,2M_a}^a\right]$	$\boldsymbol{w_k^b} = \left[w_{k1}^b \dots w_{k,2M_b}^b\right]$	$\boldsymbol{w_j^{ab}} = \left[w_{j1}^{ab} \dots w_{j,N_b}^{ab}\right]$

Fonte: Adaptado de Lopes (2005).

O algoritmo da rede neural ARTMAP *Fuzzy* consiste nos seguintes passos:

Passo 1) Ler o vetor de entrada **a** e o vetor de saída **b**, onde **b** representa a saída desejada associada ao vetor de entrada **a**.

Passo 2) Se os valores dos vetores de entrada **a** e saída **b** não estiverem entre 0 e 1 deve-se normalizá-los para prevenir a proliferação de categorias nos módulos ART_a e ART_b. A Equação (4) descreve a normalização sobre um determinado vetor **a** (CARPENTER et al., 1992).

$$\boldsymbol{I} = \frac{\boldsymbol{a}}{|\boldsymbol{a}|} \tag{4}$$

Passo 3) Aplicar operação de codificação do complemento nos vetores **a** e **b** para se preservar a amplitude da informação. A Equação (5) descreve a codificação complementar sobre um vetor de entrada $\boldsymbol{a}$ (CARPENTER et al., 1992).

$$\boldsymbol{a^c} = 1 - \boldsymbol{a} \tag{5}$$

Assim, na Equação (6) são apresentados, respectivamente, os complementos da entrada **A** e saída **B** para as camadas F_1^a e F_1^b (CARPENTER et al., 1992).

$$\boldsymbol{A} = [\boldsymbol{a}, \boldsymbol{a^c}] \text{ e } \boldsymbol{B} = [\boldsymbol{b}, \boldsymbol{b^c}] \tag{6}$$

Passo 4) Inicialização dos pesos, vetores de atividades das camadas F_2^a e F_2^b e parâmetros dos módulos ART_a, ART_b e Inter-ART.

Na Equação (7) apresentam-se os vetores pesos inicializados com 1 para identificar a inexistência de categoria ativa (CARPENTER et al., 1992).

$$\boldsymbol{w^a} = \left(w_{ij}^a\right)_{2N_a x 2M_a} = 1, \boldsymbol{w^b} = \left(w_{ij}^b\right)_{2N_b x 2M_b} = 1 \; e \; \boldsymbol{w^{ab}} = \left(w_{ij}^{ab}\right)_{2N_a x 2N_b} = 1 \tag{7}$$

Os vetores de atividades da camada de reconhecimento dos módulos ART_a e ART_b, definido em (8), são inicializados com zero para definir que nenhuma categoria foi ativada.

$$\boldsymbol{y^a} = (y_j^a)_{2N_a} = 0 \text{ e } \boldsymbol{y^b} = (y_k^b)_{2N_b} = 0 \tag{8}$$

Os parâmetros utilizados na rede neural ARTMAP *Fuzzy* para o treinamento são formados por três componentes principais:

- O parâmetro de escolha α (α > 0) define o grau de interferência na seleção do neurônio mais representativo do vetor de pesos ***w***. Quanto mais próximo de zero, menos interferência este parâmetro tem na seleção do subconjunto *Fuzzy* w_j que é o mais correlato ao padrão de entrada ***I*** (HUANG; GEORGIOPOULOS; HEILEMAN, 1995).
- O critério de vigilância ρ (ρ ∈ [0,1]) visa perceber as diferenças entre padrões de entrada que implicam na geração de novas categorias por meio de teste de similaridade. Por isso, quanto mais próximo de 1 estiver este parâmetro mais detalhes discriminantes serão percebidos pelos neurônios (HUANG; GEORGIOPOULOS; HEILEMAN, 1995).
- A taxa de treinamento β (β ∈ [0,1]) representa a velocidade com que a rede neural aprenderá. Quanto β = 1, o treinamento da rede é rápido, e β < 1 significa um treinamento mais lento, ocasionando vários ciclos de aprendizagem até os pesos se adaptarem (HUANG; GEORGIOPOULOS; HEILEMAN, 1995).

Passo 5) Calcular as funções escolha T_J e T_K, definida em (9) e (10),para os módulos ART_a e ART_b, respectivamente. Verifica-se qual categoria de reconhecimento possui vetor de pesos mais relacionado ao padrão de entrada (CARPENTER et al., 1992).

$$\mathrm{T}_j(\mathbf{A}) = \frac{\left|\mathbf{A} \wedge \mathbf{w}_j^{\boldsymbol{a}}\right|}{\alpha + \left|\mathbf{w}_j^{\boldsymbol{a}}\right|} \tag{9}$$

$$\mathrm{T}_k(\mathbf{B}) = \frac{\left|\mathbf{B} \wedge \mathbf{w}_k^{\boldsymbol{b}}\right|}{\alpha + \left|\mathbf{w}_k^{\boldsymbol{b}}\right|} \tag{10}$$

sendo:

A – vetor de entrada da camada de entrada F_0^a

B – vetor de saída da camada de entrada F_0^b

$\mathbf{w}_j^{\boldsymbol{a}}$ – vetor pesos da categoria *j* da rede ART_a

$\mathbf{w}_k^{\boldsymbol{b}}$ – vetor pesos da categoria *k* da rede ART_b

α – parâmetro de escolha

$\wedge$ - operador **and** *Fuzzy*, definido por $(\boldsymbol{I} \wedge \boldsymbol{w_i}) = min(\boldsymbol{I_i}, \boldsymbol{w_i})$

$|\,.\,|$ – operador norma, definido por $|\boldsymbol{I}| = \sum_{i=1}^{M} |\boldsymbol{I_i}|$, para qualquer vetor *M*-dimensional

Passo 6) Selecionar a categoria vencedora para os módulos ART_a e ART_b: Após o cálculo da função escolha para cada vetor de pesos da categoria $\boldsymbol{j}$, a seleção da categoria vencedora é realizada por meio de (11), onde o maior valor da função escolha dentre todos os efetuados é o escolhido. Se mais de um T_j é máximo, seleciona-se a categoria $\boldsymbol{j}$ com menor índice. Da mesma forma, ocorre no módulo ART_b para selecionar a categoria vencedora, como pode ser visto em (12).

$$\mathrm{T_J} = máx\{T_j : \; j = 1 \ldots n\} \tag{11}$$

$$\mathrm{T}_K = máx\{T_k : \; k = 1 \ldots n\} \tag{12}$$

Passo 7) Calcular a função coincidência, representada em (13), da categoria selecionada, e testar se o valor obtido excede o parâmetro de vigilância. Se a resposta for afirmativa, ocorre ressonância e a categoria vencedora coincide com o padrão de entrada $\boldsymbol{A}$ submetido. Caso contrário, desativa-se T_J com 0 para que na próxima busca em (11) esse neurônio não seja mais selecionado. Neste caso, um novo índice é escolhido em (11) e o processo de busca é repetido até que (13) encontre ressonância. Da mesma forma, ocorre no módulo ART_b para verificar se há similaridade entre categoria vencedora e o padrão de entrada $\boldsymbol{B}$, como pode ser visto em (14).

$$\frac{|\mathbf{A} \wedge \mathbf{w}_J^{\boldsymbol{a}}|}{|\mathbf{A}|} \geq \rho_a \tag{13}$$

$$\frac{|\mathbf{B} \wedge \mathbf{w}_K^{\boldsymbol{b}}|}{|\mathbf{B}|} \geq \rho_b \tag{14}$$

sendo:

A – vetor de entrada da camada de entrada F_0^a

B – vetor de saída da camada de entrada F_0^b

$\mathbf{w}_J^{\boldsymbol{a}}$ – vetor pesos da categoria vencedora J

$\mathbf{w}_K^{\boldsymbol{b}}$ – vetor pesos da categoria vencedora K

J – índice do nó ativo na camada de reconhecimento F_2^a

K – índice do nó ativo na camada de reconhecimento F_2^b

ρ_a - parâmetro de vigilância aplicado na rede ART_a

ρ_b - parâmetro de vigilância aplicado na rede ART_b

Passo 8) *Match tracking* (teste de ressonância) entre os módulos ART_a e ART_b: Verificação se a categoria de reconhecimento ativa nas redes ART_a (J) e ART_b (K) possuem

similaridade, ou seja, se o padrão de entrada submetido enquadra-se em alguma categoria de reconhecimento apresentada pela saída. Isso ocorre quando o valor calculado é maior ou igual ao parâmetro de vigilância do módulo inter-ART, apresentado em (15).

$$\frac{\left|\mathbf{y^b} \wedge \mathbf{W_{JK}^{ab}}\right|}{|\mathbf{y^b}|} \geq \rho_{ab} \tag{15}$$

sendo:

$\mathbf{W_{jK}^{ab}}$ – vetor de pesos do mapa associativo (F^{ab})

$\mathbf{y^b}$ – vetor de atividades da camada de reconhecimento F_2^b

ρ_{ab} – parâmetro de vigilância do mapa associativo

Se (15) não for satisfeita, é feito um incremento δ no parâmetro de vigilância da rede ART_a (ρ_a), representado em (16), suficiente apenas para excluir a categoria corrente da seleção executada em (15). Em seguida repete-se os passos entre **passo 6** e **passo 8**. Se nenhuma das categorias de reconhecimento existentes na rede ART_a coincide com a categoria vencedora da rede ART_b, então ativa-se uma nova categoria na rede ART_a e efetua-se sua conexão com a categoria da rede ART_b.

$$\rho_a = \frac{\left|\mathbf{A} \wedge \mathbf{w}_J^a\right|}{|\mathbf{A}|} + \delta, \qquad 0 < \delta \ll 1 \tag{16}$$

Passo 9) Adaptação dos pesos nos módulos ART_a, ART_b e inter-ART: Os pesos dos módulos ART_a, ART_b e inter-ART são atualizados em seus vetores ($\mathbf{W^a}$, $\mathbf{W^b}$ e $\mathbf{W^{ab}}$) por meio das equações descritas em (17), (18) e (19).

$$\mathbf{W_J^{novo}} = \beta\left(\mathbf{A} \wedge \mathbf{W_J^{velho}}\right) + (1-\beta)\mathbf{W_J^{velho}} \tag{17}$$

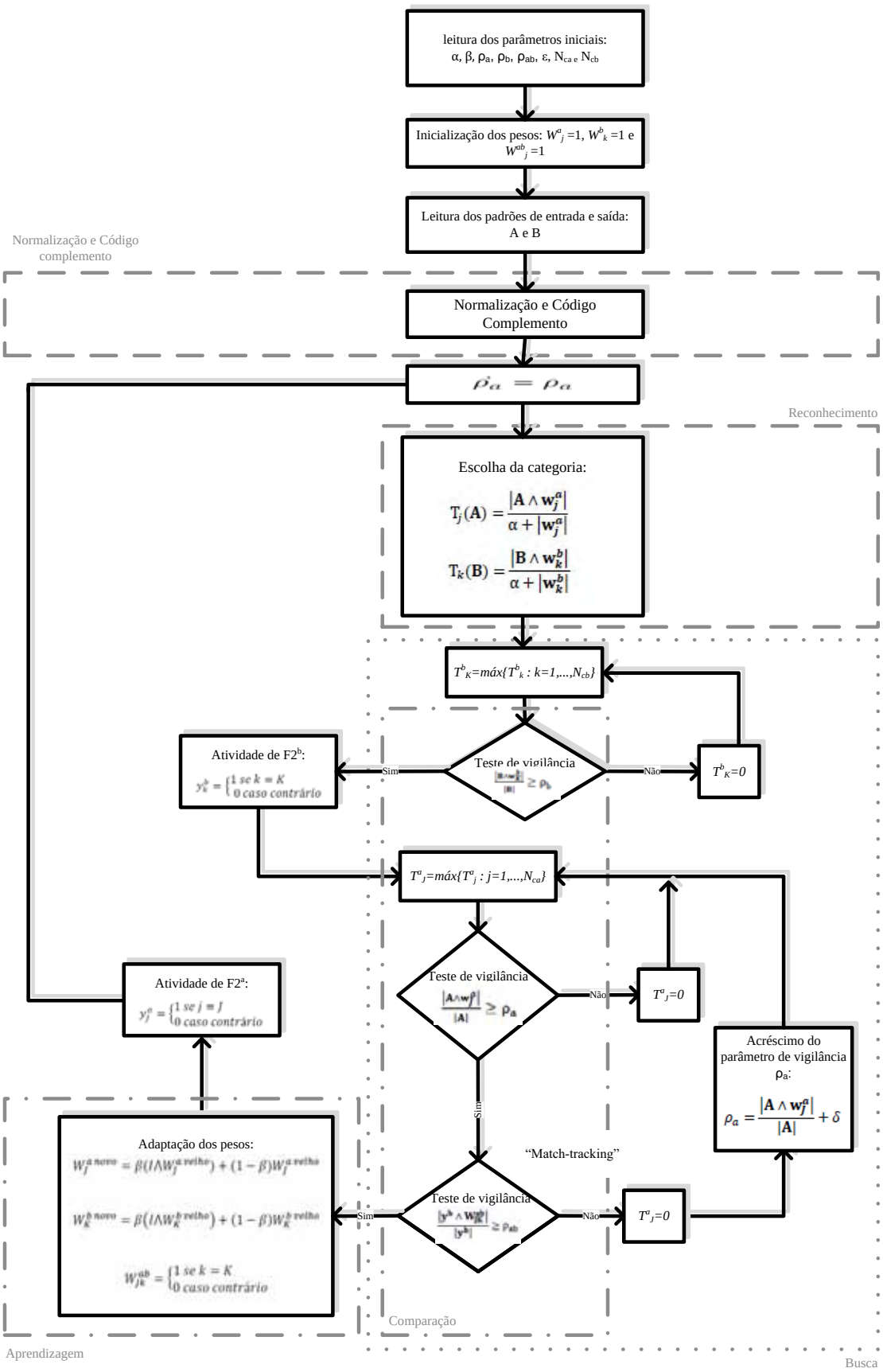
$$\mathbf{W_K^{novo}} = \beta\left(\mathbf{B} \wedge \mathbf{W_K^{velho}}\right) + (1-\beta)\mathbf{W_K^{velho}} \tag{18}$$

$$\mathbf{W_{jk}^{ab}} = \begin{cases} 1, \text{para j} = \text{J e k} = \text{K} \\ 0, \text{para j} \neq \text{J e k} \neq \text{K} \end{cases} \tag{19}$$

Passo 10) Repetir passos 5 a 9 para todos os pares a serem treinados.

O fluxograma, apresentado na Figura 17, mostra de forma gráfica a lógica do algoritmo da rede neural ARTMAP *Fuzzy*.

Figura 17 - Fluxograma do algoritmo da rede neural ARTMAP *Fuzzy*



Fonte: Adaptado de Lopes (2005).

4.4 Otimização por enxame de partículas (*particle swarm optimization* - PSO)

PSO é uma técnica de otimização estocástica baseada em população que foi inspirada no comportamento social de um bando de pássaros ou cardume de peixes (KENNEDY; EBERHART, 1995). Esta técnica compartilha muitas similaridades com as técnicas de computação evolucionária, tal como algoritmos genéticos, embora não contenha operadores de evolução tais como *crossover* e mutação. PSO pertence a uma classe de técnicas de algoritmos evolucionários que não emprega o conceito do "direito do mais forte", nem a função de seleção direta. Uma solução com valores de ajuste muito baixo podem, assim, sobreviver durante a otimização e potencialmente visitar qualquer ponto do espaço de soluções (PORTO et al., 1998). Por fim, enquanto os algoritmos genéticos foram concebidos para lidar com codificação binária, a PSO foi projetado e tem oferecido resultados efetivos na solução de problemas de otimização global cujo valor de codificação é real, o que torna a PSO adequado para estudo em escalas maiores.

Com a PSO, cada partícula corresponde a uma única resposta no espaço solução e a população de partículas é chamada de enxame. Todas as partículas estão associadas a posições, que são analisadas de acordo com a função de avaliação (*fp*) sendo otimizada, e valores de velocidade, que definem seus movimentos. As partículas deslocam através do espaço solução, seguindo as partículas com o melhor ajuste. Assumindo um espaço solução *d*-dimensional, a posição da partícula *i* no enxame de *P*-particulas é representado por um vetor *d*-dimensional $\boldsymbol{s_i} = (s_{i1}, s_{i2}, \dots, s_{id})$, para $i = 1, 2, \dots, P$. A velocidade desta partícula é referenciada pelo vetor $\boldsymbol{v_i} = (v_{i1}, v_{i2}, \dots, v_{id})$, enquanto a melhor posição visitada anteriormente desta partícula é definida como $\boldsymbol{p_i} = (p_{i1}, p_{i2}, \dots, p_{id})$. Para cada nova iteração *q+1*, a velocidade e localização da partícula *i* são atualizadas segundo as equações (20) e (21).

$$\boldsymbol{v_i^{q+1}} = w^q \boldsymbol{v_i^q} + c_1 r_1 \left(\boldsymbol{p_i^q} - \boldsymbol{s_i^q}\right) + c_2 r_2 \left(\boldsymbol{p_g^q} - \boldsymbol{s_i^q}\right) \tag{20}$$

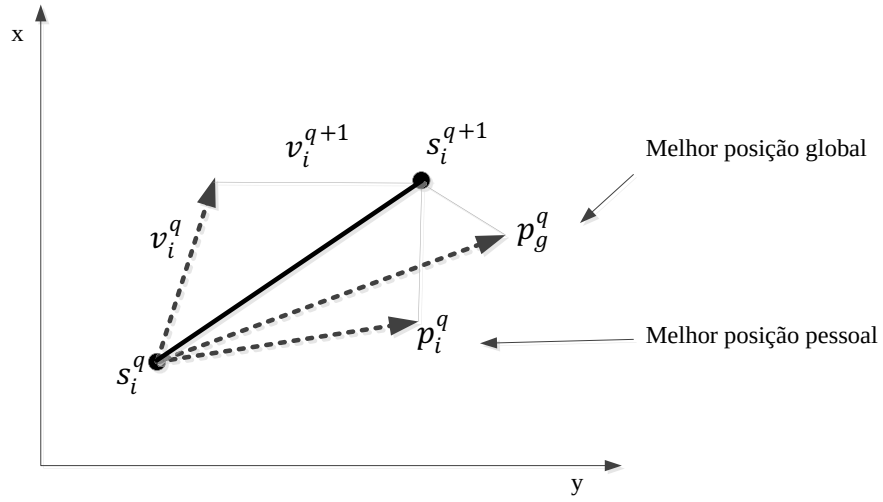
$$\boldsymbol{s_i^{q+1}} = \boldsymbol{s_i^q} + \boldsymbol{v_i^{q+1}} \tag{21}$$

Onde $\boldsymbol{p_g}$ representa a melhor localização global da partícula no enxame, w^q é o peso inercial da partícula, c_1 e c_2 são constantes positivas conhecidas como parâmetros cognitivo e social, respectivamente, e r_1 e r_2 são números aleatórios distribuídos uniformemente no intervalo [0,1].

A função de w^q regula o equilíbrio entre exploração e utilização. Um peso alto facilita uma busca global (exploração), enquanto um valor pequeno de peso tende a facilitar o ajuste numa determinada área de busca (utilização). Isto porque os valores dos pesos são definidos a

partir de uma função decrescente monotonicamente de q. Uma sintonia apropriada de c_1 e c_2 podem resultar numa convergência mais rápida do algoritmo e na atenuação do mínimo local. Kennedy e Eberhart (1995) propõem que os parâmetros cognitivo e social sejam selecionados tal que c_1=c_2=2, porque esta condição faz com que a influência tanto da experiência pessoal ($c_1 r_1(\boldsymbol{p_i^q} - \boldsymbol{s_i^q})$) quanto da experiência coletiva ($c_2 r_2(\boldsymbol{p_g^q} - \boldsymbol{s_i^q})$) tenham o mesmo peso no cálculo da velocidade em que a partícula movimenta-se no espaço solução. Finalmente, os parâmetros r_1 e r_2 são usados para manter a diversidade da população. A Figura 18 ilustra como a PSO atualiza a posição da partícula $\boldsymbol{s_i^q}$ na iteração *q+1*.

Figura 18 Atualização de uma posição de partícula $\boldsymbol{s_i^q}$ pela PSO num espaço bidimensional na iteração *q+1*.



Fonte: Adaptado de Granger et. al. (2007).

Para limitar a velocidade de uma partícula (v_i) para que o sistema não extrapole o espaço solução, são impostos limites (v_{max}) para seus valores em cada dimensão do espaço solução:

$$\text{Se } v_i > v_{max} \text{ então } v_i = v_{max},$$
$$\text{Senão se } v_i < -v_{max} \text{ então } v_i = -v_{max}.$$

O algoritmo da PSO é definido pelos seguintes passos (GRANGER et. al., 2007; KENNEDY; EBERHART, 1995; POLI; KENNEDY; BLACKWELL, 2007; SERAPIÃO, 2009):

Passo 1) Determinar o número de partículas da população (P), velocidade máxima permitida (v_{max}), peso inercial inicial (w^0), parâmetro cognitivo (c_1), parâmetro social (c_2) e números aleatórios distribuídos uniformemente (r_1 e r_2).

Passo 2) Inicializar a posição inicial das partículas de forma aleatória.

Passo 3) Inicializar a velocidade inicial das partículas de forma aleatória, tal que $0 \leq v_i^0 \leq v_{max}$, para i = 1, ..., P.

Passo 4) Para cada partícula $\boldsymbol{p}$ em P faça:

(a) Calcular sua função de avaliação $fp = f(\boldsymbol{p})$.

(b) Comparar a função de avaliação calculada fp com seu melhor valor pessoal armazenado $pbest_i$. Se o valor atual é melhor que $pbest_i$, então:

$$pbest_i = fp$$

$$\boldsymbol{p_i} = \boldsymbol{s_i}$$

Passo 5) Identificar na população a partícula com o maior valor de função de avaliação e associar seu índice a variável *g*.

Passo 6) Para cada partícula $\boldsymbol{p}$ em P faça:

(a) Atualizar velocidade: $\boldsymbol{v_i^{q+1}} = w^q \boldsymbol{v_i^q} + c_1 r_1 \left(\boldsymbol{p_i^q} - \boldsymbol{s_i^q}\right) + c_2 r_2 \left(\boldsymbol{p_g^q} - \boldsymbol{s_i^q}\right)$.

(b) Atualizar posição: $\boldsymbol{s_i^{q+1}} = \boldsymbol{s_i^q} + \boldsymbol{v_i^{q+1}}$.

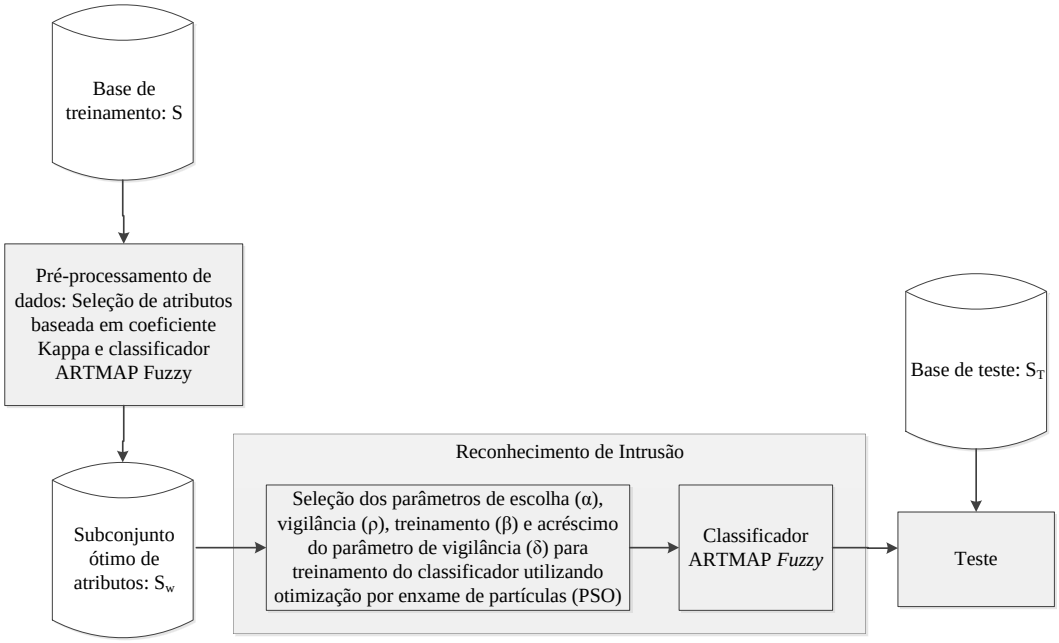
Passo 7) Atualizar o valor do peso inercial (w^{q+1}).

Passo 8) Se a condição de parada não for alcançada, retorne ao passo 4.

4.5 Visão geral do Kappa-PSO-ARTMAP *Fuzzy*

Kappa-PSO-ARTMAP *Fuzzy* é composto de quatro fases: pré-processamento de dados aplicando seleção de atributos baseada em envoltório, seleção de parâmetros ótimos para o treinamento da rede neural ARTMAP *Fuzzy* empregando otimização por enxame de partículas, classificação de ataques e teste do IDS. A Figura 19 ilustra o fluxograma desta arquitetura de detecção de intrusos.

Figura 19 - Fluxograma da arquitetura de IDS Kappa-PSO-ARTMAP *Fuzzy*.



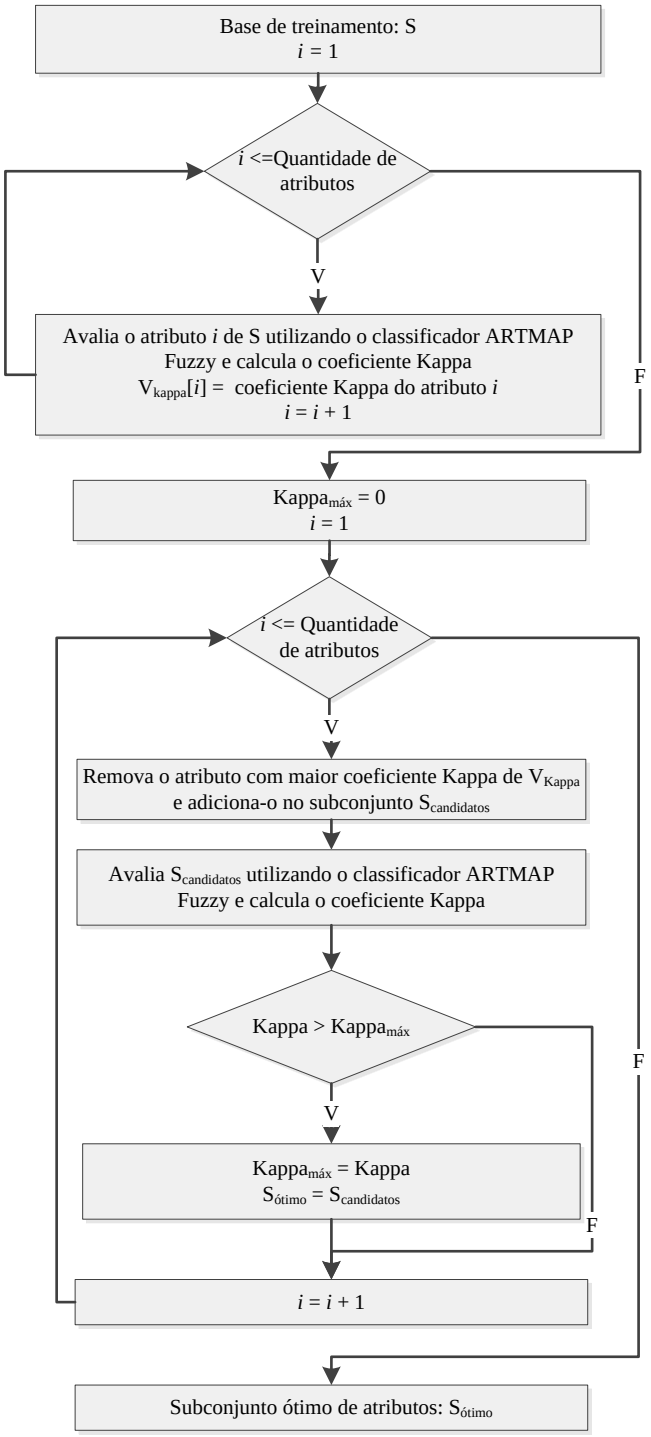
Fonte: Elaboração do próprio autor.

A fase de pré-processamento de dados, ilustrada na Figura 20, faz uso de um procedimento de seleção de atributos que, primeiramente, avalia cada atributo da base de treinamento (S) por meio do classificador ARTMAP *Fuzzy* e gera uma matriz de confusão contendo as amostras (normal e anomalia) identificadas corretamente e incorretamente. No passo seguinte calcula o coeficiente Kappa de cada matriz de confusão gerada pela avaliação dos atributos e armazena num vetor chamado de vetor dos coeficientes Kappa ($\mathbf{V_{Kappa}}$). A seguir, emprega a estratégia de busca *sequential forward search* - SFS (GUYON; ELISSEEFF, 2003) para remover a cada iteração do vetor $\mathbf{V_{Kappa}}$ o atributo com maior coeficiente Kappa e adiciona-o no subconjunto de atributos candidatos ($S_{candidatos}$). Logo após, o classificador ARTMAP *Fuzzy* e o cálculo do coeficiente Kappa são aplicados, novamente, para avaliar a taxa de classificação correta e incorreta conseguida pelo subconjunto de atributos candidatos. Na próxima etapa verifica se o coeficiente Kappa de $S_{candidatos}$ é o maior valor alcançado dos subconjuntos avaliados. Caso a resposta seja afirmativa, o subconjunto ótimo ($S_{ótimo}$) armazena os atributos de $S_{candidatos}$. A condição de parada da busca SFS ocorre quando o $\mathbf{V_{Kappa}}$ estiver vazio. Após esse processamento, o subconjunto ótimo ($S_{ótimo}$) contém o agrupamento de atributos candidatos que possui o maior coeficiente Kappa entre os subconjuntos testados no algoritmo.

Após os dados serem pré-processados inicia-se a fase de reconhecimento de intrusão, onde se utiliza uma técnica de inteligência de enxame (conhecida como otimização por

enxame de partículas) para selecionar um conjunto de parâmetros para o treinamento do classificador ARTMAP *Fuzzy*, de forma que maximize a taxa de detecção de intrusos e minimize a taxa de falsos alarmes. A função de avaliação utilizada para satisfazer estes dois critérios é o coeficiente Kappa.

Figura 20 - Fluxograma da metodologia de seleção de atributos utilizada na fase de pré-processamento de dados.



Fonte: Elaboração do próprio autor.

Nesta representação da PSO considera-se cada partícula uma rede neural ARTMAP *Fuzzy* com um espaço solução 4-dimensional, pois cada dimensão representa um parâmetro do grupo solicitado para o treinamento do classificador de ataques. Desta forma, os componentes da posição da partícula *i* no espaço solução são definidos pela Equação (22).

$$\boldsymbol{s_i^q} = (s_{11}^q, s_{12}^q, s_{13}^q, s_{14}^q) \tag{22}$$

Sendo,

s_{11}^q- parâmetro de vigilância da rede ART_a (ρ_a)

s_{12}^q- parâmetro de escolha (α)

s_{13}^q- taxa de treinamento (β)

s_{14}^q- acréscimo ao parâmetro de vigilância da rede ART_a (δ)

A escolha destes parâmetros para a composição da posição da partícula deve-se ao fato deles serem essenciais para o desenvolvimento da rede neural ARTMAP *Fuzzy* (CARPENTER et al., 1992; GRANGER et. al., 2007). A função de avaliação empregada na PSO para avaliar a qualidade das partículas é o coeficiente Kappa.

O fluxograma apresentado na Figura 21 descreve os passos necessários para a determinação deste conjunto de configuração para o treinamento do classificador de ataques.

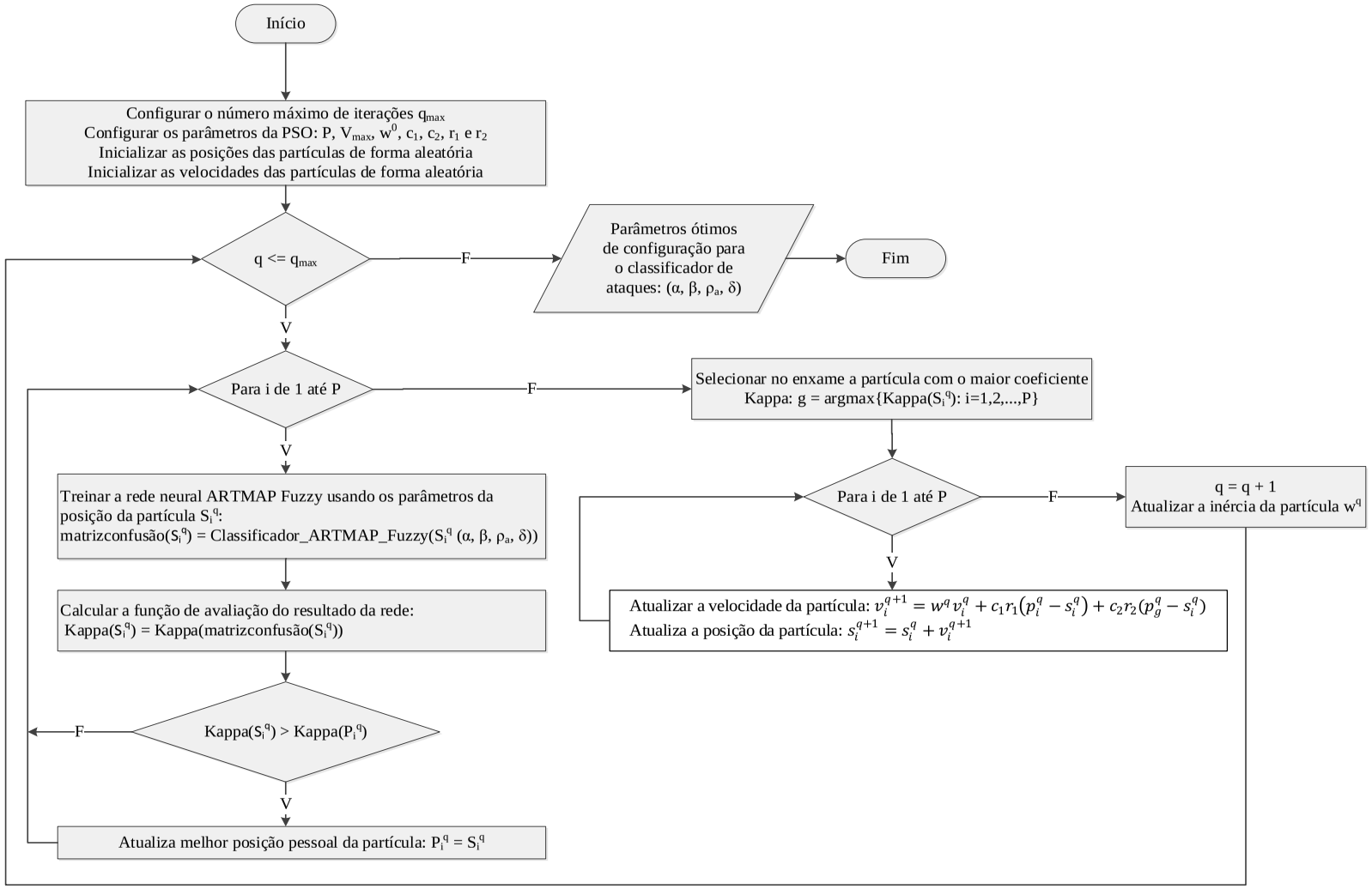
Posteriormente, ao conseguir a melhor configuração de parâmetros para o classificador ARTMAP *Fuzzy* utilizam-se estas informações como valores-padrão para o IDS na fase de teste.

4.6 Conclusões

O emprego de técnicas de inteligência computacional e seleção de atributos em IDSs tem despertado, atualmente, grande interesse na comunidade científica, visto que tais estratégias podem oferecer características que auxiliam na construção de modelos de detecção de intrusos computacionalmente mais leves (WU; BANZHAF, 2010). Seguindo esta tendência, aplicam-se dois procedimentos bem definido na proposta de IDS apresentada nesta tese. Primeiramente, é utilizada seleção de atributos baseada em envoltório para pré-processar a base de treinamento original e gerar um subconjunto ótimo de atributos. A segunda forma é aplicação de técnicas de inteligência computacional (redes neurais e inteligência de enxame) no módulo de reconhecimento de intrusão, que selecionam os melhores parâmetros para o treinamento da rede neural utilizada no classificador de ataques.

No próximo Capítulo realiza-se uma avaliação de desempenho do modelo de detecção Kappa-PSO-ARTMAP *Fuzzy* sobre três bases de conhecimentos coletadas, respectivamente, num ambiente simulado cabeado (KDD99) e num ambiente real sem fio infraestruturado (WLAN) sobre dois cenários de segurança habilitada: 1) criptografia WEP e WPA habilitada e 2) criptografia WPA2 habilitada.

Figura 21 - Fluxograma da seleção dos parâmetros ótimos para o treinamento da rede neural ARTMAP *Fuzzy* utilizando a PSO.



Fonte: Adaptado de Antunes, Araújo e Minussi (2013) e Granger et. al. (2007).

5 INVESTIGANDO O DESEMPENHO DA METODOLOGIA KAPPA-PSO-ARTMAP *FUZZY* NA DETECÇÃO DE INTRUSOS

Neste Capítulo, inicialmente, descrevem-se os três tipos de bases de dados (treinamento e teste) empregados para avaliação de desempenho das metodologias apresentadas nesse trabalho. Logo após, é mostrada a evolução dos experimentos e resultados na elaboração da metodologia proposta KAPPA-PSO-ARTMAP *Fuzzy*. No primeiro cenário apresenta-se o desempenho de um modelo de IDS utilizando apenas a rede neural ARTMAP *Fuzzy* no módulo de reconhecimento de intrusão. No segundo cenário aplica-se a mesma técnica de detecção de intrusos empregada no primeiro cenário, acrescentada de uma fase de pré-processamento de dados que utiliza seleção de atributos envoltório baseado em coeficiente Kappa e classificador ARTMAP *Fuzzy*. Finalmente, no último cenário apresenta-se avaliação de desempenho do sistema de detecção de intrusos KAPPA-PSO-ARTMAP *Fuzzy*.

5.1 Bases de dados aplicadas na avaliação do Kappa-PSO-ARTMAP *Fuzzy*

Nesta seção realiza-se uma breve descrição sobre os três tipos de bases de dados utilizadas para avaliação do IDSs implementados neste trabalho. A primeira base de dados representa uma coleta realizada sobre uma rede cabeada simulada, amplamente conhecida como KDD99 (LIPPMANN et al., 2000). A segunda base é o resultado de um monitoramento sobre uma rede infraestruturada sem fio com criptografia WEP e WPA habilitadas. A última base de dados, também, é originada do monitoramento de uma rede infraestruturada sem fio, contudo implementa-se apenas o mecanismo de segurança WPA2.

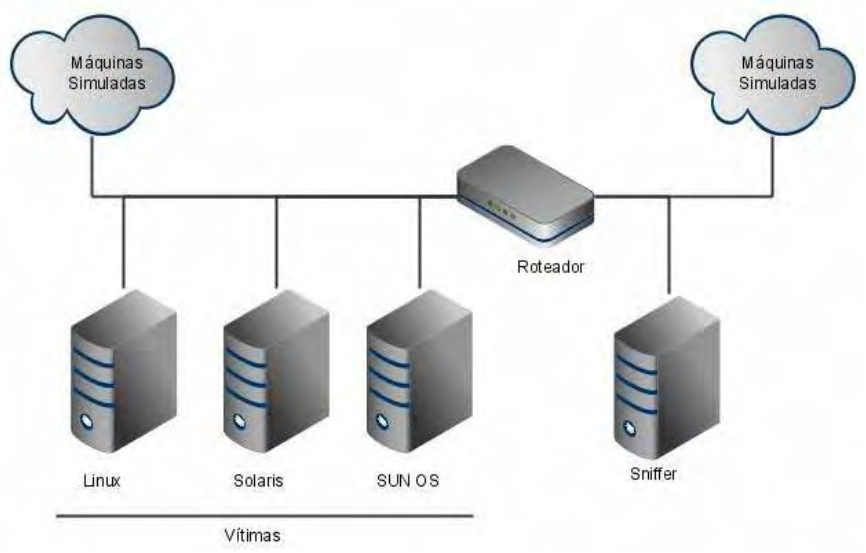
5.1.1 Base de dados coletada de uma rede cabeada simulada (KDD99)

Apesar de ser relativamente antiga, e incluir poucos ataques contra sistemas baseados em UNIX e em roteadores CISCO, a KDD99 (LIPPMANN et al., 2000) é uma base de dados amplamente utilizada por pesquisadores para avaliar algoritmos de detecção de intrusos e aprendizagem de máquina (WU; BANZHAF, 2010).

KDD99 refere-se a um conjunto de bases para treinamento e teste de IDS, criada a partir de um projeto desenvolvido pelo Laboratório Lincoln do *Massachusetts Institute of Technology*, que realizou avaliações a respeito de diferentes metodologias de detecção de intrusão.

A Figura 22 representa a topologia da rede aplicada na base KDD99, onde foi criada uma rede militar fictícia composta de três máquinas-alvo que disponibilizavam diversos sistemas operacionais e serviços. Além disso, havia três máquinas adicionais cuja função era gerar tráfego proveniente de diferentes fontes. Finalmente, foi usado um *sniffer* para registrar todo o fluxo da rede em formato TCP (*Transmission Control Protocol*) *dump*. O período total da simulação foi sete semanas.

Figura 22 - Topologia da rede aplicada no KDD99.



Fonte: Adaptado de Lippmann et al. (2000)

Os *logs* registrados a partir do *sniffer* foram divididos em cinco categorias (KAYACIK; ZINCIR-HEYWOOD; HEYWOOD, 2005; LIPPMANN et al., 2000; SOUZA, 2008):

- Normal – conexões que representam o perfil esperado numa rede militar.
- Negação de Serviço (DoS) – procura indisponibilizar os serviços da máquina-alvo aos seus usuários legítimos.
- Reconhecimento (*Probe*) – ocorre uma varredura de informações sobre a máquina-alvo com o objetivo de identificar potenciais vulnerabilidades nos serviços oferecidos.

- Remoto para Usuário (R2L) – o atacante tenta obter acesso numa máquina ou rede sem autorização.
- Usuário para Superusuário (U2R) – a máquina-alvo já foi invadida, mas o atacante tenta obter um acesso com privilégios de superusuário.

Os arquivos gerados nessa captura foram pré-processados para se adequarem a um formato padrão que contém 41 características para cada conexão registrada. Uma conexão é uma sequência de pacotes TCP com duração bem definida, que são transmitidos de uma máquina fonte para uma máquina destino, ou na direção inversa (destino-fonte) sobre um protocolo bem definido (LIPPMANN et al., 2000). Cada conexão é rotulada como normal, ou como ataque, com exatamente um tipo de ataque. Cada registro de conexão consiste de aproximadamente 100 *bytes*.

Para facilitar a compreensão da contribuição de cada um dos parâmetros da conexão na definição de um perfil, as características dos registros de conexão foram divididas em quatro grupos (KAYACIK; ZINCIR-HEYWOOD; HEYWOOD, 2005; LIPPMANN et al., 2000; SOUZA, 2008):

- Características básicas - identificam as propriedades existentes no cabeçalho do pacote. Elas representam métricas de uso fundamental numa conexão e estão detalhadas na Tabela 4.

Tabela 4 - Características intrínsecas de uma conexão TCP

Nome	Descrição	Tipo
duration	Tempo em segundos de conexão	Continuo
protocol_type	Tipo de conexão (TCP, UDP)	Simbólico
service	Tipo de serviço no destino (HTTP, Telnet)	Simbólico
src_byte	Número de bytes da origem ao destino	Contínuo
dst_byte	Número de bytes do destino à origem	Contínuo
flag	Estado da conexão (normal ou erro)	Simbólico
land	1 se o host e a porta da origem e destino são os mesmos, 0 caso contrário	Simbólico
wrong_fragment	Número de fragmentos “errados”	Contínuo
urgent	Número de pacotes urgentes	Contínuo

Fonte: Adaptado de Lippmann et al. (2000).

- Características sugeridas por meio de conhecimento da área – são informações extraídas dos pacotes, as quais têm significado apenas com o auxílio de especialistas, para se chegar a conclusões de que padrões associados a conexões podem representar um determinado tipo de ataque. Isto inclui métricas tal como a

quantidade de tentativas de acesso não autorizado numa determinada máquina. Na Tabela 5 descrevemos as métricas envolvidas neste grupo.

Tabela 5 - Características sugeridas pelo conhecimento de uma conexão TCP

Nome	Descrição	Tipo
hot	Número de indicadores "importantes"	Contínuo
num_failed_logins	Número de tentativa de login com falha	Contínuo
logged_in	1 se o *login* obteve sucesso, e 0 caso contrário	Simbólico
num_comprissed	Número de condições comprometedoras	Contínuo
root_shell	1 se o *Shell root* é obtido, 0 caso contrário	Simbólico
su_attempted	1 de houver tentativa de conseguir "su root", 0 caso contrário	Simbólico
num_root	Número de acessos como *root*	Contínuo
num_file_creations	Número de operações de criação de arquivos	Contínuo
num_shells	Números de *Shell prompts* abertos	Contínuo
num_access_files	Número de operações a arquivos de controle de acesso	Contínuo
num_outbund_cmds	Número de comandos externos (sessão FTP)	Contínuo
is_hot_login	1 se o login pertence à lista "hot", 0 caso contrário	Simbólico
is_guest_login	1 se login é do tipo "guest", 0 caso contrário	Simbólico

Fonte: Adaptado de Lippmann et al. (2000).

- Características de Tráfego calculadas usando uma janela de 2 segundos – apresenta as características ocorridas num perfil de tráfego computadas durante um determinado intervalo de tempo (2 segundos). Informações importantes referentes a certos ataques só podem ser obtidas levando-se o tempo em consideração. Um exemplo a ser citado é a quantidade de conexões para uma mesma máquina num intervalo de dois segundos. O restante das métricas é apresentado na Tabela 6.

Tabela 6 - Características de tráfego calculadas usando uma janela de 2 segundos

Nome	Descrição	Tipo
count	Número de conexões para o mesmo *host* como a conexão atual nos últimos 2 segundos	Contínuo
serror_rate	% de conexões para o mesmo *host* que tiveram erros do tipo "SYN"	Contínuo
rerror_rate1	% de conexões para o mesmo *host* que tiveram erros do tipo "REJ"	Contínuo
same_srv_rate1	% de conexões ao mesmo serviço	Contínuo
diff_srv_rate1	% de conexões a diferentes serviços	Contínuo
srv_count1	Número de conexões ao mesmo serviço como a conexão atual nos últimos 2 segundos	Contínuo
srv_serror_rate	% de conexões ao mesmo serviço que tiveram erros "SYN"	Contínuo
srv_rerror_rate2	% de conexões ao mesmo serviço que tiveram erros "REJ"	Contínuo
srv_diffe_host_rate2	% de conexões a diferentes *hosts*	Contínuo

Fonte: Adaptado de Lippmann et al. (2000).

- Características de Tráfego calculadas usando o histórico das 100 últimas conexões – as métricas, que demonstram o perfil do tráfego, são calculadas a partir de um histórico estimado sobre as cem últimas conexões realizadas. Uma métrica empregada nesse grupo é a quantidade de conexões que tem a mesma máquina destino. Na Tabela 7 é detalhada cada uma das métricas com essa característica.

Tabela 7 Características de tráfego calculadas usando o histórico das 100 últimas conexões

Nome	Descrição	Tipo
dst_host_count	Quantidade de conexões que tem o mesmo *host* destino	Contínuo
dst_host_srv_count	Quantidade de conexões que tem o mesmo *host* destino e usam o mesmo serviço	Contínuo
dst_host_same_srv_rate	% de conexões que tem o mesmo *host* destino e usam o mesmo serviço	Contínuo
dst_host_diff_srv_rate	% de diferentes serviços sobre um *host* atual	Contínuo
dst_host_same_src_port_rate	% de conexões ao *host* atual que tem a mesma porta origem	Contínuo
dst_host_srv_diff_host_rate	% de conexões a um mesmo serviço vindo de diferentes *hosts*	Contínuo
dst_host_serror_rate	% de conexões ao *host* atual que tiveram um erro s0	Contínuo
dst_host_srv_serror_rate	% de conexões ao *host* atual e serviço especificado que tiveram um erro s0	Contínuo
dst_host_rerror_rate	% de conexões ao *host* atual que tiveram um erro RST	Contínuo
dst_host_srv_rerror_rate	% de conexões ao *host* atual e serviço especificado que tiveram um erro RST	Contínuo

Fonte: Adaptado de Lippmann et al. (2000).

KDD99 é formado por três bases de dados apresentadas na Tabela 8. A maior delas é uma base chamada de "*Whole* KDD", com cerca de 4,9 milhões de registros, originada a partir do pré-processamento dos dados auditados originalmente pelo *sniffer*.

Tabela 8 - Classes de comportamentos dos subconjuntos de detecção de intrusos da base KDD99 em termo do número de amostras.

Base de Dados	Normal	Anomalia	Total de amostras
10% KDD99	97277	396743	494020
Corrected KDD99	60593	250436	311029
Whole KDD99	972780	3925650	4898430

Fonte: Adaptado de Lippmann et al. (2000).

Devido à dificuldade de manuseio da grande massa de dados e com o intuito de reduzir o custo computacional, selecionou-se aleatoriamente um subconjunto de 10% dos dados de

treinamento da base pré-processada ("*Whole* KDD"), gerando o conjunto "10% KDD", cujo propósito é o treinamento do IDS.

Na base pré-processada (*Whole* KDD) e nos dados de treinamento (10% KDD) são referenciados 22 tipos de ataque, enquanto na base de teste (*Corrected* KDD) são acrescentados mais 14 novos ataques (LIPPMANN et al., 2000).

A base de dados empregada nos experimentos é um conjunto de 10000 amostras retiradas da base 10%KDD99, respeitando a representatividade das 22 classes de ataques existentes e a classe normal. O particionamento da base de dados em 7500 amostras para o treinamento e 2500 amostras para o teste refere-se ao método *holdout* (FIELDING; BELL, 1997). A Tabela 9 apresenta a distribuição das amostras nos dois conjuntos da base de dados e nas categorias de reconhecimento analisadas nos estudos.

Tabela 9 - Distribuição das 10000 amostras coletadas na rede cabeada simulada KDD99.

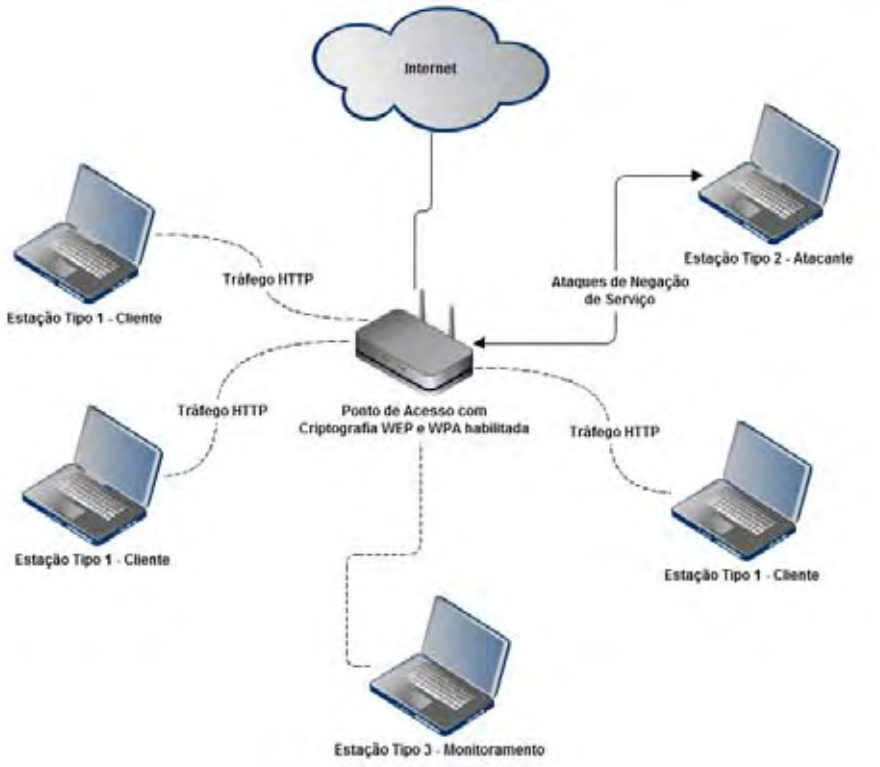
			Conjuntos da Base de Dados	
			Treinamento	Teste
Categorias de Reconhecimento	Normal		1477	500
	Anomalia	Negação de serviço	5925	1981
		Reconhecimento	60	16
		Remoto para usuário	28	3
		Usuário para superusuário	10	1
Total de Amostras			7500	2500

Fonte: Adaptado de Lippmann et al. (2000).

5.1.2 Base de dados coletada de uma rede infraestruturada sem fio com criptografia WEP e WPA habilitadas (WEP-WPA)

A segunda base de dados é o resultado do monitoramento numa rede infraestruturada sem fio (WLAN) com criptografia WEP e WPA habilitadas, cuja topologia é representada na Figura 23.

Figura 23 - Topologia da rede WLAN com criptografia WEP e WPA habilitadas.



Fonte: Adaptado de Vilela et al. (2013).

A rede analisada tem a seguinte composição: cinco estações sem fio e um ponto de acesso (AP). As estações-cliente injetam tráfego normal na rede (HTTP, FTP). A estação-atacante utiliza a ferramenta Aireplay (AIRCRACK, 2011) para realizar, simultaneamente, os quatro ataques (*chopchop*, duração, deautenticação e fragmentação) pré-definidos. A estação-monitoramento usa a ferramenta Wireshark (WIRESHARK, 2011) para realizar a captura do tráfego transeunte (normal e intruso) na rede.

A Tabela 10 apresenta a distribuição das amostras nos dois conjuntos da base de dados e nas categorias de reconhecimento analisadas nos estudos. Foram coletadas 17800 amostras divididas em 11000 amostras normais e 6800 amostras intrusivas. Como na base KDD99 também é empregado o particionamento de dados *holdout* (FIELDING; BELL, 1997) tanto para a separação do conjunto de treinamento e teste quanto para a composição de comportamento normal e anômalo.

Tabela 10 - Distribuição das 17800 amostras coletadas na rede infraestruturada sem fio com criptografia WEP e WPA habilitadas.

			Conjuntos da Base de Dados	
			Treinamento	Teste
Categorias de Reconhecimento	Normal		6000	5000
	Anomalia	ChopChop	900	800
		Deautenticação	900	800
		Duração	900	800
		Fragmentação	900	800
Total de Amostras			9600	8200

Fonte: Adaptado de Vilela et al. (2013).

A seguir, é realizado um pré-processamento nos dados capturados para se extrair somente os campos do cabeçalho MAC (*protocol version*, *type*, *subtype*, to DS, from DS, *more fragment*, *retry*, *power managment*, *more data*, *order*, *duration*, *address1*, *address2*, *address3* e *sequence control*) dos quadros de gerenciamento, pois também faz parte da pesquisa ver o impacto destas informações na especificação de assinaturas para os ataques de DoS. Por último, insere em cada amostra sua respectiva categoria de reconhecimento.

A base de dados é criada pela captura de quadros de gerenciamento da rede WLAN utilizada nos experimentos, em que a rede esteve sob condição “normal”, sem ataques, e sob os ataques *chopchop*, deautenticação, duração e fragmentação.

Os ataques empregados nos ensaios são especificados da seguinte forma:

- *Chopchop* – amostras onde o atacante intercepta um quadro criptografado e utiliza a estação base para adivinhar o texto claro do quadro por meio de uma operação de chutes que é repetida até que todos os *bytes* do quadro interceptado sejam decifrados (BITTAU; RENDLEY; LACKEY, 2006).
- Deautenticação – amostras onde o atacante transmite para as estações cliente um quadro de deautenticação falsificado para indisponibilizar os serviços da rede (BELLARDO; SAVAGE, 2003).
- Duração – amostras onde o atacante envia um quadro com o campo NAV muito alto para impedir que qualquer estação cliente utilize o meio compartilhado para transmitir (BELLARDO; SAVAGE, 2003).

- Fragmentação – amostras onde o atacante utiliza a técnica de fragmentação/montagem executada pela estação base para descobrir a chave de fluxo empregada para criptografar os quadros numa rede WLAN (BITTAU; RENDLEY; LACKEY, 2006).

Essas quatro categorias usadas na geração dos ataques foram escolhidas porque elas exploram de forma efetiva as vulnerabilidades de disponibilidade nas redes 802.11 com criptografia Pré-RSN. Os ataques de duração e deautenticação afetam a capacidade da estação base de gerenciar o acesso à infraestrutura da rede (BELLARDO; SAVAGE, 2003). Os ataques de *chopchop* e fragmentação exploram as vulnerabilidades dos mecanismos criptográficos (WEP e WPA) para indisponibilizar os serviços da rede (BITTAU; RENDLEY; LACKEY, 2006).

Finalmente, aplica-se uma segunda etapa de pré-processamento de dados sobre a base WEP-WPA contendo as 17800 amostras, onde é realizada uma remoção dos quadros da fase de descoberta da rede (*beacon*, *probe request*, *probe response*), pois estes quadros causam ruído e afetam o desempenho do IDS (ARAÚJO et al., 2012). Sendo assim, a base de dados pré-processada contém 4250 registros representada na Tabela 11.

Tabela 11 - Distribuição das 4250 amostras coletadas na rede infraestruturada sem fio com criptografia WEP e WPA habilitadas.

			Conjuntos da Base de Dados	
			Treinamento	Teste
Categorias de Reconhecimento	Normal		216	106
	Anomalia	ChopChop	256	192
		Deautenticação	893	765
		Duração	899	798
		Fragmentação	42	83
Total de Amostras			2306	1944

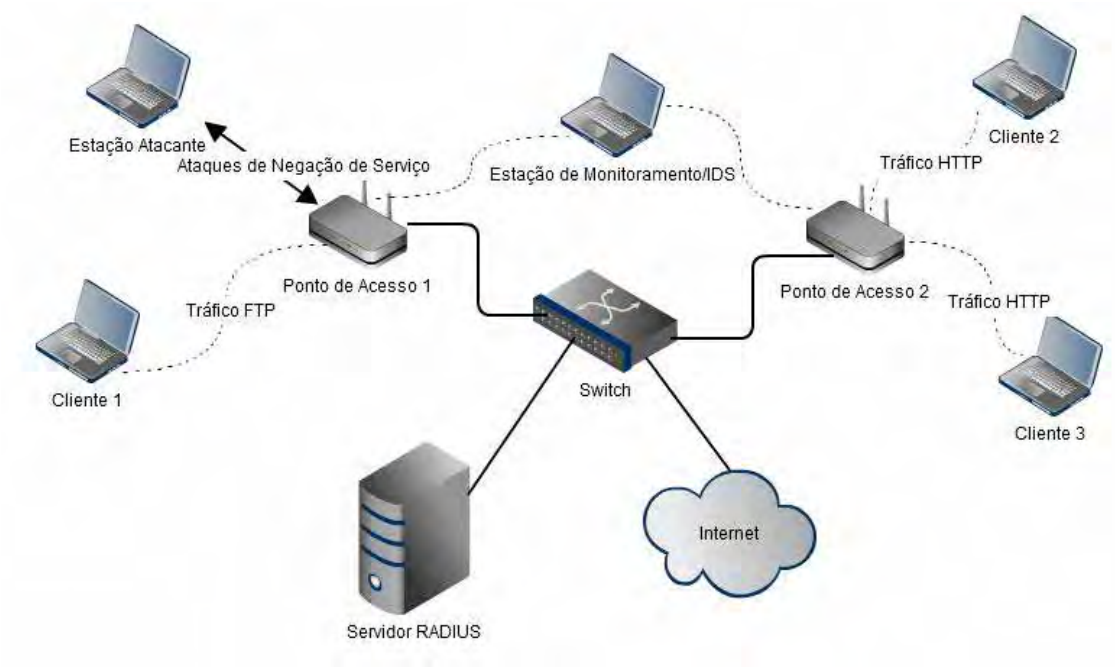
Fonte: Adaptado de Vilela et al. (2013).

5.1.3 Base de dados coletada de uma rede infraestruturada sem fio com criptografia WPA2 habilitada (WPA2)

A terceira base de dados é capturada de uma rede WLAN com criptografia WPA2 habilitada, cuja topologia (apresentada na Figura 24) segue a configuração de uma rede sem

fio com autenticação mútua e associação segura, normalmente, empregada em cenários corporativos.

Figura 24 - Topologia da rede WLAN com criptografia WPA2 habilitada.



Fonte: Adaptado de Vilela et al. (2013).

Este ambiente é composto por cinco estações sem fio, dois pontos de acesso e um servidor RADIUS. As estações-cliente geram tráfego normal na rede (HTTP, FTP). A estação-atacante emprega as ferramentas Aireplay (AIRCRACK, 2011), Hping3 (HPING, 2013) e FakeAP (BUTTI, 2013) para executar um conjunto de ataques de negação de serviço (*syn flooding*, *authentication flooding*, deautenticação e AP falso) na rede montada. A estação-monitoramento aplica a ferramenta Wireshark (WIRESHARK, 2011) para realizar o monitoramento dos dados e a ferramenta Tshark (TSHARK, 2013) realiza o pré-processamento dos dados para extrair somente as informações do cabeçalho MAC. Servidor RADIUS é responsável pelo controle de acesso à rede.

A composição dos registros deste conjunto de dados é semelhante da segunda base de dados, acrescido de dois campos: *short preamble* (indica se a estação/AP suporta este tipo de formato PPDU) e *protected frame* (identifica se o quadro está criptografado ou não). Sendo assim, a dimensão de um registro desta base contém 17 campos.

Os ataques empregados nos ensaios são especificados da seguinte forma:

- Deautenticação – semelhante ao ataque de deautenticação realizado no cenário da rede WLAN com criptografia WEP e WPA habilitadas.
- *Authenticantion flooding* – o atacante inunda o AP com solicitações de quadros de autenticação, se passando a cada tentativa de reconhecimento por um endereço MAC válido pertence à lista de clientes cadastradas nesta rede. Isto acaba afetando a capacidade de memória e processamento do AP, que termina negando serviços aos usuários legítimos (HE; MITCHELL, 2005).
- AP falso – o atacante cria um AP falso com o mesmo MAC e SSID do verdadeiro, para os clientes se associarem a ele (HE; MITCHELL, 2005).
- *Syn flooding* – o atacante envia um grande número de mensagens para um AP a uma alta taxa que o dispositivo não pode processá-las, isso faz com que outras estações não consigam acessar o canal (HE; MITCHELL, 2005).

Essas quatro categorias usadas na geração dos ataques foram escolhidas porque elas exploram de forma efetiva as vulnerabilidades de disponibilidade nas redes 802.11 com criptografia WPA2.

A base de dados contém 10000 registros, sendo particionados segundo o método *holdout* (FIELDING; BELL, 1997) numa proporção de 75% e 25%, respectivamente, nas bases de treinamento e teste, conforme apresentado na Tabela 12. Nesta base preferiu-se não aplicar a extração dos quadros de gerenciamento da fase de descoberta da rede para observar o comportamento dos resultados de classificação de padrões quando não há um pré-processamento sobre estes ruídos no conjunto de dados.

Tabela 12 - Distribuição das 10000 amostras coletadas na rede infraestruturada sem fio com criptografia WPA2 habilitada.

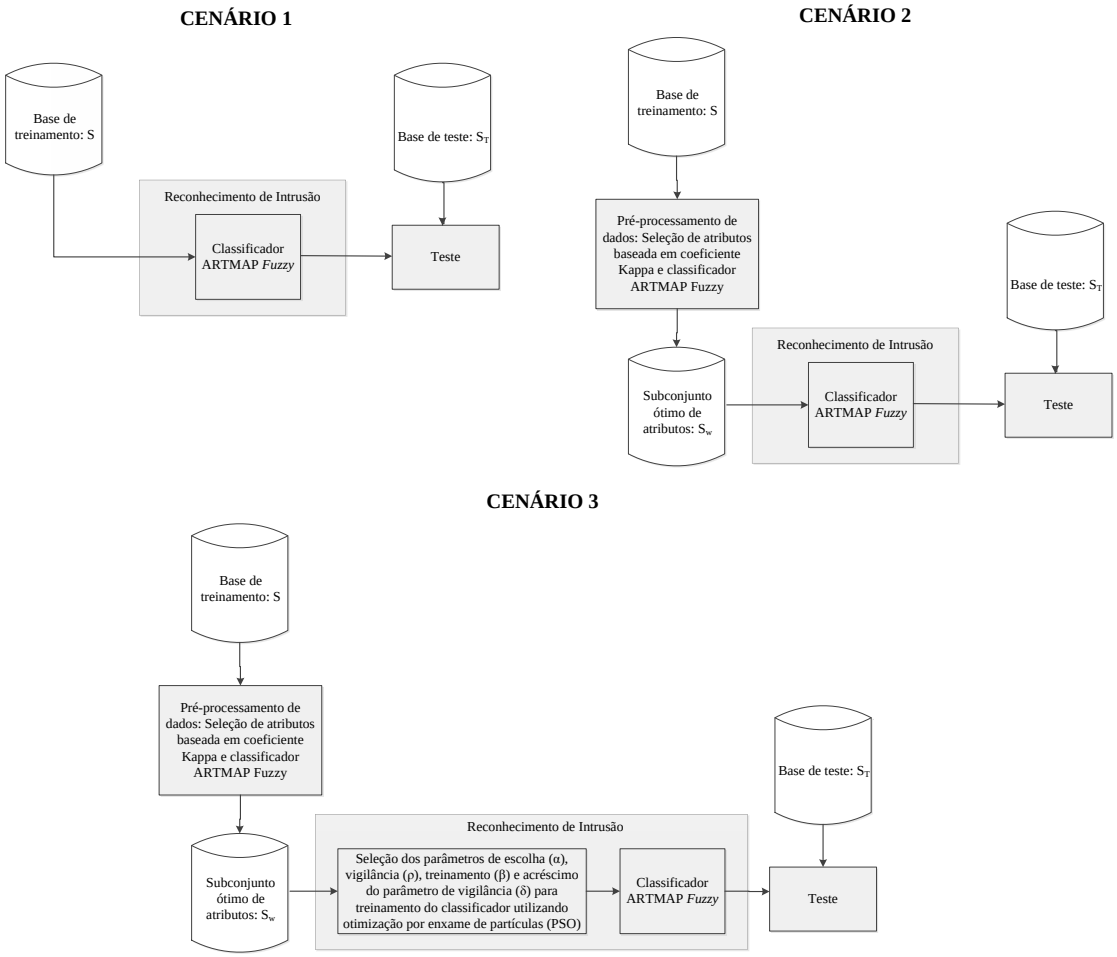
			Conjuntos da Base de Dados	
			Treinamento	Teste
Categorias de Reconhecimento	Normal		4500	1500
	Anomalia	Deautenticação	750	250
		Authentication flooding	750	250
		AP falso	750	250
		Syn flooding	750	250
Total de Amostras			7500	2500

Fonte: Adaptado de Vilela et al. (2013).

5.2 Investigando o desempenho do IDS Kappa-PSO-ARTMAP-*Fuzzy* sobre as bases de dados KDD99, WEP-WPA e WPA2

A avaliação do desempenho do IDS Kappa-PSO-ARTMAP *Fuzzy* é organizado, conforme apresentado na Figura 25, em três cenários: na primeira parte avalia-se somente o módulo do classificador ARTMAP *Fuzzy*; no próximo cenário adiciona-se na avaliação o pré-processamento por seleção de atributos baseada no coeficiente Kappa e na rede neural ARTMAP *Fuzzy*; e no último cenário acrescenta-se aos módulos anteriores a busca pelos parâmetros ótimos de configuração para o treinamento da rede neural ARTMAP *Fuzzy* utilizando a técnica de otimização por enxame de partículas (PSO).

Figura 25 - Organização dos cenários de avaliação do IDS Kappa-PSO-ARTMAP *Fuzzy*.



Fonte: Elaboração do próprio autor.

As métricas empregadas para analisar os cenários de avaliação da metodologia proposta nesta Tese são:

- Taxa de detecção - identifica a intensidade de amostras com comportamento intrusivo existente na rede monitorada;
- Taxa de falsos alarmes - apresenta a proporção de erro do classificador em reconhecer amostras normais como sendo intrusivas;
- Exatidão global - representa a capacidade do classificador em reconhecer corretamente amostras normais e intrusivas;
- Coeficiente Kappa – fornece uma idéia de quanto o resultado das previsões do classificador se afastam daquelas esperadas, indicando assim o quão legítimo essas interpretações são;
- Tempo – indica qual o tempo de processamento do IDS para executar todas as fases do cenário de avaliação;
- Número de atributos – apresenta a quantidade de atributos necessária para representar os comportamentos normal e intrusivo das amostras coletadas na rede monitorada.

As três primeiras métricas são comumente utilizadas na avaliação de desempenho de IDS, como já foi afirmado por diversos pesquisadores da área de detecção de intrusos em redes de computadores (WU; BANZHAF, 2010). O coeficiente Kappa é introduzido por ser uma das inovações apresentadas pelo trabalho na avaliação de IDS. A métrica tempo é aplicada para observarmos qual o impacto do custo computacional dos cenários investigados. Finalmente, a quantidade de atributos de cada conexão é empregada para representar a dimensão dos vetores utilizados no processamento do IDS.

Todas as simulações foram realizadas por meio da ferramenta de programação MATLAB (THE MATHWORKS, 2013) que se mostrou bastante eficiente no desenvolvimento dos cenários de avaliação.

Na Tabela 13 são apresentados os parâmetros do classificador ARTMAP *Fuzzy* empregados nos cenários de avaliação 1, 2 e 3 (somente no módulo de pré-processamento de dados). A utilização destes valores deve-se por empregar na rede neural um treinamento rápido ($\beta=1$), bem como, configurar o classificador para ser bastante sensível a alterações nos padrões de entrada que levam a uma boa decisão de classificação (ρ próximo de 1) (HUANG; GEORGIOPOULOS; HEILEMAN, 1995).

Tabela 13 - Parâmetros de configuração usados no classificador ARTMAP *Fuzzy*.

Parâmetros	Valor
Parâmetro de escolha (α)	0
Taxa de treinamento (β)	1
Parâmetro de vigilância da rede $ART_a(\rho_a)$	0,9
Parâmetro de vigilância da rede $ART_b(\rho_b)$	1
Parâmetro de vigilância do módulo inter-ART(ρ_{ab})	1
Acréscimo do parâmetro de vigilância da rede ART_a (δ)	0,01

Fonte: Adaptado de Malange (2010).

Com relação à configuração da PSO para a busca dos parâmetros ótimos no cenário 3 empregam-se os valores apresentados na Tabela 14. A utilização no processo de otimização destes valores para número de iterações (q) e partículas (P) deve-se pelo custo computacional, uma vez que um dos principais objetivos do nosso trabalho é pensar numa metodologia de IDS de baixo custo computacional, mas com alta capacidade de classificação correta (alta taxa de detecção e baixa taxa de falsos alarmes). O peso inercial inicial começa com um valor alto (próximo de 1) devido a PSO iniciar num processo de exploração, buscando uma região no espaço solução que possua bons valores de função objetivo (coeficiente Kappa).

Os parâmetros de configuração do classificador ARTMAP *Fuzzy* que não estão representados na posição da partícula (parâmetro de vigilância da rede ART_b e Parâmetro de vigilância do módulo inter-ART) possuem os mesmos valores indicados pela Tabela 13.

Tabela 14 - Parâmetros de configuração usados na PSO.

Parâmetros	Valor
Número de iterações (q)	10
Número de partículas da população (P)	5
Peso inercial inicial (w^0)	0,9
Velocidade máxima permitida (v_{max})	0,1

Fonte: Adaptado de Granger et al. (2007).

A seguir, mostram-se os resultados obtidos pelos cenários de avaliação nas bases de dados KDD99, WEP-WPA e WPA2.

5.2.1 Resultados obtidos sobre a base de dados KDD99

Aplicando os cenários de avaliação sobre a base de dados KDD99 obtém-se os resultados apresentados na Tabela 15.

Tabela 15 - Resultados obtidos dos cenários de avaliação sobre a base de dados KDD99.

Métricas de desempenho	Cenário 1 – ARTMAP *Fuzzy*	Cenário 2 – Kappa-ARTMAP *Fuzzy*	Cenário 3 – Kappa-PSO-ARTMAP *Fuzzy*
Taxa de detecção	93,93%	93,98%	93,98%
Taxa de falsos alarmes	3,26%	8,80%	3,97%
Exatidão global	94,72%	93,20%	94,56%
Kappa	0,87	0,83	0,87
Tempo	392,95s	46,49s	18,68s
Número de atributos	41	3	3

Fonte: Elaboração do próprio autor.

A primeira análise a ser expressa diz respeito ao uso do coeficiente Kappa como função objetivo do problema de detecção de intrusos, a escolha é muito acertada, pois a exatidão global oferece informações equivocadas sobre o desempenho do IDS. Uma prova disso é a elevação da taxa de falsos alarmes entre o cenário1 e o cenário 2. Há um crescimento de 170%, enquanto a exatidão global decresce 1,60%. Agora quando verifica-se o decréscimo do coeficiente Kappa, observa-se 4,6%. Isso demonstra uma maior sensibilidade do Kappa para mudanças na capacidade de classificação correta do IDS.

Ao aplicar o cenário 2 sobre a base KDD99 encontra-se os atributos mais relevantes do subconjunto ótimo, que são *src_bytes*, *dst_bytes* e *logged_in*. Estas características indicam que o comportamento intrusivo apresentado nas 10000 amostras coletadas sobre a base KDD99 é baseado na quantidade de *bytes* trocada entre as estações origem e destino e no sucesso ou insucesso na tentativa de conectar-se a rede monitorada.

O emprego do pré-processamento na base original mostra-se bastante eficiente, uma vez que o custo computacional é reduzido em 88%. No entanto, a taxa de falsos alarmes sofre um aumento vertiginoso que quase triplica quando comparado com a base original (41 atributos).

Este problema será atenuado com o emprego da busca pelos parâmetros ótimos para o treinamento do classificador ARTMAP *Fuzzy* (Cenário 3). O acréscimo de falsos alarmes no cenário 3 quando comparado com o cenário 1 é 22% maior, quase 2 vezes menor que no cenário 2. Vale salientar que mantem-se o subconjunto ótimo com 3 atributos e o custo computacional do IDS é reduzido em 95%, como pode ser observado na Tabela 16 que representa os resultados obtidos pelo classificador ARTMAP *Fuzzy* após o pré-processamento de dados e alimentado com a configuração ótima.

Tabela 16 - Resultados obtidos na configuração ótima do IDS Kappa-PSO-ARTMAP *Fuzzy* sobre a base KDD99.

Métricas de desempenho	Configuração ótima ($\alpha = 0{,}35;\ \beta = 0{,}77;\ \rho_a = 0{,}93;\ \rho_b = 1;\ \rho_{ab} = 1;\ \delta = 0{,}85$)
Taxa de detecção	93,98%
Taxa de falsos alarmes	3,97%
Exatidão global	94,56%
Kappa	0,87
Tempo	18,68s
Número de atributos	3

Fonte: Elaboração do próprio autor.

A metodologia IDS Kappa-PSO-ARTMAP *Fuzzy* sobre a base KDD99 consegue manter, praticamente, os mesmos níveis de classificação correta quando confrontada com uma solução de IDS sem pré-processamento de dados e otimização de parâmetros (cenário 1), com a grande vantagem de diminuir o custo computacional consideravelmente.

5.2.2 Resultados obtidos sobre a base de dados WEP-WPA

Aplicando os cenários de avaliação sobre a base de dados WEP-WPA obtém-se os resultados apresentados na Tabela 17.

Tabela 17 - Resultados obtidos dos cenários de avaliação sobre a base de dados WEP-WPA.

Métricas de desempenho	Cenário 1 – ARTMAP *Fuzzy*	Cenário 2 – Kappa-ARTMAP *Fuzzy*	Cenário 3 – Kappa-PSO-ARTMAP *Fuzzy*
Taxa de detecção	100,00%	96,95%	97,38%
Taxa de falsos alarmes	100,00%	6,60%	2,83%
Exatidão global	94,54%	96,75%	97,37%
Kappa	0	0,77	0,78
Tempo	7,54s	1,47s	1,58s
Número de atributos	15	1	1

Fonte: Elaboração do próprio autor.

A deficiência da exatidão global torna-se mais visível na base WEP-WPA devido à divisão de amostras entre normal e anomalia na base de teste ser bastante desbalanceada (5,5% de amostras normais e 94,5% de amostras anômalas). Por isso mesmo identificando todo o tráfego normal incorretamente e o tráfego anômalo corretamente, a métrica de exatidão

global aponta um valor muito alto (94,5%). Ao contrário do coeficiente Kappa que identifica a incapacidade do classificador ao registrar zero.

O uso de pré-processamento de dados no cenário 2 sobre a base WEP-WPA produz um subconjunto ótimo com o atributo *fromDS*. Esta característica demontra que o comportamento intrusivo existente na base WEP-WPA é originado a partir do ponto de acesso, que pode invadir as estações clientes associadas a esta rede, provocando desde o roubo de informações pessoais dessas máquinas até impedí-las de acessar os serviços da rede.

Além disso, a seleção do atributo *fromDS* para representar o perfil de comportamento de tráfego na base WEP-WPA resulta numa melhoria do problema da elevada taxa de falsos alarmes encontrada no cenário 1, atenuando este valor em 93,4%, sem causar este mesmo efeito na taxa de detecção. Como consequência, consegue-se um avanço no desempenho do coeficiente Kappa em 77% e uma diminuição no custo computacional do IDS em 80%.

Quando aplica-se o cenário 3 sobre a base WEP-WPA obtêm-se uma maior atenuação na taxa de falsos alarmes, reduzindo este valor em 97% quando confrontado com o cenário 1. A Tabela 18 mostra os resultados obtidos na configuração ótima do cenário 3 sobre a base WEP-WPA.

Tabela 18 - Resultados obtidos na configuração ótima do IDS Kappa-PSO-ARTMAP *Fuzzy* sobre a base WEP-WPA.

Métricas de desempenho	Configuração ótima ($\alpha = 0{,}30;\ \beta = 0{,}73;\ \rho_a = 0{,}78;\ \rho_b = 1;\ \rho_{ab} = 1;\ \delta = 0{,}07$)
Taxa de detecção	97,38%
Taxa de falsos alarmes	2,83%
Exatidão global	97,37%
Kappa	0,78
Tempo	1,58s
Número de atributos	1

Fonte: Elaboração do próprio autor.

A metodologia IDS Kappa-PSO-ARTMAP *Fuzzy* sobre a base WEP-WPA repete os bons resultados apresentados na avaliação da base KDD99, acrescentando um progresso na capacidade de classificação correta do IDS com o uso dos módulos de pré-processamento de dados e otimização de parâmetros, bem como a redução do custo computacional.

5.2.3 Resultados obtidos sobre a base de dados WPA2

Aplicando os cenários de avaliação sobre a base de dados WPA2 obtém-se os resultados apresentados na Tabela 19.

Tabela 19 - Resultados obtidos dos cenários de avaliação sobre a base de dados WPA2.

Métricas de desempenho	Cenário 1 – ARTMAP *Fuzzy*	Cenário 2 – Kappa-ARTMAP *Fuzzy*	Cenário 3 – Kappa-PSO-ARTMAP *Fuzzy*
Taxa de detecção	55,20%	51,10%	65,40%
Taxa de falsos alarmes	4,60%	0,33%	1,13%
Exatidão global	79,32%	80,24%	85,48%
Kappa	0,54	0,55	0,68
Tempo	86,68s	23,65s	17,14s
Número de atributos	17	3	3

Fonte: Elaboração do próprio autor.

A principal observação apresentada pelos resultados em todos os cenários de avaliação sobre a base WPA2 é a baixa taxa de detecção de intrusos (aproximadamente 45% menor que nas bases KDD99 e WEP-WPA). Uma possível razão para esta deficiência é o ruído na base de dados WPA2 e falta de representatividade dos atributos para a construção do perfil de anomalia.

O problema do ruído na base de dados atrapalhar o processo de reconhecimento de ataques já foi identificado na base WEP-WPA (ARAÚJO et al., 2012), por isso foi aplicado a extração dos quadros de gerenciamento da fase de reconhecimento da rede na base de dados.

Os atributos *short preamble*, *duration* e *subtype* são componentes do subconjunto ótimo gerado pelo cenário 2 sobre a base WPA2. Estas características demonstram que o comportamento intrusivo existente na base WPA2 tem os seguintes princípios:

- O ataque, provavelmente, ocorre por meio dos quadros de controle RTS e CTS, uma vez que para programar o tempo de duração cujo uma estação aloca o meio sem fio, estes quadros possuem essa função.
- O invasor utiliza quadro com prêambulo pequeno para realizar os ataques, que condiz com o tamanho dos quadros de controle RTS e CTS;
- O atacante consegue controlar o tempo que o meio sem fio estará reservado para a transmissão de uma determinada estação cliente associada, propiciando

perigosamente a indisponibilização dos serviços de rede para as estações legítimas;

Quando é confrontado os cenários 1 e 2, observa-se que a taxa de falsos alarmes consegue reduzir seus valores em 92%, mas prejudica a capacidade do classificador em reconhecer comportamento intrusivo, reduzindo a taxa de detecção em 7,42% .

A Tabela 20 mostra que a otimização dos parâmetros da rede neural ARTMAP *Fuzzy* ocasiona um avanço de 18% na identificação de amostras anômalas e uma redução do custo computacional em 80% na comparação com o cenário 1.

Tabela 20 - Resultados obtidos na configuração ótima do IDS Kappa-PSO-ARTMAP *Fuzzy* sobre a base WPA2.

Métricas de desempenho	Configuração ótima ($\alpha = 0{,}05;\ \beta = 1;\ \rho_a = 1;\ \rho_b = 1;\ \rho_{ab} = 1;\ \delta = 0{,}1$)
Taxa de detecção	65,40%
Taxa de falsos alarmes	1,13%
Exatidão global	85,48%
Kappa	0.68
Tempo	17,14s
Número de atributos	3

Fonte: Elaboração do próprio autor.

A metodologia IDS Kappa-PSO-ARTMAP *Fuzzy* mostra-se bastante efetiva sobre a base WPA2, confirmando a eficiência do coeficiente Kappa como função objetivo do problema de detecção de intrusos, a redução de atributos para mitigar o custo computacional do IDS e o uso da otimização de parâmetros para buscar uma configuração ótima para o treinamento do classificador. Os valores reduzidos de taxa de detecção não tiveram origem no baixo poder de classificação do IDS e sim devido a ruídos na base de dados que afetam a identificação correta das amostras.

5.3 Conclusões

As respostas obtidas pela metodologia Kappa-PSO-ARTMAP *Fuzzy* sobre as bases de dados analisadas demonstram que a utilização do coeficiente Kappa como medida de avaliação de desempenho de IDS é mais apropriada que a tradicional exatidão global, principalmente, quando a formação do conjunto de dados é muito desbalanceada. Outro fator

importante expressado pela análise do Kappa-PSO-ARTMAP *Fuzzy* aponta que a seleção de atributos surte efeitos positivos na redução do custo computacional do IDS, sem comprometer a capacidade de classificação correta. Além disso, a aplicação da técnica de PSO para encontrar os parâmetros ótimos para o treinamento do IDS ampliam os resultados positivos quanto ao custo computacional, a taxa de detecção e a taxa de falsos alarmes.

Apesar dos avanços apresentados no uso do Kappa-PSO-ARTMAP *Fuzzy* existe a necessidade de realizar uma verificação prévia da base de dados analisada, pois como é demonstrado nesta pesquisa (na base WPA2) os atributos selecionados para formar as amostras são essenciais para obter bons resultados na capacidade de classificação correta do IDS.

6 CONCLUSÕES E TRABALHOS FUTUROS

O emprego do coeficiente Kappa como medida de desempenho do IDS mostra-se bastante promissor sobre os cenários de avaliação investigados, principalmente, quando a base WEP-WPA é submetida sobre o classificador ARTMAP *Fuzzy* com ajuste padrão. Neste cenário, a exatidão global informa que a porcentagem de amostras identificadas corretamente atinge por volta de 94%, mas por outro lado todas as amostras normais são classificadas como ataques. O coeficiente Kappa demonstra um comportamento mais conservador, detectando o problema da alta taxa de falsos alarmes devido a isso pode-se concluir que este coeficiente Kappa apresenta uma maior sensibilidade na identificação correta das amostras. Outra percepção bastante evidente quanto ao uso da exatidão global para avaliação de IDS é a forte influência da classe de amostras que possui predomínio na base de dados. Isso vem confirmar que a exatidão global não é apropriada para aferir o desempenho de um classificador quando se submete base de dados altamente desbalanceada.

Com relação ao desempenho da metodologia Kappa-PSO-ARTMAP *Fuzzy* sobre as bases de dados analisadas, observa-se a necessidade de um pré-processamento mais rigoroso nas bases coletadas a partir de redes infraestruturadas sem fio, pois a utilização dos campos do cabeçalho MAC na definição do comportamento das amostras não demonstram ser muito eficaz, bem como, causam ruídos nas bases de dados ocasionando uma maior confusão por parte do classificador de padrões em identificar corretamente as amostras.

Este problema torna-se mais perceptível quando se contrapõem os resultados obtidos nos cenários de avaliação da base WEP-WPA (que passa por um processo mais preciso de pré-processamento) e a base WPA2 (onde apenas simplesmente extraíram-se os campos do cabeçalho MAC dos *logs* coletados). No cenário da configuração ótima do Kappa-PSO-ARTMAP *Fuzzy*, o coeficiente Kappa sobre a base WEP-WPA possui um desempenho 10% superior à base WPA2.

O combate ao custo computacional do IDS neste trabalho é desenvolvido pelo módulo de pré-processamento de dados que aplica a técnica de seleção de atributos sobre as bases de dados avaliadas. Os resultados obtidos atestam que a extração das características mais importantes da base original para a geração do subconjunto ótimo de atributos contribui para uma redução significativa no tempo de treinamento do IDS sem afetar o nível de classificação correta das amostras, exceto na base de dados coletada da rede cabeada (KDD99). Uma possível razão para o aumento da taxa de falsos alarmes na base KDD99 é o fato dos três

atributos pertencente ao subconjunto ótimo serem mais representativos ao perfil de comportamento de anomalia, retornando ao problema de especificação do limiar entre um comportamento normal e intrusivo.

A aplicação de otimização de parâmetros (PSO) na busca da configuração ótima do classificador ARTMAP *Fuzzy* expressa a importância deste mecanismo na melhoria das taxas de detecção e falsos alarmes do módulo de reconhecimento de intrusão. Quando utilizado o cenário Kappa-PSO-ARTMAP *Fuzzy* percebe-se em todas as bases de dados avaliadas neste trabalho um avanço ou manutenção no reconhecimento correto dos registros classificados, em conjunto com uma diminuição expressiva no custo computacional decorrido do processamento destas classificações.

A limitação da otimização computacional da PSO em 5 partículas e 10 iterações pode ter restringido a busca por valores ótimos no espaço solução, mas a priorização em atenuar o custo computacional nos leva a investigar um conjunto mais reduzido de partículas e iterações.

Em geral, o uso do classificador ARTMAP *Fuzzy* nas diversas fases da metodologia de detecção de intrusos proposta nesta tese apresenta um desempenho animador, demonstrando que a característica de estabilidade-plasticidade (reter os padrões assimilados e aprender padrões desconhecidos) comprova-se eficiente para o problema de detecção de intrusos, ainda mais quando procura um ajuste ótimo para o treinamento desta rede neural.

Após essas análises conclui-se que o objetivo inicial de desenvolver um IDS onde houvesse uma priorização na diminuição do custo computacional sem acarretar problemas na identificação correta das amostras classificadas e possuísse uma abrangência de aplicação sobre redes cabeadas e sem fio foi alcançado.

A partir dos resultados obtidos nesta pesquisa, sugestões para trabalhos futuros podem ser os seguintes tópicos:

- Comparação do Kappa-PSO-ARTMAP-*Fuzzy* com metodologias de detecção de intrusos que abordem outras técnicas de inteligência computacional (redes neurais artificiais, sistemas *Fuzzy*, computação evolucionária, sistemas imuno-artificiais, inteligência de enxame e *soft computing*);
- Aprofundar a investigação na definição de atributos que melhor definam os comportamentos de tráfego nas redes infraestrururada sem fio com segurança habilitada;
- Implementar e coletar dados de uma rede WLAN com suporte a emenda de segurança IEEE 802.11w;

- Aplicar e ajustar a metodologia Kappa-PSO-ARTMAP-*Fuzzy* sobre outros tipos de tecnologias de rede (redes *adhoc* sem fio, redes sensores sem fio, dentre outras);
- Investigar o desempenho da metodologia Kappa-PSO-ARTMAP *Fuzzy* na segurança em redes Smart Grids;
- Examinar a metodologia Kappa-PSO-ARTMAP *Fuzzy* na área de Forense Computacional;
- Procurar técnicas de pré-processamento de dados que busquem mitigar o problema do ruído nas bases de dados de detecção de intrusos.

REFERÊNCIAS

ABOBA, B. et al. **IETF RFC 3748:** Extensible Authentication Protocol (EAP). New York: IETF, 2004. Disponível em: <http://www.ietf.org/rfc/rfc3748.txt>. Acesso em: 12 maio 2012.

AHMAD, M. S.; TADAKAMADLA, S. Short paper: security evaluation of IEEE 802.11w specification. In: THE ACM CONFERENCE ON WIRELESS NETWORK SECURITY, 4., 2011, Hamburgo. **Proceedings…** New York: ACM, 2011. p. 53-58. Disponível em: <http://dl.acm.org/citation.cfm?id=1998424>. Acesso em: 5 maio 2012.

AIRCRACK. **Aircrack.** 2011. Disponível em: <http://www.aircrack-ng.org/>. Acesso em: 9 out. 2011.

ARAUZO-AZOFRA, A.; AZNARTE, J. L.; BENÍTEZ, J. M. Empirical study of feature selection methods based on individual feature evaluation for classification problems. **Expert Systems With Applications**, Kidlington, v. 38, n. 7, p. 8170-8177, 1 July 2011. Disponível em: <http://www.sciencedirect.com/science/article/pii/S095741741001523X>. Acesso em: 18 abr. 2013.

BELLARDO, J.; SAVAGE, S. 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In: CONFERENCE ON USENIX SECURITY SYMPOSIUM, 12., 2003, Washington-DC. **Proceedings…**Washington-DC: Usenix, 2003. p. 15-28. Disponível em: <http://static.usenix.org/event/sec03/tech/full_papers/bellardo/bellardo_html/>. Acesso em: 10 maio 2013.

BICAKCI, K.; TAVLI, B. Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks. **Computer Standards & Interfaces**, New York, v. 31, n. 5, p. 931-941, Sept. 2009. Disponível em: <http://bicakci.etu.edu.tr/dos_csi.pdf>. Acesso em: 5 maio 2012.

BITTAU, A.; HANDLEY, M.; LACKEY, J.. The final nail in WEP. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2006, Berkeley. **Proceedings…**Piscataway: IEEE, 2006. p. 386-400. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1624028>. Acesso em: 10 maio 2013.

BOUCKAERT, R. R. et al. **WEKA manual for version 3-7-0.** Waikato: Weka, 2009. Disponível em: <http://www.cs.waikato.ac.nz/ml/weka/>. Acesso em: 20 agosto 2011.

BSILA, A.; GOMBAULT, S.; BELGHITH, A. Improving traffic transformation to detect novel attacks. In: INTERNATIONAL CONFERENCE: SCIENCES OF ELETRONIC, TECHNOLOGIES OF INFORMATION AND TELECOMMUNICATIONS, 4., 2007, Tunisia. **Proceedings…** Tunisia: SETIT, 2007. 8 p. Disponível em: <http://ww.setit.rnu.tn/last_edition/setit2007/R/178.pdf>. Acesso em: 10 maio 2013.

BUTTI, L. **Raw fake AP 0.2.** 2013. Disponível em: <http://linux.softpedia.com/get/Security/Raw-Fake-AP-6440.shtml>. Acesso em: 08 maio 2013.

CARPENTER, G. A.; GROSSBERG, S. A massively parallel architecture for a self-organization neural pattern recognition machine. **Computer Vision, Graphics, And Image Processing**, Maryland Heights, v. 37, p.54-115, 1987. Disponível em: <http://cns.bu.edu/Profiles/Grossberg/CarGro1987CVGIP.pdf>. Acesso em: 3 jul. 2012.

CARPENTER, G. A.; GROSSBERG, S. ART2: Self-organization of stable category recognition codes for analog input patterns. **Applied Optics:** Special Issue on Neural Networks, Washington-DC, v. 26, p. 4919-4930, 1987. Disponível em: <http://ce.sharif.ir/courses/85-86/2/ce667/resources/root/08%20-%20ART/ART2.pdf>. Acesso em: 3 jul. 2012.

CARPENTER, G. A.; GROSSBERG, S. The ART of adaptive pattern recognition by a self-organizing neural network. **Computer**, Piscataway, v. 21, n. 3, p. 77-88, Março 1988. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=33&isnumber=4>. Acesso em: 29 jun. 2012.

CARPENTER, G. A.; GROSSBERG, S.; REYNOLDS, J. H. ARTMAP: supervised real-time learning and classification of nonstationary data by a self-organizing neural network. **Neural Networks**, Kidlington, v. 4, n. 5, p. 565-588, 1991. Disponível em: <http://techlab.bu.edu/files/resources/articles_cns/CarpenterGrossbergReynolds1991.pdf>. Acesso em: 3 jul. 2012.

CARPENTER, G. A.; GROSSBERG, S.; ROSEN, D. B. Fuzzy ART: fast stable learning and categorization of analog patterns by an adaptive resonance system. **Neural Networks**, Kidlington , v. 4, n. 6, p. 759-771, 1991. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.64.2379>. Acesso em: 3 jul. 2012.

CARPENTER, G. A. et al. Fuzzy ARTMAP: a neural network architecture for incremental supervised learning of analog multidimensional maps. **IEEE Transactions on Neural Networks**, Piscataway, v. 3, n. 5, p. 698-713, Sept. 1992. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=159059&isnumber=4097>. Acesso em: 29 jun. 2012.

CHEN, Y. et al. Survey and taxonomy of feature selection algorithms in intrusion detection system. **Lecture Notes In Computer Science**, Heidelberg, v. 4318, p.153-167, 2006. Disponível em: <http://link.springer.com/chapter/10.1007/11937807_13>. Acesso em: 10 maio 2013.

COHEN, J. A coefficient of agreement for nominal scales. **Educational and Psychological Measurement**, Thousand Oaks, v. 20, n. 1, p. 37-46, 1 Abr. 1960. Disponível em: <http://dx.doi.org/10.1177/001316446002000104>. Acesso em: 22 abr. 2013.

DANZINGER, M.; LIMA NETO, F. B. A hybrid approach for IEEE 802.11 intrusion detection based on AIS, MAS and Naive Bayes. In: INTERNATIONAL CONFERENCE ON HYBRID INTELLIGENT SYSTEMS, 10., 2010, Atlanta. **Proceedings…** Piscataway: IEEE, 2010. p. 201-204. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5600083>. Acesso em: 10 maio 2013.

EL-KHATIB, K. Impact of feature reduction on the efficiency of wireless intrusion detection systems. **IEEE Transactions on Parallel and Distributed Systems**, Piscataway, v. 21, n. 8, p. 1143-1149, 2010. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5226620>. Acesso em: 10 maio 2013.

FAYSSAL, S.; HARIRI, S.; AL-NASHIF, Y. Anomaly-based behavior analysis of wireless network security. In: INTERNATIONAL CONFERENCE ON MOBILE AND UBIQUITOUS SYSTEMS: NETWORKING SERVICES, 4., 2007, Philadelphia. **Proceedings…** Piscataway: IEEE, 2007. 8 p. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4451054>. Acesso em: 10 maio 2013.

FIELDING, A. H.; BELL, J. F. A review of methods for the assessment of prediction errors in conservation presence/absence models. **Environmental Conservation**, Cambridge, v. 1, n. 24, p.38-49, 01 mar. 1997. Disponível em: <http://journals.cambridge.org/download.php?file=%2FENC%2FENC24_01%2FS0376892997000088a.pdf&code=86760416779be6256ca4bcf617ba24df>. Acesso em: 8 maio 2013.

GILL, R.; SMITH, J.; CLARK, A. Specification-based intrusion detection in WLANs. In: COMPUTER SECURITY APPLICATIONS CONFERENCE, 22., 2006, Miami Beach. **Proceedings…** Piscataway: IEEE, 2006. p. 141-150. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4041162>. Acesso em: 10 maio 2013.

GILL, R. S. **Intrusion detection techniques in wireless local area networks.** 2009. 264 f. Information Technology (Doctor Of Philosophy) - Faculty de Information Technology, Queensland University Of Technology, Queensland, 2009. Disponível em: <http://eprints.qut.edu.au/29351/1/Rupinder_Gill_Thesis.pdf>. Acesso em: 5 abr. 2012.

GRANGER, E. et. al. Supervised learning of Fuzzy ARTMAP neural networks through Particle Swarm Optimization. **Journal of Pattern Recognition Research**, San Diego, v. 2, n. 1, p. 27-60, 2007. Disponível em:<http://www.jprr.org/index.php/jprr/article/view/23/12>. Acesso em: 1 ago. 2012.

GUENNOUN, M.; LBEKKOURI, A.; EL-KHATIB, K. Optimizing the feature set of wireless intrusion detection systems. **International Journal of Computer Science and Network Security,** Seoul, p. 127-131. 2008. Disponível em: <http://paper.ijcsns.org/07_book/html/200810/200810019.html>. Acesso em: 10 maio 2013.

GUYON, I.; ELISSEEFF, A. An introduction to variable and feature selection. **Journal of Machine Learning Research**, Cambridge, v. 3, p.1157-1182, 3 Jan. 2003. Disponível em: <http://dl.acm.org/citation.cfm?id=944919.944968>. Acesso em: 18 abr. 2013.

HABIB, S. J.; ALKAZEMI, B. S. Comparative study between the internal behavior of GA and PSO through problem-specific distance functions. In: IEEE CONGRESS ON EVOLUTIONARY COMPUTATION, 2005, Edinburgh. **Proceedings...** Piscataway: IEEE, 2005. p. 2190-2195. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1554966>. Acesso em: 10 maio 2013.

HADDADI, F.; SARRAM, M. Wireless intrusion detection system using a lightweight agent. In: INTERNATIONAL CONFERENCE ON COMPUTER AND NETWORK TECHNOLOGY, 2., 2010, Bangkok. **Proceedings…**Piscataway: IEEE, 2010. p. 84-87.

Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5474532>. Acesso em: 10 maio 2013.

HE, C.; MITCHELL, J. C. Security analysis and improvements for IEEE 802.11i. In: ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, 12., 2005, San Diego. **Proceedings…**Stanford: Internet Society, 2005. p. 90-110. Disponível em: <http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf>. Acesso em: 8 maio 2013.

HPING. **Hping.** Disponível em: <http://www.hping.org/>. Acesso em: 08 maio 2013.

HUANG, J.; GEORGIOPOULOS, M.; HEILEMAN, G. Fuzzy ART properties. **Neural Networks**, Kidlington, v. 8, n. 2, p. 203-213, 1995. Disponível em: <http://www.sciencedirect.com/science/article/pii/089360809400073U>. Acesso em: 3 jul. 2012.

IDC BRASIL. **Mercado de tablets no Brasil foi o que mais cresceu em 2012, revela estudo da IDC.** São Paulo, 2013. Disponível em: <http://br.idclatin.com/releases/news.aspx?id=1457>. Acesso em: 1 mar. 2013.

IDC BRASIL. **Mercado brasileiro de celulares encerrou 2012 com a marca de 59,5 milhões de unidades comercializadas, segundo estudo da IDC.** São Paulo, 2013. Disponível em: <http://br.idclatin.com/releases/news.aspx?id=1458>. Acesso em: 1 mar. 2013.

IDC BRASIL. **Segundo estudo da IDC, mercado brasileiro de computadores comercializou 30 unidades por minuto em 2012.** São Paulo, 2013. Disponível em: <http://br.idclatin.com/releases/news.aspx?id=1459>. Acesso em: 1 mar. 2013.

INSTITUTE OF ELETRICAL AND ELETRONICS ENGINEERS – IEEE. **IEEE Std 802.11™ – 1999**: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). Piscataway: IEEE, 1999. 1184 p. Disponível em: <http://www.cs.mun.ca/~yzchen/bib/802.11-2007.pdf>. Acesso em: 10 maio 2013.

INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS - IEEE. **IEEE Std 802.1X-2001:** IEEE Standard for local and metropolitan area networks - port-based network acess control. Piscataway: IEEE, 2001. 999 p. Disponível em: <http://www.dmi.unipg.it/~bista/didattica/reti/seminari-reti-2007-08/802-1-x.pdf>. Acesso em: 12 abr. 2012.

INSTITUTE OF ELETRICAL AND ELETRONICS ENGINEERS – IEEE. **IEEE Std 802.11i™ – 2004**: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY): Medium Access Control (MAC) Security Enhancements. Piscataway: IEEE, 2004. 175 p. Disponível em: <http://www.stephan-robert.ch/attachments/File/TIN08/802-11i-2004.pdf>. Acesso em: 12 abr. 2012.

INSTITUTE OF ELETRICAL AND ELETRONICS ENGINEERS – IEEE. **IEEE Std 802.11w™ – 2009**: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY): Protected Management Frames. Piscataway: IEEE, 2009. 91 p. Disponível em:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5278657>. Acesso em: 12 abr. 2012.

KAYACIK, H. G.; ZINCIR-HEYWOOD, A. N.; HEYWOOD, M. I. Selecting features for intrusion detection: a feature relevance analysis on KDD 99. In: ANNUAL CONFERENCE ON PRIVACY, SECURITY AND TRUST, 3., 2005, [S.l]. **Proceedings…**[S.l.: s.n.], 2005. Disponível em: <ftp://ppp-5.cs.um.edu.mt/PhD/Project/Research/Papers/K99features2.PDF>. Acesso em: 10 maio 2013.

KENNEDY, J.; EBERHART, R. Particle swarm intelligence. In: IEEE INTERNATIONAL CONFERENCE ON NEURAL NETWORKS, 1995, Washington-DC. **Proceedings…**Piscataway: IEEE, 1995. v. 4, p. 1942-1948. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=488968&isnumber=10434>. Acesso em: 1 ago. 2012.

KHOSHGOFTAAR, T. et al. Intrusion detection in wireless networks using clustering techniques with expert analysis. In: INTERNATIONAL CONFERENCE ON MACHINE LEARNING AND APPLICATIONS, 4., 2005, Los Angeles. **Proceedings…** Piscataway: IEEE, 2005. p. 120-125. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1607440>. Acesso em: 10 maio 2013.

KOLIAS, C.; KAMBOURAKIS, G.; MARAGOUDAKIS, M. Swarm intelligence in intrusion detection: A survey. **Computer & Security**, Kidlington, v. 30, n. 8, p. 625-642, nov. 2011. Disponível em: <http://www.sciencedirect.com/science/article/pii/S016740481100109X>. Acesso em: 10 maio 2013.

KUBAT, M.; HOLTE, R. C.; MATWIN, S. Machine learning for the detection of oil spills in satellite radar images. **Machine Learning**, New York, v. 30, n. 2-3, p. 195-215, 1 Feb. 1998. Disponível em: <http://dx.doi.org/10.1023/a:1007452223027>. Acesso em: 22 abr. 2013.

LASHKARI, A. H.; MANSOOR, M.; DANESH, A. S. Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). In: INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING SYSTEMS, 2009, Kuala Lumpur. **Proceedings…** Piscataway: IEEE, 2009. p. 445-449. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5166826>. Acesso em: 09 maio 2012.

LERNER, B.; GUTERMAN, H. Advanced developments and applications of the fuzzy ARTMAP neural network in pattern classification. **Studies In Computational Intelligence**, Berlin, v. 137, p.77-107, 2008. Disponível em: <http://link.springer.com/chapter/10.1007/978-3-540-79474-5_4>. Acesso em: 10 maio 2013.

LINHARES, A. G.; GONÇALVES, P. A. da S. **Uma análise dos mecanismos de segurança de redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w**. Recife: UFPE, 2012. Disponível em: <http://www.cin.ufpe.br/~pasg/gpublications/LiGo06.pdf>. Acesso em: 14 maio 2012.

LIPPMANN, R. Pattern classification using neural networks. **IEEE Communication Magazine**, Piscataway, v. 27, n. 11, p.47-62, 1989. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=41401>. Acesso em: 10 maio 2013.

LIPPMANN, R. et al. The 1999 DARPA off-line intrusion detection evaluation. **Computer Networks**, Amsterdam, v. 34, n. 4, p. 579-595, 2000. Disponível em <http://www.sciencedirect.com/science/article/pii/S1389128600001390>. Acesso em: 10 maio 2013.

LIU, H.; YU, L. Toward integrating feature selection algorithms for classification and clustering. **IEEE Transactions on Knowledge and Data Engineering**, Piscataway, v. 17, n. 4, p. 491-502, 1 Apr. 2005. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1401889&isnumber=30435>. Acesso em: 20 abr. 2013.

LIU, Y.; TIAN, D.; LI, B. A wireless intrusion detection method based on dynamic growing neural network. In: INTERNATIONAL MULTI-SYMPOSIUMS ON COMPUTER AND COMPUTATIONAL SCIENCES, 1., 2006, Hangzhou. **Proceedings…** Piscataway: IEEE, 2006. p. 611-615. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4673773>. Acesso em: 10 maio 2013.

LOPES, M. L. M. **Desenvolvimento de redes neurais para previsão de cargas elétricas de sistemas de energia elétrica.** 2005. 149 f. Tese (Doutorado em Engenharia Elétrica) - Faculdade de Engenharia, Universidade Estadual Paulista Júlio de Mesquita Filho, Ilha Solteira, 2005. Disponível em: <http://www.athena.biblioteca.unesp.br/exlibris/bd/bis/33004099080P0/2005/lopes_mlm_dr_ilha.pdf>. Acesso em: 29 abr. 2013.

MAIMOM, O.; ROKACH, L. **Decomposition methodology for knowledge discovery and data mining:** theory and applications. New Jersey: World Scientific, 2005. Disponível em: <http://link.springer.com/chapter/10.1007/0-387-25465-X_46>. Acesso em: 10 maio 2013.

MAKANJU, A.; LAROCHE, P.; ZINCIR-HEYWOOD, A. N. A Comparison between signature and GP-based IDSs for link layer attacks on WiFi networks. In: IEEE SYMPOSIUM SERIES ON COMPUTATIONAL INTELLIGENCE, 2007, Honolulu. **Proceedings…** Piscataway: IEEE, 2006. p. 213-219. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4219103>. Acesso em: 10 maio 2013.

MALANGE, F. C. V. **Rede Neuro-Fuzzy-Wavelet para detecção e classificação de anomalias de tensão em sistemas elétricos de potência.** 2010. f. Tese (Doutorado em Engenharia Elétrica) – Faculdade de Engenharia, Universidade Estadual Paulista Júlio de Mesquita Filho, Ilha Solteira, 2010. Disponível em: <http://dee.feis.unesp.br/Home/departamentos/engenhariaeletrica/pos-graduacao/065-tese_fernando_malange.pdf >. Acesso em: 10 maio 2013.

MAR, J.; YEH, Y.-C..; HSIAO, I.-F. An ANFIS-IDS against deauthentication DOS Attacks for a WLAN. In: INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY AND ITS APPLICATIONS, 2010, Taichung. **Proceedings…** Piscataway: IEEE, 2010. p. 548-553. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5654405>. Acesso em: 10 maio 2013.

MCQUEEN, J. Some methods for classification and analysis of multivariate observations. In: BERKELEY SYMPOSIUM ON MATHEMATICAL STATISTICS AND PROBABILITY, 5., 1967, Berkeley. **Proceedings…** Berkeley: University of California Press, 1967. p. 281-

297. Disponível em: <http://www-m9.ma.tum.de/foswiki/pub/WS2010/CombOptSem/kMeans.pdf>. Acesso em: 10 maio 2013.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. **Advanced Encryption Standard.** Gaithersburg, 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>. Acesso em: 10 maio 2012.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. **Establishing wireless robust security networks:** a guide to IEEE 802.11i. Gaithersburg, 2007. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf>. Acesso em: 7 maio 2012.

NETGEAR. **WEP Shared Key Authentication.** 2012. Disponível em: <http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-09.html>. Acesso em: 27 abr. 2012.

POLI, R.; KENNEDY, J.; BLACKWELL, T. Particle swarm optimization: an overview. **Swarm Intelligence**, Berlin, v. 1, n. 1, p. 33-57, 1 Aug. 2007. Disponível em: <http://dx.doi.org/10.1007/s11721-007-0002-0>. Acesso em: 29 abr. 2013.

PORTO, V. W. et al. Lecture notes in computer science: evolutionary programming VII. In: EBERHART, R. C.; SHI, Y. **Comparison between genetic algorithms and particle swarm optimization.** Berlin: Springer, 1998. p. 611-616. Disponível em: <http://link.springer.com/chapter/10.1007/BFb0040812>. Acesso em: 27 abril 2013.

RIGNEY, C.; WILLENS, S. **IETF RFC 2865:** Remote Authentication Dial in User Service (RADIUS). New York: Ietf, 2000. Disponível em: <http://www.ietf.org/rfc/rfc2865.txt>. Acesso em: 7 maio 2012.

SANTRA, A. K.; NAGARAJAN, S.; JINESH, V. N. Intrusion detection in wireless networks using fuzzy neural networks and dynamic context-aware role based access control security (DCARBAC). **International Journal of Computer Applications,** New York, v. 39, n. 4, p. 23-31, 2012. Disponível em: <http://research.ijcaonline.org/volume39/number4/pxc3877002.pdf>. Acesso em: 11 maio 2013.

SCHNEIDER, B. **Applied cryptography:** protocols, algorithms and source code in C. Nova York: John Wiley & Sons, 1996. Disponível em: <http://gov.wiley.com/remtitle.cgi?isbn=0471117099>. Acesso em: 11 maio 2013.

SERAPIÃO, A. B. de S. Fundamentos de otimização por inteligência de enxames: uma visão geral. **SBA Controle e Automação**, Campinas, v. 20, n. 3, p. 271-304, 1 set. 2009. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-17592009000300002&lng=en&nrm=iso>. Acesso em: 29 abr. 2013.

SETTLES, M.; RODEBAUGH, B.; SOULE, T. Comparison of genetic algorithm and particle swarm optimizer when evolving a recurrent neural network. In: GENETIC AND EVOLUTIONARY COMPUTATION CONFERENCE, 2003, Chicago. **Proceedings…** Berlin: Springer Berlin Heidelberg, 2003. p. 148-149. Disponível em: <http://link.springer.com/chapter/10.1007/3-540-45105-6_17>. Acesso em: 11 maio 2013.

SOARES, J. de A. **Pré-processamento em mineração de dados:** um estudo comparativo em complementação. 2007. f. Tese (Doutorado) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2007.

SOBH, T. S. Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art. **Computer Standards & Interfaces**, New York, v. 28, n. 6, p. 670-694, Sep. 2006. Disponível em: <http://www.sciencedirect.com/science/article/pii/S092054890500098X >. Acesso em: 14 maio 2012.

SOUZA, E. P. **Estudo sobre sistemas de detecção de intrusão por anomalias:** uma abordagem utilizando redes neurais. 2008. f. Dissertação (Mestrado) - Universidade de Salvador, Salvador, 2008. Disponível em: <http://xa.yimg.com/kq/groups/21601917/1740343897/name/wgrs7.pdf>. Acesso em: 11 maio 2013.

TANG, H.-R.; SUN, R.-L.; KONG, W.-Q. Wireless intrusion detection for defending against TCP SYN flooding attack and man-in-the-middle attack. In: INTERNATIONAL CONFERENCE ON MACHINE LEARNING AND CYBERNETICS, 8., 2009, Toronto. **Proceedings…** Piscataway: IEEE, 2009. p. 1464-1470. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5212317>. Acesso em: 11 maio 2013.

THE MATHWORKS. **MATLAB.** Disponível em: <http://www.mathworks.com/products/matlab/>. Acesso em: 23 jun. 2013.

TSAI, C.-F. et al. Intrusion detection by machine learning: a review. **Expert Systems With Applications**, Kidlington, v. 36, n. 10, p. 11994-12000, 1 Dec. 2009. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0957417409004801>. Acesso em: 18 abr. 2013.

TSHARK. **Tshark.** 2013. Disponível em: <http://www.wireshark.org/docs/man-pages/tshark.html>. Acesso em: 08 maio 2013.

VILAKAZI, C. B.; MARWALA, T. Application of feature selection and fuzzy ARTMAP to intrusion detection. In: CONFERENCE INTERNATIONAL ON SYSTEMS, MAN AND CYBERNETICS, 2007, Montreal. **Proceedings…** Piscataway: IEEE, 2007. p. 4880-4885. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4274687>. Acesso em: 11 maio 2013.

YAO, X. Evolving artificial neural networks. **Proceedings of the IEEE**,Piscataway, v. 87, n. 9, p. 1423-1447, 1 Sep. 1999. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=784219&tag=1>. Acesso em: 7 ago. 2012.

WALKER, J. **Unsafe at any key size:** an analysis of the WEP encapsulation. IEEE 802.11-00/362. PIscataway: IEEE, 2000.

WELCH, D.; LANTHROP, S. Wireless security threat taxonomy. In: INTERNATIONAL WORKSHOP ON INFORMATION ASSURANCE, 1., 2003, West Point. **Proceedings…** Piscataway: IEEE, 2003. p. 76-83. Disponível em:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1232404&userType=&tag=1>. Acesso em: 14 maio 2012.

WHITLEY, D.; STARKWEATHER, T.; BOGART, C. Genetic algorithms and neural networks: optimizing connections and connectivity. **Parallel Computing**, Amsterdam, v. 3, n. 14, p. 347-361, Aug. 1990. Disponível em: <http://www.sciencedirect.com/science/article/pii/016781919090086O>. Acesso em: 7 ago. 2012.

WHITING, D.; HOUSLEY, R.; FERGUSON, N. **Counter with CBC-MAC (CCM).** Gaithersburg, NIST, 2003. Disponível em: <http://csrc.nist.gov/encryption/modes/proposedmodes/ccm/ccm.pdf>. Acesso em: 2 maio 2012.

WIRESHARK. **Wireshark.** [S.l.], 2011. Disponível em: <http://www.wireshark.org/>. Acesso em: 9 out. 2011.

WU, S. X.; BANZHAF, W. The use of computational intelligence in intrusion detection systems: a review. **Applied Soft Computing**, New York, v. 10, n. 1, 35 p., Jan. 2010. Disponível em: <http://www.mun.ca/computerscience/research/MUN-CS-2008-05.pdf>. Acesso em: 2 abr. 2012.

APÊNDICE A - Artigos publicados, aceitos e em submissão relacionados a presente tese.

ARAÚJO, Nelcileno et al. Otimizando a base de dados de detecção de intrusão KDD 99 por meio da seleção de atributos com abordagem híbrida. In: CONGRESSO IBERO-LATINO-AMERICANO DE MÉTODOS COMPUTACIONAIS EM ENGENHARIA, 30., 2009, Armação de Búzios. **Anais...** Armação de Búzios: [s.n.], 2009. CD-ROM.

ARAÚJO, Nelcileno et al. Identificando características importantes na base de dados de detecção de intrusão KDD99 por meio da seleção de atributos com abordagem híbrida. In: INTERNATIONAL INFORMATION AND TELECOMMUNICATION TECHNOLOGIES SYMPOSIUM, 8., 2009, Florianópolis. **Proceedings…** Florianópolis: [s.n.], 2009. CD-ROM.

ARAÚJO, Nelcileno et al. Identifying important characteristics in the KDD99 intrusion detection dataset by feature selection using a hybrid approach. In: IEEE INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS, 17., 2010, Dubai. **Proceedings…** Piscataway: IEEE, 2010. p. 552-558. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5478852>. Acesso em: 10 maio 2013.

ARAÚJO, Nelcileno et al. Investigando o desempenho do classificador ARTMAP fuzzy na detecção de intrusos. In: INFORMATION AND TELECOMMUNICATION TECHNOLOGIES CONFERENCE, 9., 2010, Rio de Janeiro. **Proceedings…** Rio de Janeiro: [s.n.], 2010. CD-ROM.

ARAÚJO, Nelcileno et al. Performance evaluation of the fuzzy ARTMAP for network intrusion detection. In: THAMPI, S. M. et al. **Recent trends in computer networks and distributed systems security:** International Conference on Security in Computer Networks and Distributed Systems, 2012, Trivandrum. Londres: Springer, 2013. p. 23-34.Disponível em: <http://link.springer.com/chapter/10.1007%2F978-3-642-34135-9_3>. Acesso em: 8 maio 2013.

ARAÚJO, Nelcileno et al. Avaliação do classificador ARTMAP fuzzy em redes 802.11 com criptografia pré-robust security network (WEP e WPA). In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG 2012), 12., 2012, Curitiba. **Anais...** Porto Alegre: SBC, 2012. p. 310-316. Disponível em: <http://sbseg2012.ppgia.pucpr.br/@docs/SBSeg2012Anais.pdf>. Acesso em: 24 maio 2013.

VILELA, Douglas Willer Ferrari Luz et al. Construção de uma base de dados para auxiliar a avaliação de sistemas de detecção de intrusos em uma rede IEEE 802.11 com criptografia WEP, WPA e WPA2 habilitada. In: ENCONTRO ANUAL DE COMPUTAÇÃO, 10., 2013, Catalão. **Anais...** Porto Alegre: SBC, 2013. p. 145-151. Disponível em: <http://www.enacomp.com.br/anais/pdf/19.pdf>. Acesso em: 7 maio 2013.

ARAÚJO, Nelcileno Virgílio de Souza et al. Kappa-ARTMAP Fuzzy: uma metodologia para detecção de intrusos com seleção de atributos em redes de computadores. In: WORKSHOP DE GERÊNCIA E OPERAÇÃO DE REDES E SERVIÇOS (WGRS), 18., 2013, Brasília. **Anais...** Porto Alegre: SBC, 2013. p. 119-130. Disponível em: <http://sbrc2013.unb.br/files/anais/wgrs/artigos/artigo-9.pdf>. Acesso em: 24 maio 2013.

ANTUNES, Juliana Fonseca; ARAÚJO, Nelcileno Virgílio de Souza; MINUSSI, Carlos Roberto. Multinodal load forecasting using an ART-ARTMAP-Fuzzy neural network and PSO strategy. In: IEEE POWERTECH, 2013, Grenoble. **Proceedings…** Piscataway: IEEE, 2013. (**Aceito**).

ARAÚJO, Nelcileno et al. Kappa-ARTMAP Fuzzy: a feature selection based methodology to intrusion detection in computer networks. In: IEEE INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS (IEEE TRUSTCOM-13), 12., 2013, Melbourne. **Proceedings…** Piscataway: IEEE, 2013. (**Aceito**)