UNIVERSIDADE ESTADUAL PAULISTA "JULIO DE MESQUITA FILHO"
FACULDADE DE ENGENHARIA ELÉTRICA
CÂMPUS DE ILHA SOLTEIRA

DOUGLAS WILLER FERRARI LUZ VILELA

SEGURANÇA EM REDES SEM FIO: ESTUDO SOBRE O DESENVOLVIMENTO DE CONJUNTOS DE DADOS PARA COMPARAÇÃO DE IDS

Ilha Solteira
2014

DOUGLAS WILLER FERRARI LUZ VILELA

SEGURANÇA EM REDES SEM FIO: ESTUDO SOBRE O DESENVOLVIMENTO DE CONJUNTOS DE DADOS PARA COMPARAÇÃO DE IDS

Dissertação apresentada à Faculdade de Engenharia - UNESP - Campus de Ilha Solteira, como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica.

Área de Conhecimento: Automação.

Prof. Dr. AÍLTON AKIRA SHINODA
Orientador
Prof. Dr. ED' WILSON TAVARES FERREIRA
Co-Orientador

Ilha Solteira
2014

FICHA CATALOGRÁFICA
Desenvolvido pelo Serviço Técnico de Biblioteca e Documentação

V699s

Vilela, Douglas Willer Ferrari Luz.
Segurança em redes sem fio: estudo sobre o desenvolvimento de conjuntos de dados para comparação de IDS / Douglas Willer Ferrari Luz Vilela. -- Ilha Solteira: [s.n.], 2014
83 f. : il.

Dissertação (mestrado) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de conhecimento: Automação, 2014

Orientador: Aílton Akira Shinoda
Co-orientador: Ed' Wilson Tavares Ferreira
Inclui bibliografia

1. Conjunto de dados. 2. Sistema de detecção de intrusos. 3. Segurança em redes sem fio.

unesp

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

CERTIFICADO DE APROVAÇÃO

TÍTULO: Segurança em Redes sem Fio: Estudo sobre o Desenvolvimento de Conjuntos de Dados para Comparação de IDS

AUTOR: DOUGLAS WILLER FERRARI LUZ VILELA
ORIENTADOR: Prof. Dr. AILTON AKIRA SHINODA
CO-ORIENTADOR: Prof. Dr. ED' WILSON TAVARES FERREIRA

Aprovado como parte das exigências para obtenção do Título de Mestre em Engenharia Elétrica , Área: AUTOMAÇÃO, pela Comissão Examinadora:

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

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

Valtemir E. Nascimento
Prof. Dr. VALTEMIR EMERENCIO DO NASCIMENTO
Departamento de Área de Informática / Instituto Federal do Mato Grosso

Data da realização: 05 de dezembro de 2014.

Dedico aos meus pais, Walmiro Vilela dos Santos e Loraine Ferrari Luz, pelo amor e ensinamentos que me deram, isto possibilitou tal feito.

RESUMO

O crescimento vertiginoso da tecnologia de redes sem fio tem sido muito significativo nos últimos anos, sua utilização ocorre em diversos setores da sociedade. O padrão IEEE 802.11 destaca-se nesse cenário. No entanto, os mecanismos de proteção empregados por este padrão de rede sem fio não tem apresentado eficiência no combate a ataques de negação de serviço. Os sistemas de detecção de intrusão são vistos como uma forma eficaz de minimizar essas ameaças. Nesta pesquisa foi proposta a construção de três conjuntos de dados que represente de forma significativa o tráfego de rede sem fio. Os conjuntos gerados têm finalidade de auxiliar na avaliação de algoritmos de detecção de intrusos para redes sem fio. Para a construção dos conjuntos de dados foram implementados três cenários de redes sem fio, todos em ambientes reais e operacionais. Em cada cenário foi habilitado um mecanismo de segurança: cenário 1 protocolo WEP, cenário 2 foi utilizado IEEE 802.11i e cenário 3 o IEEE 802.11i associada à emenda IEEE 802.11w. A escolha por cenários diferentes e divisão dos conjuntos de acordo com os ambientes tem a finalidade analisar a evolução dos mecanismos de segurança. Com isto é possível categorizar cada ambiente. Após a construção dos ambientes de rede sem fio foi inoculado tráfego de rede normal e anômalo, com isto iniciou-se a coleta dos dados. Com os dados coletados foi realizado um pré-processamento de cada conjunto capturando apenas os quadros do cabeçalho *Media Access Control* - MAC do IEEE 802.11. A escolha foi definida em virtude de este quadro possuir características especifica das redes sem fio. Para validar os conjuntos de dados foram empregadosalgoritmos de classificação e reconhecimento de padrões. Os algoritmos empregados na validação foram *Multilayer Perceptron* - MLP, *Radial Basis Function* - RBF e *Bayes Net*. Os resultados obtidos com a avaliação dos conjuntos de dados gerados demonstram que a abordagem proposta é bastante promissora.

Palavras-Chave: Conjunto de dados. Sistema de detecção de intrusos. Segurança em redes sem fio.

ABSTRACT

The fast growth of wireless network technology has been very significant lately, its occurs in diverse sectors of society. The standard IEEE 802.11 stands out in this scenario. However, the protection mechanisms employed by this standard wireless network has not shown effectiveness in combating denial of service attacks. The intrusion detection systems are seen as an effective way to minimize these threats. We proposed in this research to build three data sets, which represent traffic wireless network. The sets are generated auxiliary purpose in assessing intrusion detection algorithms for wireless networks. For the construction of the data sets three scenarios of wireless networks, all in real operational environments and have been implemented. In each scenario was one enabled security mechanisms: WEP protocol scenario 1, scenario 2 was used IEEE 802.11i scenario 3 the associated IEEE 802.11i amendment to the IEEE 802.11w. The choice of different sets of scenarios and divide according to the environments aims to analyze the evolution of the security mechanisms. This makes it possible to categorize each environment. After the construction of wireless network environments normal and anomalous traffic were inoculated and thus collect the data. With the collected data pre-processing each set only extracting the frames from the MAC header was conducted. The choice was defined as this has specific characteristics of wireless networks. To validate the data sets and sorting algorithms were employed pattern recognition. The algorithms were used in the validation MLP, RBF and Bayes Net. The results obtained from the evaluation of the generated data sets demonstrate that the proposed approach is quite promising.

Keywords*:* Dataset. Intrusion detection system. Wireless networks security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE SIGLAS

ACK	*Acknowledgment*
AES	*Advanced Encryption Standard*
AP	Ponto de Acesso
AS	*Authenticator Server*
BIP	*Bearer Independent Protocol*
BSS	*Basic service Set*
BSSID	*Basic Service Set Identification*
CAP	*Contention Active Period*
CBC-MAC	*Cipher Block Chaining Authentication Code*
CCA	*Community Choice Awards*
CCA	*Clear Channel Assessment*
CCMP	*Counter-Mode/Cipher Chaining Message Authentication Code*
CFP	*Contention-Free Period*
CP	*Contention Period*
CRC	*Cyclic Redundant Check*
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
CTS	*Clear to Send*
CW	*Content Window*
DA	*Destination Address*
DCF	*Distributed Control Function*
DIFS	*Distributed Inter Frame Space*
DoS	*Denial of Service*
DS	*Distribution System*
DSSS	*Direct Sequence Spread Spectrum*
EAP	*Extensible Authentication Protocol*
EAPoL	*EAP over LAN*
ESS	*Extended Service Set*
FCC	*Federal Communications Commission*
FCS	*Frame Check Sequence*
FHSS	*Frequency Hopping Spread Spectrum*
FTP	*File Transfer Protocol*

HR-DSSS	*High Rate Direct Sequence Spread Spectrum*
ICV	*Integrity Check Value*
IDS	*Intrusion Detection System*
IEEE	*Institute of Electrical and Electronics Engineers*
IFS	*Inter Frame Space*
IGTK	*Integrity Group Temporal Key*
IP	Protocolo *Internet*
ISM	*Industrial, Scientific and Medical*
IV	*Initialization Vector*
KDD99	*Knowledge Discovery and Data Mining*
KSA	*Key-Scheduling Algorithm*
LAN	Rede Local
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*
OFDM	*Orthogonal Frequency Division Multiplexing*
PCF	*Point Coordination Function*
PEAP	*Protected Extensible Authentication Protocol*
PHY	Camada Física
PIFS	*PCF Interframe Space*
PLCP	*Physical Layer Convergence Protocol*
PMK	*Pairwise Master Key*
PS	*Power Save*
PSK	*Pre Shared Key*
PTK	*Pairwise Transit key*
RC4	*Rivest Cipher 4*

RF	*Radio Frequency*
RM	*Robust Management Frame*
RSN	*Robust Security Network*
RSNA	*Robust Security Network Association*
RTS	*Request-to-Send*
SA	Associação Segura
SIFS	*Short Interframe Space*
SSID	*Service Set Identify*
STA	*Wireless Station*
TIE	*Time Element Information*
TKIP	*Temporal Key Integrity Protocol*
TMK	*Temporal MIC Key*
WEP	*Wired Equivalent Privacy*
WLAN	*Wireless Local Area Network*
WPA	*WiFi Protected Access*
WPA2	*WiFi Protected Access Version 2*

SUMÁRIO

1 INTRODUÇÃO

A utilização das redes sem fio tem se tornado cada vez mais comum e com um público diversificado. Esta preferência engloba uma série de fatores, destacam-se entre eles o baixo custo de implementação quando comparado à uma rede cabeada, mobilidade e diversidade de dispositivos existentes. A variedade de dispositivos que possuem conectividade sem fio é enorme, entre eles: *notebooks*, *tablets*, *smartphones*, televisores e outros. Essa diversidade faz com que o uso das redes sem fio, principalmente o padrão IEEE 802.11 (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 1999) sejam mais utilizado atualmente (FENG, 2012). Estão presentes nos mais variados ambientes, tais como, coorporativos, meios acadêmicos, ônibus e até aviões.

No entanto o padrão IEEE 802.11tem apresentando problemas de segurança em relação aos seus mecanismos de segurança. Com o decorrer dos anos houveram atualizações nas emendas de segurança das redes sem fio IEEE 802.11, isto ocorreu da seguinte forma: a primeira emenda foi o *Wired Equivalent Privacy* – WEP (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 1999). O WEP utiliza algoritmo RC4 e chave compartilhada, seu objetivo é proteger os quadros de dados. No entanto, não se mostrou eficaz, apresentando diversas vulnerabilidades (TEWS, 2007). Em 2004 foi apresentada a emenda de segurança IEEE 802.11i ou comercialmente chamado de *WiFi Protected Access Version 2* - WPA2 (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 2004). Suas principais melhorias estão relacionadas à confidencialidade, integridade e autenticidade dos dados transmitidos na rede. Porém não apresenta proteção aos quadros de controle e gerenciamento (LINHARES; GONÇALVES, 2012). O último mecanismo de segurança apresentado é a emenda IEEE 802.11w (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 2009). O protocolo oferece proteção a alguns quadros de gerenciamento (AHAMAD; TADAKAMADLA, 2011). Isto possibilita que os dispositivos troquem quadros de gerenciamento de forma segura. A emenda IEEE 802.11w não contempla proteção aos quadros de controle.

As atualizações apresentadas pelas emendas de segurança corrigiram algumas falhas e apresentaram melhorias para alguns tipos de ameaças, isto reduziu o risco para certos tipos de ataques. Porém um grande explorador das vulnerabilidades das redes sem fio são os ataques de negação de serviço, também denominados *Denial of Service* - *DoS*. Os ataques de negação de serviço tem como objetivo afetar a disponibilidade dos recursos e serviços da rede

(SANDSTROM, 2001), nas redes sem fio exploram a falta de proteção nos quadros de gerenciamento e controle dos protocolos WEP e IEEE 802.11i. No padrão IEEE 802.11w utilizam da falta de proteção dos quadros de controle. Uma alternativa para reduzir os incidentes ocasionados por este tipo de ameaça seria utilizar mecanismo de proteção junto as emendas de segurança.

Um sistema que se apresenta de maneira eficaz no combate aos ataques de *DoS* nas redes sem fio são os sistemas de detecção de intrusos - IDS. Os IDS podem ser baseados em assinatura ou anomalia. O IDS baseado em assinatura analisa o tráfego monitorado a partir de um conjunto de assinaturas de ataques. No método baseado em anomalia, o IDS constrói modelos de comportamento normal e caracteriza como evento intrusivo todo tráfego que difere deste modelo. Para cada modelo existem diferentes técnicas propostas para sua implementação, geralmente essas abordagens possuem especificidades de acordo com o tipo de rede. Isto acontece pelo fato de cada tipo de rede possuir características diferentes de funcionamento. O principal objetivo do IDS consiste em identificar eventos anômalos, isso sem comprometer o funcionamento da rede.

Nesta dissertação foi apresentada a proposta de construção de três conjuntos de dados que representem o tráfego de rede sem fio. Os conjuntos de dados têm como objetivo servir de base de conhecimento para o treinamento e avaliação de IDS sem fio baseados em anomalias. Existem poucos conjuntos de dados específicos para o treinamento de algoritmos de detecção de intrusos sem fio (SHIRAVI et al., 2012). Com isto é possível aumentar o poder de identificação de eventos intrusivos em uma rede sem fio pelo IDS.

Para a construção dos conjuntos de dados foi considerado a evolução dos mecanismos de segurança propostos pelo IEEE, desta forma, foram gerados dados representativos que categorizam cada emenda de segurança. Os conjuntos foram organizados a partir da coleta de dados de redes sem fio implementadas em ambientes reais. Para isto foram habilitadas as seguintes emendas de segurança para cada conjuntos gerado: WEP, IEEE 802.11i e IEEE 802.11i associado ao IEEE 802.11w. Cada conjunto passou por uma etapa de pré-processamento, em que foram utilizados os dados do cabeçalho MAC. Este procedimento foi adotado pelo fato desses dados possuírem características especificas da rede sem fio. Por fim foi realizada a identificação do tipo de tráfego para cada pacote pertencente ao conjunto de dados.

Os conjuntos de dados gerados pelas redes sem fio empregadas nesta pesquisa foram avaliados por técnicas de reconhecimento e classificação de padrões, com objetivo de mostrar

sua capacidade de reconhecimento. As respostas obtidas pelos classificadores empregados na avaliação permitem concluir que a abordagem proposta é promissora. A diversificação dos cenários e tipos de ataques permitiu categorizar vários tipos de tráfego, tanto normal quanto anômalo.

1.1 TRABALHOS RELACIONADOS

A utilização de conjuntos de dados para o treinamento de algoritmos de detecção de intrusos é analisada por vários trabalhos presentes na literatura, alguns são descritos nessa seção.

No trabalho de El-Khatib (2010) foi gerado um conjunto de dados baseado em uma rede sem fio com criptografia WEP/WPA habilitado. Destaca-se que a otimização do conjunto de atributos de uma rede sem fio influencia significativamente na eficiência e precisão de um IDS. O conjunto de dados gerado foi obtido através da coleta de uma rede sem fio real. Porém, não foi gerado nenhum conjunto que contemple as emendas IEEE 802.11i e IEEE 802.11w.

Na abordagem proposta por Shiravi et al. (2012), os autores destacam a ausência de conjuntos de dados públicos para avaliação de sistemas de detecção de intrusos. Embora existam importantes contribuições como o conjunto de dados KDD99 (LIPPMANN, 1989), seus resultados não são muito satisfatórios quando relacionados a redes sem fio, primeiro que os conjuntos de dados foram gerados também com o emprego simulação, outro fator é que essa simulação foi realizada em uma rede cabeada. Com isto, os autores propõem uma sistemática para construir um conjunto de dados com características reais. O método utilizado consiste em gerar perfis com descrições detalhadas dos intrusos, protocolos e dados da camada mais baixa da rede.

O trabalho de Sommer e Paxson (2010) estuda o uso de algoritmos baseados na aprendizagem de máquina. Os autores destacam o esforço da comunidade científica em relação aos IDS. Abordam também a ausência de implementações reais nos ambientes operacionais. Tem como proposta para aumentar o desempenho dos IDS com criação de diretrizes e utilização dos conjuntos de dados para treinamento e avaliação. Por fim, relatam que as dificuldades em encontrar conjuntos de dados públicos disponíveis para auxiliar na realização de pesquisas.

Na abordagem realizada por Nasr, El Kalam e Fraboul (2012) os autores colocam em evidência a importância do IDS como uma segunda linha de defesa na segurança das redes

sem fio. Destacam a utilização de IDS baseados em anomalias como forma de identificar novos ataques através do desvio de comportamento da rede. Os autores desenvolveram um método baseado em especificação, para isto foram gerados conjuntos de dados com características em comum, facilitando a extração de dados representativos. Com este estudo é possível definir uma taxonomia de ataques sem fio de forma global.

O trabalho realizado por Araújo et al. (2013) propõe a utilização o classificador ARTMAP *Fuzzy* na detecção de intrusos. Com método empregado foi desenvolvido um IDS com um baixo custo computacional, sem comprometer a identificação correta das amostras. A área de atuação do IDS empregado pelos autores envolve redes cabeadas e sem fio. Utilizou-se o conjunto de dados KDD99, além de um conjunto com criptografia WEP/WPA e IEEE 802.11i. Os autores relatam que o método aplicado apresentou resultados animadores.

1.2 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado em quatro capítulos, distribuídos da seguinte forma:

- capítulo 1 – Introdução e trabalhos relacionados;
- capítulo 2 – é apresentada a fundamentação teórica das redes sem fio IEEE 802.11 e suas operações;
- capítulo 3 – é apresentada uma contextualização sobre segurança em redes sem fio IEEE 802.11, os mecanismos de segurança presentes nas redes WLAN e suas principais ameaças e tipos de ataques;
- capítulo 4 – é descrito neste capítulo os conceitos básicos relacionados aos sistemas de detecção de intrusos;
- capítulo 5 – é abordado neste capítulo a proposta de implementação dos cenários de rede sem fio IEEE 802.11, a metodologia desenvolvida para coleta e processamento dos dados e a avaliação dos conjuntos de dados gerados;
- capítulo 6 –considerações finais e perspectivas de trabalhos futuros;
- capítulo 7 – referências bibliográficas; e
- capítulo 8 – apêndices com os trabalhos publicados.

2 PADRÃO IEEE 802.11

A transmissão sem fio em redes de computadores começou a ser difundida através da iniciativa das empresas e instituições de pesquisas. Com isto, o IEEE buscando viabilizar a tecnologia criou um grupo de pesquisa denominado IEEE 802.11 para que fossem criados padrões abertos da mesma, mas pela taxa de transferência de dados proposta, o padrão não foi validado. Apenas em 1997, o IEEE publicou o padrão para as *Wireless Local Area Networks*- WLANs. A WLAN é um sistema que realiza a interconexão de diversos dispositivos, tanto móveis quanto fixos utilizando rádio frequência - RF como meio de transmissão.

*2.*1 ARQUITETURA DO PADRÃO IEEE 802.11

A arquitetura do padrão IEEE 802.11 é composta por múltiplos componentes, estes realizam interação para prover a mobilidade nas estações de modo que seja transparente para as camadas superiores. Os principais componentes desta tecnologia são:

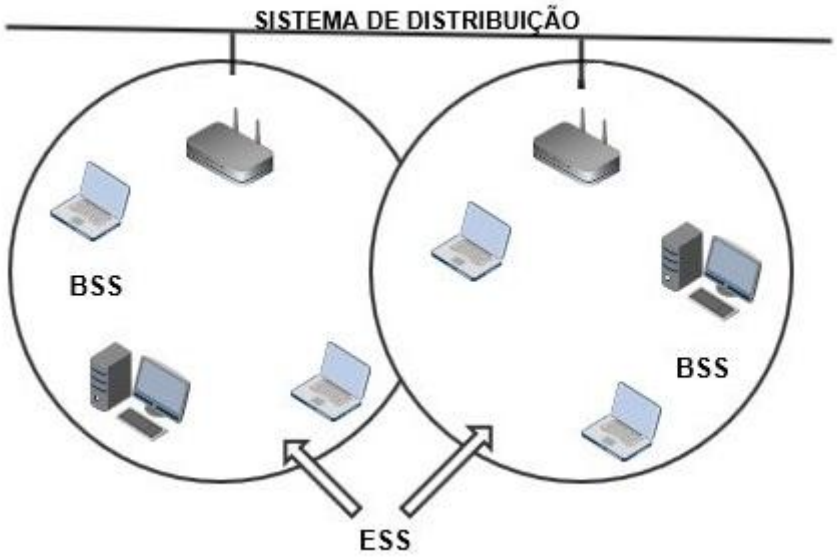
- unidade básica (*Basic Service Set* - BSS) – É o bloco principal da construção da arquitetura IEEE 802.11, definido como um grupo de estações, que ficam sob o domínio direto de uma mesma função de coordenação. Esta determina o envio e recebimento de dados através do meio de transmissão sem fio utilizado pelas estações;
- sistema de distribuição (*Distribution System* – DS) - Componente lógico destinado a enviar quadros entre estações pertencentes a diferentes BSSs e uma rede local cabeada (LAN);
- estação sem fio (*Wireless Station* - STA) – Qualquer dispositivo que acesse o meio sem fio; e
- ponto de acesso (*Access Point* - AP) - É uma estação STA que fornece conectividade entre vários STAs e entre STAs e DS.

As redes sem fio seguem uma arquitetura modular, em que o sistema é particionado em células. Cada uma destas células é chamada de BSS, que são compostas por uma ou mais estações e pelo AP. O AP realiza todo o controle das estações conectadas nesta célula.

As redes sem fio podem se constituir através de uma única célula, com apenas um AP, entretanto para a construção de redes com área de cobertura maior que uma célula, é utilizado um DS, em que os APs são conectados através de um *backbone ethernet* ou *wireless*. Sendo assim o DS representa a infraestrutura de comunicação que interconectam as células constituintes da rede.

A união de um conjunto de STAs e APs oriundos de BSS diferentes interligados a um DS é denominado como um conjunto estendido de serviços. O *Extended Service Set* - ESS é visto pela camada de protocolo superior *Internet Protocol* - IP como apenas uma rede IEEE 802.11. Na Figura 1 é apresentado os diversos componentes que compõem a arquitetura IEEE 802.11.

Figura 1 - Exemplo de uma WLAN.



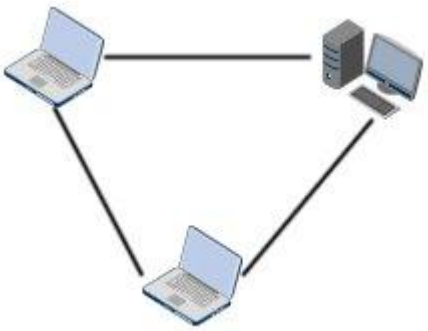
FONTE: Tanembaum (2011).

2.2 TOPOLOGIAS DO PADRÃO IEEE 802.11

De acordo com as especificações definidas pelo padrão IEEE 802.11, as WLANs podem ser organizadas em duas topologias básicas: infraestruturada e *ad-hoc* (GAST, 2005).

As redes *ad-hoc* são compostas apenas por estações móveis, estas realizam comunicação entre si sem a necessidade de uma estação base. Essa comunicação ocorre através de uma conexão ponto a ponto, dispensando o uso de qualquer estrutura de comunicação de apoio. Isto faz com que a utilização do AP seja dispensável, pois as estações de um BSS são aptas a iniciar uma comunicação direta sem que as informações passem por um ponto de acesso centralizado. A Figura 2 apresenta um exemplo de uma rede *Ad-Hoc*.

Figura 2 - Componentes de uma rede IEEE 802.11 ad-hoc.



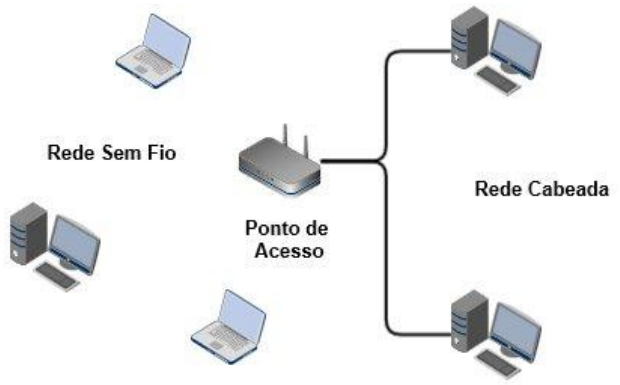
Fonte: Tanembaum (2011).

As redes com infraestrutura são compostas por estações e pontos de acesso. Diferente de uma rede *ad-hoc*, uma estação em uma BSS não está apta a estabelecer uma comunicação com outras estações sem que as informações trafegadas passem por um ponto de acesso centralizador. A comunicação dentro da BSS é realizada de forma que, obrigatoriamente quando uma STA deseja estabelecer uma comunicação com outra deve primeiramente transmitir os dados para o AP, para posteriormente serem encaminhados à estação de destino. Um AP desempenha as seguintes funções dentro de uma BSS:

- autenticação, associação e reassociação - em que pelo meio da função *handoff*, um nó móvel se desloca da sua BSS de origem e continua conectado à infraestrutura sem cessar a conexão;
- gerenciamento de potência - o AP faz a buferização do tráfego para uma STA enquanto estiver trabalhando com capacidade reduzida de energia, utilizando o modo de economia de energia; e
- sincronização - todas STAs associadas a um ponto de acesso são sincronizadas por um relógio comum.

Com a finalidade de aumentar a área de cobertura destas redes diversos APs podem se interligar por meio de um *backbone,* com isto forma-se uma ESS. A infraestrutura destas redes é mostrada pela presença do AP e pelo DS que os interliga. A Figura 3 apresenta um exemplo de rede infraestruturada.

Figura 3 – Componentes de uma rede IEEE 802.11 infraestruturada.

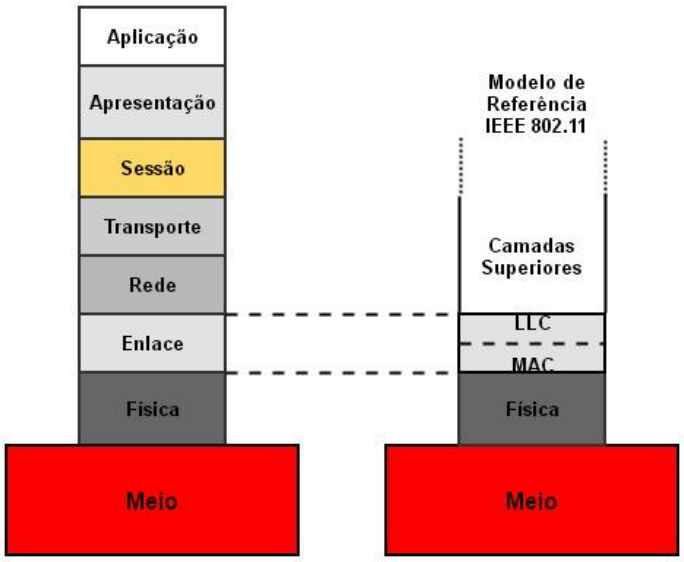


Fonte: Elaborado pelo autor.

2.3 CAMADA FÍSICA DO PADRÃO IEEE 802.11

A camada física do padrão IEEE 802.11 é semelhante à camada física do modelo *Open Systems Interconnection* - OSI, conforme apresentado na Figura 4. Essa camada física do padrão IEEE 802.11 é responsável pela transmissão pelo canal de comunicação (TANEMBAUM, 2011).

Figura 4 – Modelo OSI e modelo IEEE 802.11.



Fonte: Tanembaum (2011).

A transmissão dos dados da camada física do padrão IEEE 802.11 é definida através de três técnicas de transmissão: duas utilizam métodos de rádio frequência, sendo, espalhamento espectral por salto em frequências (*Frequency Hopping Spread Spectrum* – FHSS) e espalhamento espectral por sequência direta (*Direct Sequence Spread Spectrum* – DSSS) e

outra infravermelho. A escolha de uma dessas técnicas depende de fatores relacionados com as aplicações dos usuários e os ambientes em que a rede irá atuar. Em 1999, foram introduzidas duas técnicas novas de RF, estas possibilitavam um alcance maior de largura de banda. O *Orthogonal Frequency Division Multiplexing* - OFDM e o *High Rate Direct Sequence Spread Spectrum* - HR-DSSS (TANEMBAUM, 2011).

A escolha do método de transmissão depende de diversos fatores relacionados com a aplicação do usuário e ambiente de operação de rede, com isto os dados podem ser codificados e modulados para equilibrar velocidade, distância e capacidade de transmissão.

Na transmissão de RF são utilizadas técnicas que transmitem os quadros de dados por vários canais disponíveis dentro de uma determinada frequência, com isto a transmissão não se restringe a apenas um canal. Isto permite a transmissão simultânea de diversos quadros.

O padrão IEEE 802.11 define que as tecnologias de transmissão por espalhamento espectral devem atuar na faixa de 2,400 a 2,4835 GHz da banda *Industrial, Scientific and Medical* - ISM. A regulamentação da banda ISM é definida pelo *Federal Communication Commission* - FCC.

2.4 SUBCAMADA DE CONTROLE DE ACESSO AO MEIO DO PADRÃO IEEE 802.11

A especificação da MAC IEEE 802.11 é diferente do padrão IEEE 802.3, isso ocorre em virtude da complexidade da comunicação sem fio. Na comunicação sem fio os rádios têm uma deficiência em transmitir e receber pacotes de forma simultânea em uma única frequência. Isto ocorre em virtude do sinal recebido ser menor que o sinal transmitido, fazendo com que não sejam detectados ao mesmo tempo. Diferente do ambiente e*thernet*, pois neste é necessário apenas que o meio esteja inativo para que haja transmissão. O padrão IEEE 802.11 usa o protocolo denominado *Carrier Sense Multiple Access with Collision Avoidance* - CSMA/CA, para evitar colisões. O funcionamento deste protocolo ocorre da seguinte forma: as estações realizam uma consulta no canal de comunicação antes de transmitir, caso o canal esteja ocupado a transmissão não é realizada. Se o canal estiver livre é feita a transmissão.

O controle de acesso ao meio do padrão IEEE 802.11 é realizado através de funções de coordenação, são estas que determinam qual e quando uma STA vinculada à BSS apresenta permissão de enviar e receber dados através do meio sem fio. Dois mecanismos de controle são especificados pelo padrão IEEE 802.11: *Distributed Coordination Function* - DCF e *Point Coordination Function* - PCF.

O DCF é um método de acesso distribuído, em que a estação tem o poder de decidir ou não pela transmissão, sendo assim existe a possibilidade de que haja colisões.

O PCF é um método de acesso em que o controle é centralizado, e que apenas uma estação tem o poder de permitir ou não uma transmissão, desta forma ela determina quem pode transmitir e em qual momento, reduzindo a possibilidade de colisões.

Em ambos os métodos de acesso são definidos parâmetros que determinam o tempo de espera antes de liberar o acesso ao canal de comunicação para uma estação, sendo que o meio pode estar ocupado com transmissão de quadro de dados, quadros de controle ou ainda estar disponível, isto possibilita que qualquer estação possa utilizar o canal de comunicação.

Para haver uma transmissão o meio deve estar livre por um período de silêncio mínimo *Inter Frame Space* - IFS, sendo assim a estação deve monitorar o meio antes de utilizá-lo. Existem três prioridades de acesso ao meio, através de diferentes intervalos de tempo:

- *distributed inter frame space* - DIFS - indica o maior tempo de espera para transmitir o quadro, é definido pelo espaço distribuído entre quadros DCF;
- *short inter frame space* - SIFS - são utilizados para transmissões de quadros com resposta imediata, como *Acknowledgment* - ACK ou *Clear to Send* - CTS, possuem a mais alta prioridade; e
- *priority inter frame space* - PIFS – é o espaço de tempo entre o DIFS e o SIFS, é utilizado por uma estação que possui controle sobre outras estações, desta forma possui uma prioridade maior que as estações comuns, é definido pelo PCF.

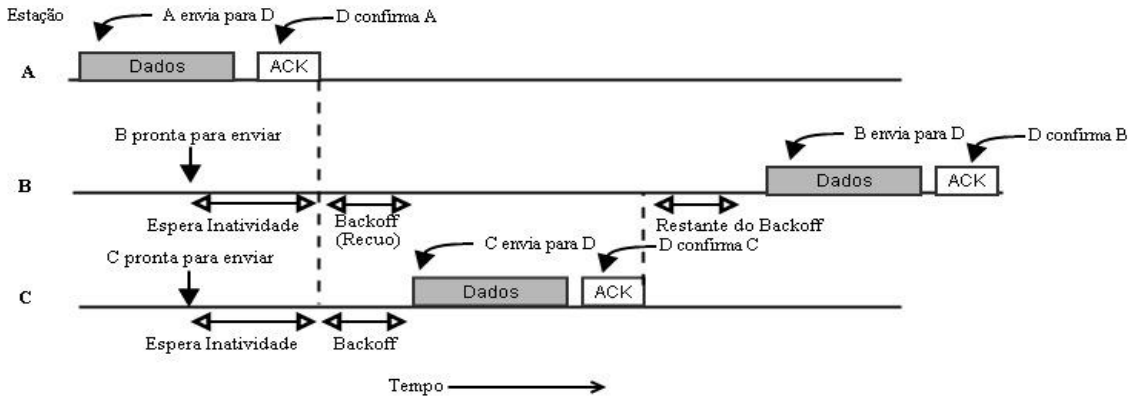
O método de acesso DCF opera tanto em modo *ad-hoc* como em modo infraestruturado, entretanto o PCF é opcional e opera somente em redes infraestruturadas.

O DCF é o mecanismo básico de gerência de acesso ao meio da camada MAC do IEEE 802.11 através do método CSMA/CA. A transmissão de quadros no DCF funciona da seguinte forma: quando uma estação deseja realizar a transmissão de uma mensagem, ela verifica o canal de comunicação por um período denominado DIFS, ao término do DIFS, se o canal estiver disponível é realizada a transmissão. O receptor ao receber a mensagem aguarda por um período denominado SIFS, e em seguida encaminha uma mensagem de reconhecimento positivo (ACK). Caso o meio de comunicação esteja ocupado após o período DIFS, as outras estações iniciam a fase de contenção. Quando as estações entram em fase de contenção, cada uma delas determina um tempo aleatório. Ao final deste tempo é realizada

uma nova tentativa de acesso ao meio. Portanto, se o meio de comunicação ainda estiver ocupado durante este intervalo, é estabelecido que a estação perdeu o primeiro ciclo, e inicia-se a espera da duração de um tempo DIFS.

Quando uma estação não consegue realizar a transmissão no primeiro ciclo, é realizada a espera e seu contador entra em decréscimo. Em consequência disto, possivelmente a estação mais antiga terá seu contador com um tempo menor. Desta forma a estação acessa o meio quando seu contador expirar. A Figura 5 demonstra o método de transmissão de um quadro CSMA/CA utilizando a função DCF (TANEMBAUM, 2011).

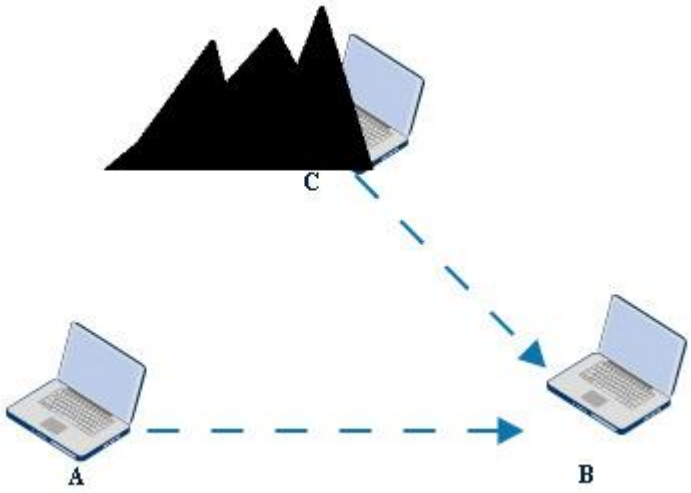
Figura 5 – Transmissão quadro CSMA/CA.



Fonte: Tanenbaum (2011).

O DCF concede um esquema opcional além do básico, este é fundamentado em pacotes de solicitação *Request to Send* - RTS e permissão de transmissão CTS evitando problema causado por terminais ocultos. O problema relacionado aos terminais ocultos acontece quando as estações não estão todas dentro da mesma área de cobertura de rádio. Isto ocorre da seguinte forma: A estação A transmite para estação B; a estação C ao checar o canal de comunicação não identifica nenhuma transmissão, consequentemente assimila que o canal está disponível e realiza uma transmissão para estação B, ocasionando-se assim uma colisão.

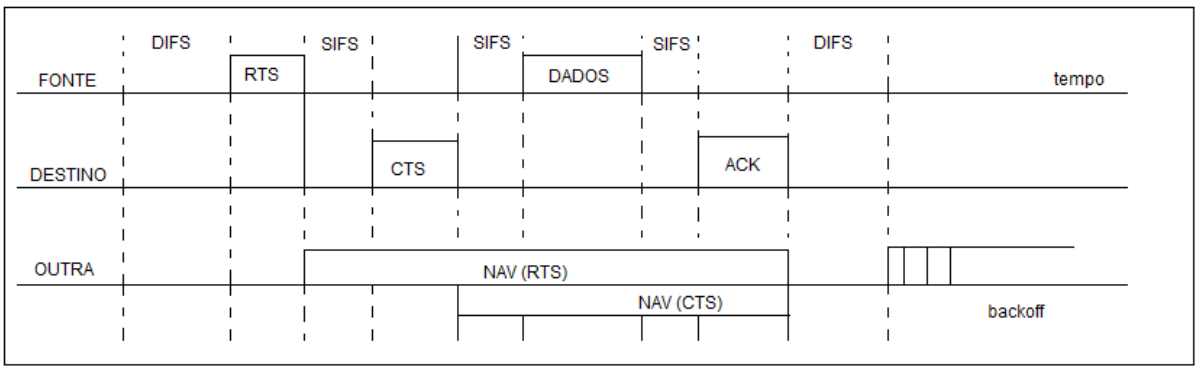
Figura 6 – Terminal oculto.



Fonte: Elaborado pelo autor.

O outro método de transmissão concedido pelo DCF reduz os problemas ocasionados pelo terminal oculto. Este método funciona da seguinte forma no mecanismo de detecção virtual: as STAs trocam quadros de controle RTS e CTS antes de transmitir os dados, com o objetivo de reservar o meio de transmissão para a troca dos quadros de dados entre as STAs (RUBINSTEIN; REZENDE, 2002). Os pacotes RST e CTS têm um campo denominado *Duration*/ID que determina o tempo de acesso ao meio de que as estações necessitam para transmitir o pacote de dados, incluindo também o ACK. Na Figura 7 é apresentado o método DCF com as extensões RTS e CTS.

Figura 7– Acesso DCF com extensão RTS e CTS.



Fonte: Rubinstein (2002).

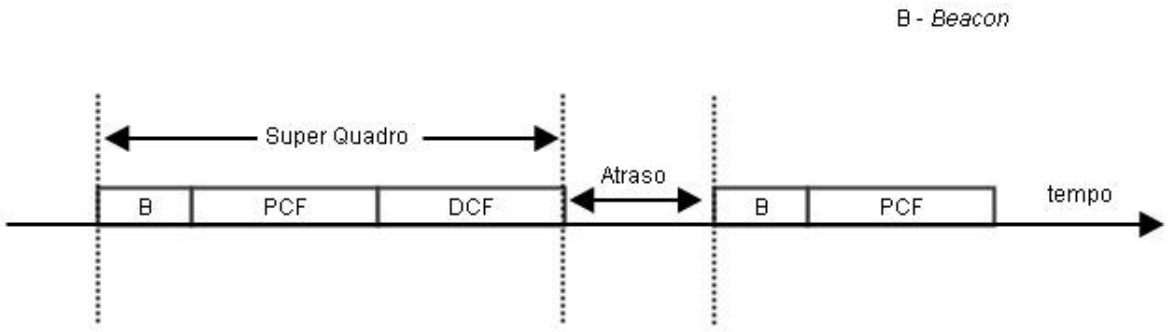
A estação observa o meio por um tempo maior ou igual ao DIFS antes de executar a transmissão. Caso o canal esteja livre por pelo menos DIFS segundos, é transmitido pela STA um quadro de solicitação RTS, para reservar o canal. Se o receptor estiver apto a receber,

responde com um CTS. Ao finalizar a transmissão do quadro de dados a STA aguarda o recebimento do ACK.

Os quadros RTS e CTS possuem um campo indicando o tempo de envio dos quadros. Os RTS e CTS são recebidos por todas STAs da área de cobertura do transmissor e do receptor ao término da troca de RTS/CTS. Estas estações, que estão dentro da área de cobertura dos participantes da negociação armazenam informações relacionadas ao tempo de transmissão do pacote de dados e atualizam os vetores de alocação da rede *Net Allocation Vectors* - NAV, utilizado para detecção virtual da portadora. Aponta-se então o tempo que um nó poderá transmitir dados, mesmo o *Community Choice Awards* - CCA apresentando meio de transmissão livre. Desta forma evitam-se colisões, pois o terminal oculto poderá adiar a sua transmissão.

O PCF é utilizado apenas em redes sem fio infraestruturadas, sendo assim, apenas um único ponto controla o acesso ao meio (RUBINSTEIN, 2002). O ponto controlador - PC está presente no AP, gerenciando os serviços de contenção, pois este é quem autoriza as estações a transmitirem. A autorização para transmissão de pacotes no meio ocorre por uma ordem de prioridades, que é definida da seguinte forma: o PC inicia um período livre de contenção e executa um *pooling* entre as estações, com isto consegue definir quais desejam transmitir; realiza um registro na lista de *pooling*, diferencia certas estações e define as estações aptas para tráfego. O PCF aplica-se sobre a base do DCF, conforme é apresentado na Figura 8.

Figura 8 – Métodos de acesso PCF e DCF.



Fonte: Rubinstein (2002).

O tempo de acesso é dividido pelo PC em períodos de superquadros, no qual cada um destes tem um período livre de contenção *Contention Free Period* - CFP concedido pelo PCF e um período de contenção *Contention Period* - CP concedido pelo DCF. O PC escuta o canal por um determinado tempo de PIFS segundos e estabelece um período de livre contenção. O

PIFS é inferior ao DIFS, desta forma as STAs não tem permissão para iniciar o processo de transmissão de dados no modo DCF antes do PC. Na abertura de cada período livre de contenção, depois de analisar o meio por PIFS, o PC comunica o tempo de duração máximo do período livre de contenção (CFP *maxduration*) através da propagação de um sinal de *beacon.* Na tentativa de evitar que alguma estação tome o controle do canal neste período, todas as estações estabelecem em seus NAVs a duração máxima de CFP.

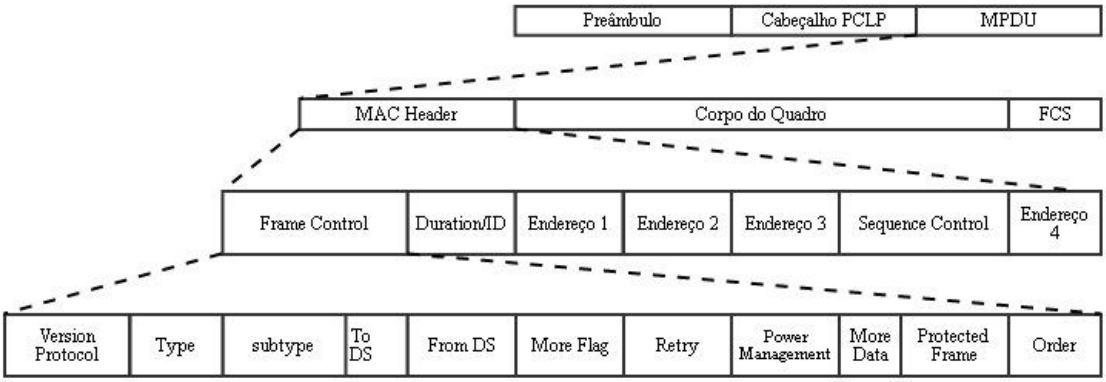
Depois de respeitar um tempo SIFS, o PC estará apto a enviar dados, solicitar que as STAs encaminhem dados, certificar o recebimento de dados e dependendo da disponibilidade do tráfego e tamanho do *pooling* a qualquer instante finalizar com o CFP, encaminhando um quadro de CF*end* mesmo que o tempo de duração do quadro *beacon* não tenha terminado. Qualquer STA pode receber dados, entretanto as STAs que podem receber são apenas as que estão na lista de *pooling*. Depois de todas as transmissões contidas na lista serem concluídas, o PC realiza uma nova consulta, após PFIS segundos.

2.5 QUADRO MAC DO IEEE 802.11

A composição do quadro IEEE 802.11 é descrita da seguinte maneira: preâmbulo, cabeçalho *Physical Layer Convergence Protocol* - PLCP e MAC *Protocol Data Unit* – MPDU, que são campos pertencentes ao nível mais elevado, conforme é apresentado na Figura 9. O campo MPDU da subcamada MAC contém os dados transmitidos, ele é composto dos seguintes componentes básicos (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 1999):

- MAC *Header* (cabeçalho) – contém informações de controle do campo, duração, endereços e informações de controle de sequência;
- corpo do quadro *(Frame Body* – FB) - contém os dados que serão transmitidos; e
- *frame check sequence* - FCS – possui o valor do *Cyclic Redudant Check* - CRC, utilizado para detecção de erro.

Figura 9 – Organização do formato do quadro IEEE 802.11.



Fonte: Institute of Eletronic and Eletrical Engineers (1999).

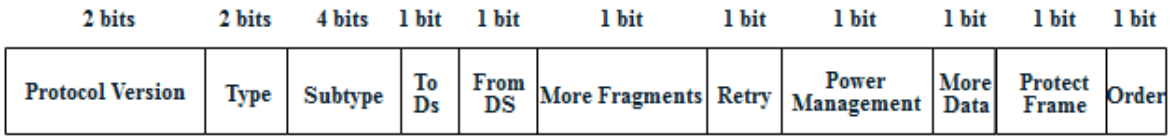
A composição de cada campo é detalhada a seguir, devido à base do trabalho estar relacionada ao MAC *Header.*

- *frame control* - FC – compõe informações de controle encaminhadas pela STA transmissora para STA receptora. Este campo é subdividido em outros, em que cada um possui funções diferentes: versão, tipo de protocolo, informações de fragmentação, gerência de energia e encriptação WEP;
- *duration* ID – possui definições diferentes, dependendo da circunstância, que pode ser:
  - para pacotes de controle do subtipo *Power Save* - PS, possui informações de identificação de conexão; e
  - para pacotes do campo *Duration*/ID determina o tempo de duração da transmissão. Este campo é utilizado para atualizar o NAV das estações sem fio.
- endereços 1,2,3,4 – estes campos possuem diferentes tipo de endereços, de acordo com o tipo de pacote encaminhado. Os endereços podem ser; e
  - *destination address* - DA – endereço do destino final do pacote;
  - *source address* - SA – endereço de destino;
  - *receiver address* - RA – endereço que define o destino instantâneo do pacote;
  - *transmitter address* - TA – endereço que define a STA que realizou a transmissão do *frame*; e
  - *basic service set identification* - BSSID - identifica a BSS em que as estações se encontram. Outra função é limitar o alcance de *broadcast*.

- *sequence control* - SC – este campo zela pelo controle da sequência dos pacotes fragmentados. Ele identifica em quantos pacotes a mensagem será dividida e informa qual parte do pacote será transmitida neste instante.

O campo FC está contido em todos os pacotes transmitidos, sua estrutura é composta por onze subcampos conforme é apresentado na Figura 10.

Figura 10 - Formato do campo FC.



Fonte: Institute of Eletronic and Eletrical Engineers (1999).

- *protocol version* – aponta a versão do protocolo;
- *type* – aponta o tipo do quadro transmitido. Estes são definidos conforme mostra o Quadro 1;

Quadro 1 - Tipos de quadros.

00	Gerenciamento
01	Controle
10	Dados
11	Reservado

Fonte: Elaborado pelo autor.

- *subtype* – aponta o subtipo do quadro e de acordo com o campo *Type*, define a função do quadro. Essa combinação entre tipo e subtipo pode resultar em *frames* de: associação, reassociação, autenticação, RTS, CTS, entre outros;
- *to* DS e *From* DS – indicam se o quadro está indo ou vindo da rede conectada aos APs, chamado sistema de distribuição;
- *more fragments* – indica se existem mais fragmentos pertencentes ao mesmo quadro*;*
- *retry* – indica se a informação está ou não sendo retransmitida;
- *power management* – indica que o receptor irá entrar em modo de economia de energia;

- *more data* – aponta que a STA transmissora dispõe de quadros extras para a STA receptora;
- *protected frame* – aponta se o quadro possui ou não processo de criptografia e autenticação. Esta configuração pode ser realizada para todos os quadros de dados e gerenciamento que tem o subtipo configurado para autenticação; e
- *order* – aponta se os quadros estão sendo transmitidos através da classe de serviço denominada *strict order*, usada principalmente quando existe a fragmentação.

Os padrões de quadros em uma rede IEEE 802.11 são definidos em três classes: gerenciamento, controle e dados.

Os quadros de gerenciamento são responsáveis pela associação, desassociação, e autenticação das STAs perante o ponto de acesso. Os quadros de gerenciamento possuem informações referentes às configurações padrão da camada de enlace, como taxas suportadas, operações de segurança e definição de *status* de conexão. Todas as estações pertencentes à rede sem fio irão receber *beacons,* quadros com a identificação da rede acessível no ambiente. Estes quadros identificam o canal usado pela rede sem fio para a transmissão e o SSID da rede. Em seguida a STA cliente envia um quadro de associação pedindo permissão para o AP. Após a concessão pelo AP a STA envia uma solicitação de autenticação na rede.

Os quadros de gerenciamento podem ser subdivididos conforme demonstra o Quadro 2:

Quadro 2 - Divisão dos quadros de gerenciamento.

Tipo	**Subtipo**	**Função do quadro**
Gerenciamento	*Association Request*	é encaminhado da STA para o AP requisitando associação ao AP e abriga as informações de capacidade da STA.
Gerenciamento	*Association Response*	é encaminhado do AP para STA em resposta ao quadro de *Association Request*, informando o aceite ou não da solicitação encaminhada pela STA.
Gerenciamento	*Reassociation Request*	é encaminhado pelo AP via STA, quando uma STA se desloca de uma BSS para outra BSS. Desta forma o AP tem que negociar com o AP antigo para encaminhar os quadros armazenados. Estes quadros podem ser usados para atualizar os atributos de associação à STA que estiver associada ao AP.
Gerenciamento	*Reassociation Response*	é a resposta do AP a requisição feita pela STA via *Reassociation Request*.
Gerenciamento	*Probe Request*	é encaminhado pela STA a fim de adquirir informações sobre o AP do qual a STA tenha interesse em se associar.
Gerenciamento	*Probe Response*	contêm as informações solicitadas pela STA ao AP através do quadro *Probe Resquest*.
Gerenciamento	*Beacon*	é transmitido regularmente pelo AP, sua função é informar sua presença e informações para as STAs.
Gerenciamento	*Deassociation*	é utilizado para finalizar uma associação entre STA e o AP.
Gerenciamento	*Authentication*	são trocados entre STA e AP para autenticação entre os mesmo durante associação.
Gerenciamento	*Deauthentication*	é utilizado para encerrar a autenticação entre AP e STA.

Fonte: Elaborado pelo autor.

Os quadros de controle ajudam na entregados quadros de dados aumentando a confiabilidade nas transmissões. Estes são subdivididos conforme apresenta o Quadro 3.

Quadro 3 - Divisão dos quadros de controle.

Tipo	**Subtipo**	**Função do Quadro**
Controle	*Power Save-Poll*	realiza uma requisição ao AP, para que este encaminhe os quadros guardados para uma STA que neste instante acabou de despertar do modo *Power-Save.*
Controle	RTS	é utilizado no mecanismo *handshake* RTS/CTS para que a STA realize um alerta aos destinatários e outras STAs no perímetro em que deseja transmitir um quadro para o destinatário.
Controle	CTS	é o segundo quadro do mecanismo *handshake* RTS-CTS. É encaminhado pela STA de destino para STA remetente, atua com aprovação do RTS e permite que a STA remetente encaminhe os quadros de dados.
Controle	ACK	é encaminhado pelo destinatário para o remetente, sua função principal é informar ao remetente que a transmissão do quadro foi realizada com êxito.

Fonte: Elaborado pelo autor.

Os quadros de dados são responsáveis pela transmissão. Estes são subdivididos conforme apresenta Quadro 4.

Quadro 4 - Divisão dos quadros de dados.

Tipo	**Subtipo**	**Função do quadro**
Dados	*Data*	realiza o encapsulamento dos dados recebidos das camadas superiores das redes sem fio.
Dados	*Null function*	é responsável pela gerência de energia.

Fonte: Elaborado pelo autor.

2.6 FUNCIONAMENTO DA REDE

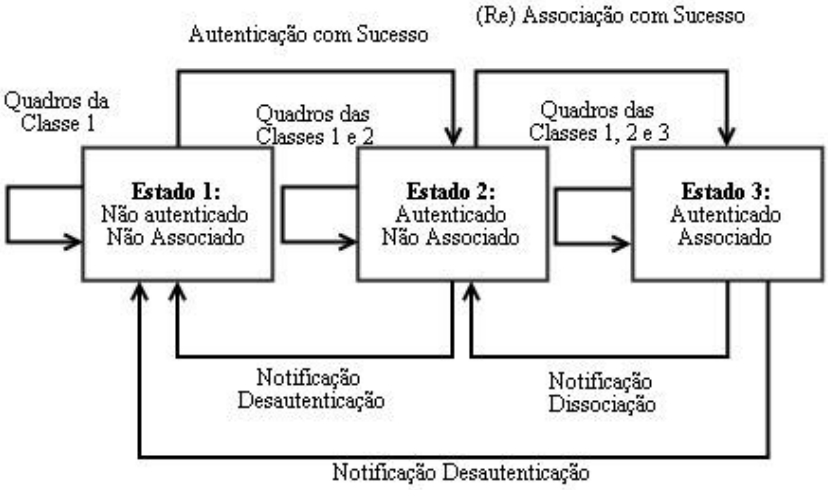
O padrão IEEE 802.11 estabelece que todas as estações devem manter duas variáveis de estado, estas são dependentes dos serviços de autenticação, desautenticação, associação, reassociação e desassociação. Estas variáveis de estados são referenciadas como: o estado da autenticação e o estado da associação das estações. Estas variáveis possuem três estados praticáveis para cada uma das estações. Estes estados são (PEREIRA, 2005):

- estado 1 – estado inicial, estação desautenticada e desassociada;

- estado 2 – estado intermediário, estação autenticada e desassociada; e
- estado 3 – estação final, estação autenticada e associada.

O diagrama de estados é representado na Figura 11.

Figura 11 - Diagrama de estados IEEE 802.11.



Fonte: Pereira (2005).

O estado atual entre estação de origem e estação destino define qual tipo de quadro que deve ser trocados entre as estações. Os quadros autorizados são reunidos em classes, as que condizem ao estado:

- classe 1 – os quadros condizentes a classe 1 são autorizados nos estados 1, 2 e 3, cujo serviço de autenticação é implementado;
- classe 2 – os quadros desta classe são autorizados apenas nos estados 2 e 3, cujos serviços de associação, desassociação e reassociação são implementados; e
- classe 3 - os quadros da classe 3 são utilizados apenas no estado 3, ou seja, são permitidos todos os tipos de quadros, inclusive os que autorizam a utilização do serviço de dados.

Foi apresentado neste capítulo fundamentação teórica das redes sem fio IEEE 802.11 e suas operações. No próximo capítulo é apresentada uma contextualização sobre segurança em redes sem fio IEEE 802.11, os mecanismos de segurança presentes nas redes WLAN e suas principais ameaças e tipos de ataques.

3 SEGURANÇA EM REDES PADRÃO IEEE 802.11

Os mecanismos de segurança definidos para redes sem fio são diferentes dos implementados em uma rede cabeada. Porém existem paridades entre os princípios básicos de segurança entre ambas as redes. A segurança das redes sem fio possui quatro princípios de segurança fundamentais: a confidencialidade, integridade, disponibilidade e controle de acesso. Estes são descritos a conforme Singh, Singh e Singh (2011):

- confidencialidade – consiste em assegurar que nenhuma entidade não autorizada faça a leitura das informações trocadas entre duas estações;
- integridade – garantir que os dados trafegados não tenham seu conteúdo alterado durante seu transporte ou existência;
- disponibilidade – consiste em assegurar que determinado recurso, serviço ou informação, não seja negado a utilizadores legítimos; e
- controle de acesso – consiste em garantir a legitimidade a certos recursos, e que estes não sejam acessados por entidades não autorizadas.

Questões relacionadas à segurança das redes sem fio dependem de aspectos especiais, quando comparadas as redes cabeadas. Estas utilizam meio de interconexão entre estações através do cabo e possuem características de segurança física inexistentes em redes sem fio. Como a comunicação é realizada por ondas de rádio, qualquer dispositivo que esteja dentro da área de cobertura, poderá receber informações desta rede.

3.1 MECANISMOS DE SEGURANÇA NORMA IEEE 802.11

O IEEE definiu normas para o padrão IEEE 802.11 que consistem em uma série de especificações de segurança, de forma que as transmissões realizadas no canal de comunicação sejam seguras. Também são descritas nas subseções seguintes as vulnerabilidades apresentadas pelos mecanismos de segurança propostos.

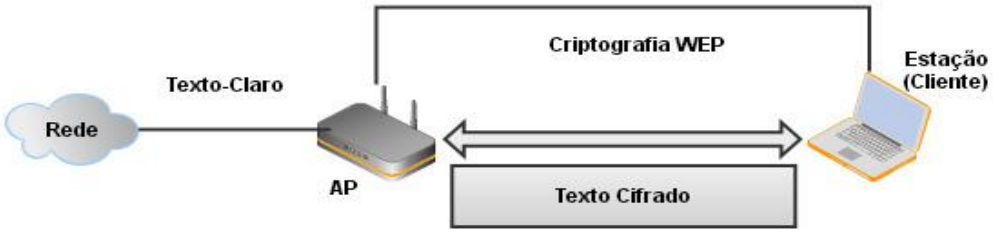
3.2 EMENDA DE SEGURANÇA WIRED EQUIVALENT PROTOCOL - WEP

Para proteger a camada de enlace de dados durante a transmissão nas WLANs, o IEEE lançou em 1999 seu primeiro protocolo de segurança, denominado WEP. Este protocolo tem objetivo prover segurança equivalente ao ambiente de redes cabeadas.

O WEP possui dois meios de autenticação para os dispositivos: *Cyclic Redundancy Check* 32 - CRC-32 que é uma função detectora de erros, realiza um cálculo de *checksum* gerando

Integrity Check Value - ICV atribuído à mensagem, para garantir a sua integridade. Este pode detectar com alta probabilidade mudanças não solicitadas nas mensagens, possibilitando a análise de integridade. O WEP também utiliza o algoritmo de criptografia *Ron's Code*#4 - RC4, desenvolvido por Ron Rivest em 1987, mas que é considerado por muitos especialistas como sua principal vulnerabilidade (LINHARES; GONÇALVES, 2012). O RC4 criptografa os dados, juntamente com um vetor de inicialização - IV de 24 bits com uma chave secreta compartilhada de 40 ou 104 bits, os quais geram as informações criptografadas. O IV ao ser encadeada a mensagem cifrada, forma uma chave de 64 ou 128 bits. O WEP é usado entre o AP e a estação cliente, ou na comunicação direta entre cliente quando utilizado em modo *ad-hoc*. A criptografia do WEP é aplicada apenas no tráfego do canal de comunicação, deixando sem criptografia todo tráfego roteado por fora da rede sem fio, conforme a Figura 12.

Figura 12 – O protocolo de segurança WEP.



Fonte: Linhares e Gonçalves (2008).

3.2.1 Autenticação do Protocolo WEP

São definidas pelo IEEE 802.11 duas maneiras de legitimar as estações que desejam se autenticar a um AP. Estas são conhecidas como autenticação por chave compartilhada (s*hared-key authentication)* e autenticação aberta (*open system authentication)*. A diferenciação entre esses métodos de autenticação acontece pela utilização ou não da chave criptográfica. Além desses dois métodos definidos pelo IEEE 802.11, existem outras duas maneiras que são utilizadas por fabricantes de dispositivos sem fio. Estes mecanismos são autenticação por MAC e autenticação por *Service Set Identifier* - SSID.

Os mecanismos de autenticação definidos pela norma se referem à autenticação de STAs ou dispositivos sem fio e não autenticação de usuários. As estações enviam quadros do tipo *probe request* na tentativa de encontrar um AP, os APs que estão dentro desta área do sinal de rádio irão responder com um quadro do tipo *probe response*. A partir desse momento inicia-se o processo de autenticação, em que a estação escolhe a qual AP deseja se autenticar. Após

receber uma indicação positiva a estação envia um quadro do tipo *association request* dando inicio ao processo de associação. Em seguida o AP retorna um quadro do tipo *association response* indicando o aceite da associação. A seguir é detalhado o processo de autenticação usando os mecanismos de autenticação aberta e chave compartilhada.

- autenticação aberta - O método de autenticação aberta é muito simples. Se um AP operar em modo de autenticação aberta, irá aceitar todas as solicitações de autenticação. Na primeira fase a estação que deseja se autenticar envia um quadro do tipo *authentication request*, posteriormente é encaminhada uma resposta positiva do AP através do quadro tipo *authentication response* (GAST, 2005), conforme é mostrado na Figura 13; e

Figura 13 - Mensagens trocadas no mecanismo de autenticação open system.

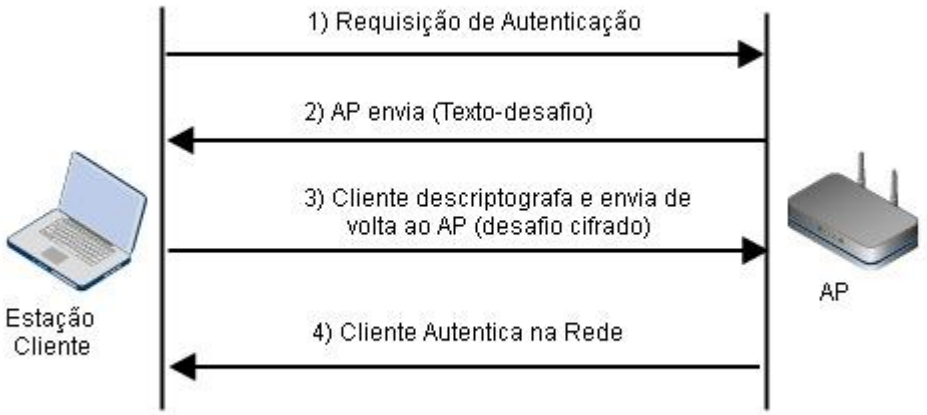
Fonte: Elaborado pelo autor.

- autenticação chave compartilhada - O método de autenticação compartilhada aceita autenticação das estações, estas, porém devem ter ciência da chave secreta compartilhada ao ponto de acesso em que ela deseja se autenticar. O procedimento para se estabelecer a autenticação funciona da seguinte forma: a estação encaminha uma solicitação de autenticação, *authentication request* para o AP com a identificação do algoritmo de autenticação que será usado. O AP responde encaminhando um *authentication response* que abriga um "desafio" *challenge text* com 128 bits de tamanho.

A estação responde com outro quadro, *authentication request*, com o desafio recebido do AP cifrado com a chave WEP. Em seguida o AP decifra o quadro recebido com sua chave e analisa se o desafio decifrado corresponde ao enviado. Caso a chave secreta encaminhada pela estação esteja de acordo com a chave encaminhada pelo AP a autenticação é realizada com

sucesso, encaminhado a estação um quadro do tipo *authentication response* com valor do campo *status code* igual a 0 (Figura 14).

Figura 14 – Mensagens trocadas no mecanismo de autenticação de chave compartilhada.



Fonte: Gast (2005) e Linhares e Gonçalves (2008).

3.2.2 Integridade do Protocolo WEP

O protocolo WEP inclui na mensagem a ser enviada um ICV, para verificar a integridade das mensagens recebidas. O ICV é um CRC que foi incluso na mensagem legitima antes da realização da criptografia. Quando a mensagem é recebida por uma estação cliente ou AP, esta decodifica e calcula o CRC-32, comparando com o CRC-32 anunciado no ICV. Caso sejam diferente o descarte da mensagem é efetuado.

3.2.3 Confidencialidade do Protocolo WEP

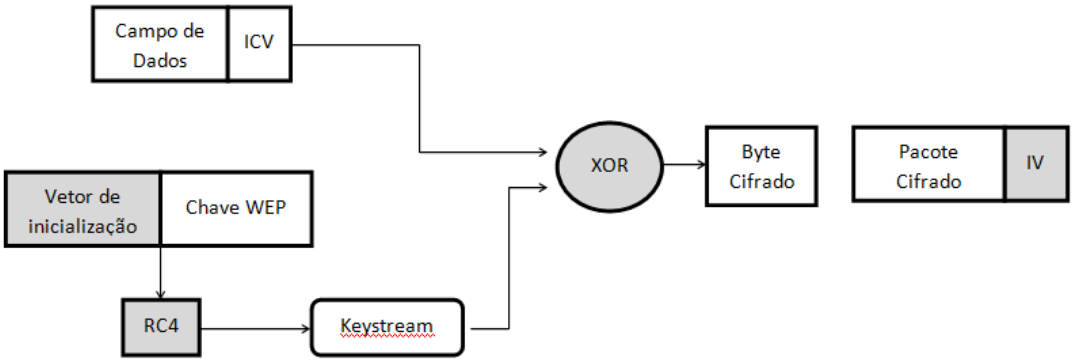
O WEP utiliza o algoritmo de criptografia RC4 no processo de confidencialidade das mensagens. Somente a mensagem e o ICV são criptografados, o cabeçalho IEEE 802.11 é transmitido de forma transparente utilizado um IV de 24 bits dinâmicos. A norma IEEE 802.11 especifica que a chave WEP de 64 bits usada pelo RC4 é constituída pelo IV de 24 bits associada a chave estática de 40 bits.

O algoritmo criptográfico RC4 é dividido em dois: *Key-Scheduling Algorithm* - KSA e *Pseudo-Random Generation Algorithm* – PRGA.

Para cada mensagem criptografada transmitida com seu ICV é gerado um IV novo, a fim de evitar a repetição de chaves. Levando em consideração que o RC4 é simétrico, a mesma chave é utilizada no método de decodificação. É decorrente disto que o IV é encaminhado de

forma transparente associada à mensagem criptografada, conforme é mostrado na Figura 15. Esse método é denominado encapsulamento WEP.

Figura 15 – Encapsulamento WEP.



Fonte: Linhares e Gonçalves (2008).

É realizado um XOR (OU Exclusivo) entre o byte do pacote e o byte gerado pelo RC4. O resultado é outro *byte* semelhante à cifra do pacote. Este ciclo é realizado até que o último *byte* do pacote e para cada ciclo do RC4 é gerada uma nova *keystream*.

3.2.4 Vulnerabilidades do Protocolo WEP

O protocolo WEP apresentou diversas vulnerabilidades:

- tamanho da chave – o WEP é passível a ataques de força bruta utilizando o método de dicionário, devido ao tamanho reduzido da chave compartilhada;
- alteração de mensagem – o CRC-32 foi originalmente desenvolvido para checagem de erros dos quadros de dados durante a transmissão (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 1999). É vulnerável ao ataque de modificação;
- problemas do RC4 – para a obtenção da chave secreta é utilizado um ataque denominado FMS. Este ataque captura informações e processa *byte* a *byte* até obter o valor provável da chave. Pode-se encontrar na internet diversos *softwares* capazes de realizar este ataque, tais como WEP *Crack* e *Airsnort*;
- reuso de chaves – em virtude de falhas na implementação e ao tamanho do IV que é de apenas 24 bits, o número de chaves é relativamente pequeno. Com isto, dependendo do tráfego da rede os IVs irão se repetir e consequentemente as chaves utilizadas pelo RC4 também;
- IV passado em claro - durante a conexão de um suplicante ao ponto de acesso, a chave secreta é passada de forma transparente e logo depois criptografada. Assim, é possível

ter acesso ao mesmo conteúdo das duas formas, facilitando o processo de obtenção da chave secreta;

- *backdoors* nos *firmwares* – é encaminhada uma *string* "*gstsearch*" via *broadcast* para porta UDP 27155 e o AP retorna com: senha de administrador, chave mestra WEP e filtro de MAC;
- gerenciamento de chaves – não possui gerenciamento de chaves, complicando a manutenção das redes, pois a troca de chaves não é realizada dinamicamente e sim manualmente. Em consequência disto, as chaves não são trocadas com certa frequência, colaborando para enfraquecimento da segurança; e
- negação de serviço - o atacante inocula este tipo de ataque no WEP principalmente nos quadros de gerenciamento e controle com a finalidade de afetar a disponibilidade da rede.

Nas especificações do protocolo WEP não foram aplicados mecanismos que ofereçam segurança contra ataques de *DoS* as camadas PHY e MAC. Desta forma, a camada PHY fica passível a ataques que utilizem a técnica de interferência, esta pode ser ocasionada de forma maliciosa ou por equipamentos que utilizem a mesma faixa de frequência. Já na camada MAC, a técnica de inundação de pacotes na rede sem fio podem ser realizadas com a inoculação de quadros falsificados, ou utilizar quadros de gerenciamento fabricados corrompendo associações seguras.

3.3 EMENDA DE SEGURANÇA WPA

O protocolo WEP apresentou diversas vulnerabilidades, com isto o grupo de trabalho do IEEE 802.11 iniciou uma pesquisa para a criação de um novo padrão de segurança que pudesse corrigir todas as falhas apresentadas pelo WEP. Este novo padrão se intitulou como IEEE 802.11i. Entretanto, devido às pressões do mercado, a *Wi-Fi Alliance* utilizou uma série de especificações propostas para o novo protocolo IEEE 802.11i e elaborou o protocolo WPA. O WPA apresenta uma série de mecanismos que solucionam alguns problemas de segurança vinculados ao WEP. Em seguida é apresentado um conjunto de características implementadas no protocolo WPA:

- o protocolo WPA envia e troca as chaves usadas para criptografia e integridade dos dados. Solucionando a questão do uso da chave estática do WEP;
- não suporta redes do tipo *ad-hoc;*

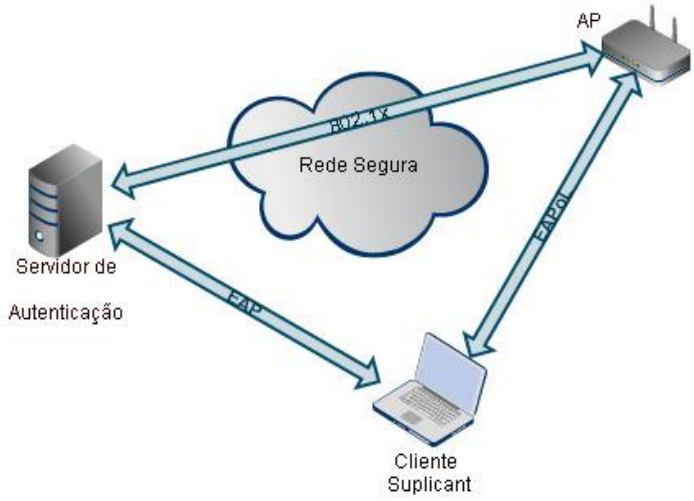
- foi implementado um novo código de checagem de mensagens, em que é utilizado um novo campo de 64 bits, o *Message Integrity Code* - MIC. Este realiza uma checagem do conteúdo do quadro de dados analisando se houve ou não modificação ou erros na transmissão de dados; e
- o IV reduzido do WEP possibilitava a repetição em um período de tempo curto; já com o WPA foi implementado um IV de 48 bits. Desta forma é possível mais de 280 trilhões de IVs diferentes (KATZ, 2012).

3.3.1 Autenticação do protocolo WPA

Existem dois métodos distintos de autenticação no protocolo WPA. Um elaborado para redes de pequeno porte, ou seja, redes domésticas, e outro método mais robusto usado em rede de grande porte que utiliza um servidor de autenticação RADIUS 802.1x/EAP (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 2001).

- WPA pessoal – método de autenticação utilizado para redes domésticas. A autenticação neste método é realizada pelo AP, é compartilhada entre o AP e a estação cliente uma WPA-*Pre Shared Key* - WPA-PSK que é uma *passphrase*. Esta é configurada de forma manual em cada equipamento pertencente à rede variando de 8 a 63 caracteres ASCII; e
- WPA corporativo – toda autenticação é realizada por um servidor de autenticação, independente se esta seja solicitada por um usuário ou dispositivo. Isto ocorre através da utilização de um servidor que utiliza o IEEE 802.1x associado a um tipo de e*xtensible authentication protocol* - EAP. Este protocolo é usado entre o AP e o servidor de autenticação. Funciona da seguinte forma: um cliente solicita uma autenticação, logo após o servidor checa em sua base de dados se o solicitante possui credenciais válidas. Caso as credenciais sejam válidas o cliente é autenticado e lhe é encaminhado uma chave *Master Session Key* - MSK. O canal lógico de comunicação segura gerada entre a estação cliente e o autenticador é feito pelo EAP, é neste meio que serão trafegadas as credenciais. É realizada uma comunicação física entre cliente e AP através do protocolo *extensible authentication protocol over LAN* - EAPoL e em sequência o AP realiza comunicação com o servidor de autenticação utilizando o protocolo IEEE 802.1x, conforme é ilustrado na Figura 16.

Figura 16 – WPA Corporativo.



Fonte: Elaborado pelo autor.

Os tipos de EAP mais usados no protocolo WPA são: EAP-MD5, EAP-*Transport Layer Security* - EAP-TLS, EAP-*Tunneled Transport Layer Security* - EAP-TTLS e *Protected Extensible Authentication Protocol* - PEAP.

Depois de realizada a autenticação é estabelecida as chaves através de um processo de derivação da *Pairwise Master Key* - PMK, denominado 4-*Way-Hadshake*. Caso a autenticação seja realizada no modo PSK, a chave é a mesma PSK. Já no outro modo de autenticação temos a PMK derivada com base na MSK compartilhada no processo de autenticação IEEE 802.1x/EAP. A PMK é utilizada apenas para gerar chaves temporárias *Pairwise Transient Key* - PTK e chave de integridade *Temporal MIC Key* - TMK. Após esse processo do 4-*WAY-Handshake* são confirmadas as equivalências das chaves, habilitando a troca de informações entre AP e estação cliente.

3.3.2 Integridade do protocolo WPA

Para análise da integridade dos dados no protocolo WPA é usado o ICV já utilizado no protocolo WEP e acrescentado ao quadro o MIC (KATZ, 2012). Para implementação do MIC é utilizado um algoritmo intitulado *Michael*. Diferente do CRC-32 o *Michael* é uma função *hash* não linear, totalmente diferente do CRC-32.

3.3.3 Confidencialidade do protocolo WPA

No protocolo WPA foi implementada o *Temporal Key Integrity Protocol* - TKIP, este solucionou várias vulnerabilidades existentes no WEP. O TKIP é formado através do conceito

de chaves temporais. Funciona da seguinte maneira: a chave é utilizada durante um período de tempo e trocada posteriormente de forma dinâmica.

O IV do WPA tem 48 bits sendo quase impossível o seu reuso. Como no cabeçalho do IEEE 802.11 é disponibilizado um campo para o IV de apenas 24 bits, foi criado um novo campo denominado IV *extended* para alocar o restante do IV. Este campo não faz parte do cabeçalho IEEE 802.11.

A forma de codificar é parecida com a do protocolo WEP, a diferença principal está em como a chave alimenta o RC4. A chave é gerada por um algoritmo de combinação de chave, em que a introdução é o IV, o endereço MAC do transmissor e a chave criptográfica. Logo em seguida a chave gerada pelo algoritmo de combinação e o IV são encaminhados para o RC4.

3.3.4 Vulnerabilidades do protocolo WPA

O WPA conseguiu conter algumas vulnerabilidades contidas no WEP, porém apresentou falhas em sua implementação, tornando-o vulnerável. Algumas dessas vulnerabilidades são apresentadas em seguida.

- ataques de dicionário – este ataque é utilizado quando o método de autenticação PSK é habilitado. Ocorre devido ao hábito das pessoas utilizarem palavras fáceis, diferente do ataque de força bruta o de dicionário esgota todas possibilidades de derivações de palavras pertencentes ao dicionário construído. Lembrando que caso a chave PSK tenha mais que vinte caracteres não existem tempo hábil para a quebra da senha; e
- negação de Serviço – o WPA apresenta os mesmos problemas relacionados a negação de serviço que o WEP apresentou, tendo em vista que estes ataques são realizados nos quadros de gerenciamento. Além destes, o MIC do WAP tem um mecanismo de proteção para inibir ataques de força bruta, mas este mecanismo também pode gerar um ataque de *DoS*. Quando dois erros de MIC são descobertos em um intervalo de tempo de um minuto o AP finaliza a conexão por sessenta segundos e troca a chave de integridade. Este processo, faz com que uma inoculação de pacotes mal formados gere um ataque de *DoS*.

3.4 EMENDA DE SEGURANÇA IEEE 802.11I (WPA2)

O padrão IEEE 802.11i foi criado para sanar problemas de segurança apresentados pelo WEP. Este padrão foi apresentado em 2004, e visa manter um nível mais elevado na segurança da comunicação. Algumas características do WPA estão presentes no WPA2, tendo

em vista que o WPA foi baseado em um esboço do WPA2 (LINHARES; GONÇALVES, 2008). A relevância deste padrão é a introdução do conceito de rede com segurança forte - RSN, este condiciona o acesso à rede somente pela Associação de Rede com Segurança Forte - RSNA. Uma RSN inclui controle de acesso IEEE 802.1x baseados em portas, técnicas de gerenciamento de chaves e protocolos de confidencialidade e integridade TKIP e CCMP. A segurança é realizada apenas na rede sem fio.

3.4.1 Autenticação da emenda IEEE 802.11i

No processo de autenticação do IEEE 802.11i é utilizado um *framework* IEEE 802.1x que promove a autenticação mútua e realiza o controle de acesso na WLAN. Este tipo de autenticação é composto por três elementos principais: autenticador, suplicante e servidor de autenticação - SA. Onde o suplicante são as estações, o autenticador é o AP e o servidor usado para autenticação RADIUS. O IEEE 802.1x realiza controle de acesso baseado em porta para controlar o fluxo de dados entre o DS e as estações. As requisições de autenticação EAP são realizadas através de uma porta não controlada pelo autenticador e os quadros de dados não EAP são encaminhado para uma porta controlada IEEE 802.1x. Somente é permitido o tráfego não EAP, caso o solicitante tenha êxito no processo de autenticação com SA. Desta forma, o IEEE 802.1x efetua o acesso não autorizado na WLAN (SAKIB et al., 2012). Ao final da autenticação EAP a porta controlada do autenticador permanece bloqueada. Mesmo que se tenha êxito na autenticação, a porta só é liberada quando as chaves temporárias forem negociadas e instaladas sobre o suplicante o autenticador, utilizando o método 4-*way handshake.* Além disso, o IEEE 802.11i possibilita autenticação PSK. Caso a chave pré-compartilhada esteja sendo utilizada não haverá autenticação EAP.

3.4.2 Disponibilidade da emenda IEEE 802.11i

Assim como no WEP e WPA, a ementa de segurança IEEE 802.11i não fornece proteção contra ataques de *DoS* nas camadas MAC e PHY. Desta forma, os quadros de gerenciamento e controle continuam desprotegidos, tal situação também acontece para os quadros EAP e EAPoL, podendo ser usados em ataques de *DoS* nas WLANs (ARAÚJO et al., 2013).

As RSNA são conexões sem fio que oferecem maior proteção as redes sem fio. A organização de uma RSNA pode ser demonstrada em cinco fases distintas:

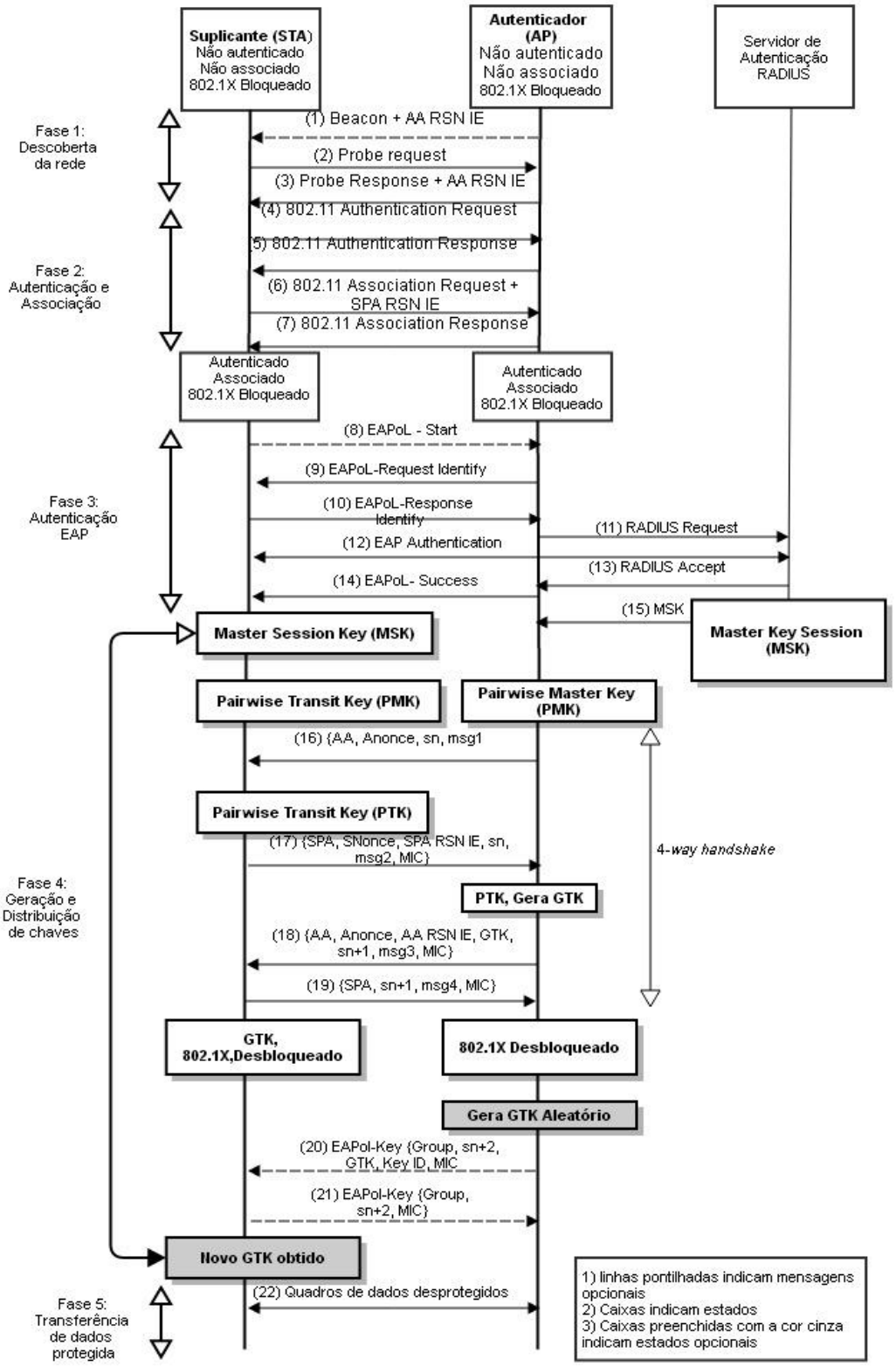
- fase 1 (descoberta da rede) – nesta fase o AP utiliza os quadros *beacon* e *probe response* para informar os seus serviços e política de segurança pelo elemento RSN

(RSN IE). Com estas informações a estação escolhe em qual AP deseja realizar uma associação segura. Neste período é realizada entre AP e estação uma negociação de protocolos de confidencialidade e integridade buscando proteger o tráfego *unicast*, método de autenticação recíproco entre AP e SA, um esquema de gerenciamento de chave criptográfica e serviços de pré-autenticação;

- fase 2 (autenticação e associação) – nesta fase o AP e a estação trocam identidades um com outro. Para que haja compatibilidade com versões de *hardware* mais antigas, a etapa *open system authentication* permanece antes da execução do *framework* de autenticação IEEE 802.1x na sessão EAP. O AP não envolve em sua própria autenticação, ele apenas repassa as mensagens entre estação e SA;
- fase 3 (geração e distribuição de chaves) – nesta fase o AP e a estação realizam várias operações para gerar e instalar chaves criptográficas sobre eles;
- fase 4(transferência de dados com proteção) – nesta fase essencialmente todos os quadros de dados enviados entre AP e estação possuem criptografia e colocam um conjunto de cifras negociadas na fase de descoberta da rede; e
- fase 5 (finalização da conexão) – é finalizada a associação segura entre WLAN e a estação.

A Figura 17 reproduz os passos realizados na consolidação de uma RSNA. As mensagens (1), (2) e (3) são referentes a fase de descoberta da rede. As mensagens de (4) a (15) são relativas à fase de autenticação e autenticação EAP. As mensagens (4) a (7) representam a autenticação da estação com o AP, nesta fase é necessário à realização desta autenticação simplificada antes da autenticação EAP. Em seguida a autenticação EAP inicia a troca de mensagens entre estação e SA. Nesta fase o AP desempenha o papel de intermediador, repassando as mensagens entre estação e SA. Na mensagem (8) é aplicado o quadro EAPoL-*Start* em que a autenticação é iniciada pelo suplicante ou pelo SA aplicando o quadro EAP-*Request Identify* conforme mensagem (9). Após a autenticação EAP realizada com sucesso, a mensagem (14) usando o quadro EAPoL-*Success* é compartilhada entre estação e SA denominando-se MSK. A MSK é utilizada pela estação para gerar uma PMK, desta forma comunicando-se de forma segura com o AP. As mensagens de (16) a (21) são referentes à fase de criação e distribuição de chaves, executadas pelo esquema 4-*way handshake.* Para que o estabelecimento de uma RSNA seja considerado com sucesso o esquema *4-way-handshake* tem que ser executado.

Figura 17 – Estabelecimento de uma RSNA.



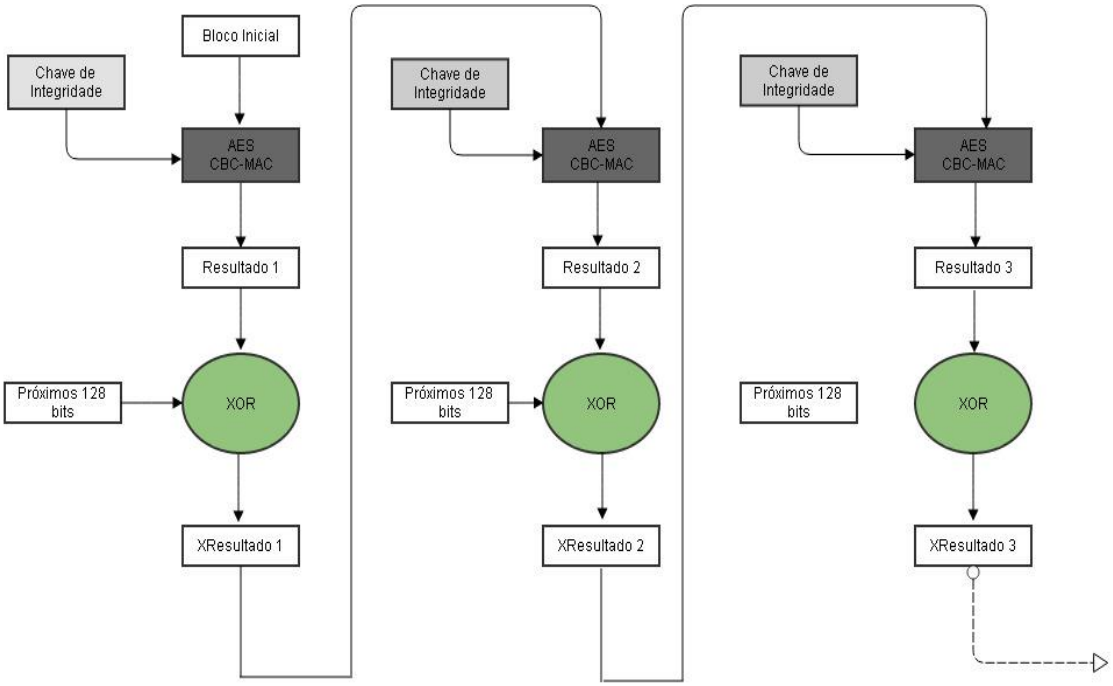
Fonte: Gill (2009).

3.4.3 Integridade da emenda IEEE 802.11i

A responsabilidade pela integridade e confidencialidade dos dados no WPA2 é o protocolo *Counter-Mode/Cipher Chaining Message Authentication Code* - CCMP. O CCMP é baseado no *Advanced Encryption Standard* - AES. A técnica de funcionamento do AES implementado pelo WPA2 é o CCM com chaves e bloco de 128 bits.

A responsabilidade pela integridade dos quadros e seu desempenho é o *Cipher Block Chaining Authentication Code* - CBC-MAC, de acordo com a Figura 18. A caixa "Bloco Inicial" corresponde aos 128 bits do campo de dados, em seguida é transmitido para o CBC-MAC o bloco e a chave de integridade. Na saída são gerados outros 128 bits, denominado "Resultado1". Em seguida é realizado um XOR entre o "Resultado1" e o bloco seguinte, apresentando como resultado "Xresultado1". Este é encaminhado para o CBC-MAC, gerando um novo resultado denominado "Resultado2". Este processo é repetido até o último campo de dados do pacote. Ao final deste fluxo, os 64 bits mais expressivos vão para o MIC.

Figura 18 – Integridade WPA2.



Fonte: Linhares e Gonçalves (2008).

3.4.4 Confidencialidade da emenda IEEE 802.11i

O conceito de chaves temporais também é aplicado no CCMP, igual o TKIP no WPA. Desta forma existe uma hierarquia de chave, em que as derivações da PMK criam chaves temporárias de criptografia e integridade. O responsável por criptografar os *frames* é o AES *Counter Mode* - CTR. A chave criptográfica é de forma simétrica e seu tamanho de 128 bits. O IV se mantém com 48 bits.

3.4.5 Vulnerabilidades da emenda IEEE 802.11i

- PSK reduzido - PSK com caracteres inferiores a 20 estão expostos a ataques de dicionário. Ressaltando que esta é uma falha do usuário e não do protocolo; e
- negação de serviço – assim como no WEP/WPA o WPA2 não oferece proteção aos quadros de gerenciamento e controle. Portanto, o padrão ainda é vulnerável a ataques deste tipo.

3.5 EMENDA DE SEGURANÇA IEEE 802.11W

Os mecanismos de segurança IEEE 802.11i apresentou melhorias quando comparado aos padrões WEP e WPA. No entanto, assim como os anteriores, o foco foi apenas na proteção dos quadros de dados, deixando os quadros de gerenciamento e controle ainda sem proteção. A ausência de proteção nesses quadros faz com que as redes sem fio se tornem vulnerável a ataques contra indisponibilidade de serviço. A implementação de novas ementas (IEEE 802.11r, IEEE 802.11k e IEEE 802.11v) que incluem aos quadros de gerenciamento novas informações importantes sobre a rede sem fio, visando melhorar a proteção nos quadros de gerenciamento e assegurar que as informações contidas nesses quadros não sejam utilizadas em ataques de indisponibilidade da WLAN, foi ratificada em 2009 a ementa IEEE 802.11w (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 2009).

O conceito de quadro de gerenciamento seguro é utilizado na ementa IEEE 802.11w, este compõe alguns princípios de segurança na WLAN, tais como Ahamad e Tadakamadla (2011) e Institute of Eletronic and Eletrical Engineers (2009) apresentam:

- proteção dos quadros de gerenciamento (*Management Frame Protection* – MFP) – é requisitada quando uma associação segura (RSNA) é requisitada, protegendo os quadros de RM contra falsificação e interceptação dos dados. São colocadas as regras após a chave PTK que protege os quadros de *unicast* estabelecida. Quanto aos quadros

de *broadcast/multicast*, as regras são impostas somente após a chave *integrity group temporal key* - IGTK ser instalada. Esta tem como objetivo proteger a integridade dos quadros RM destinados a um conjunto de estações;

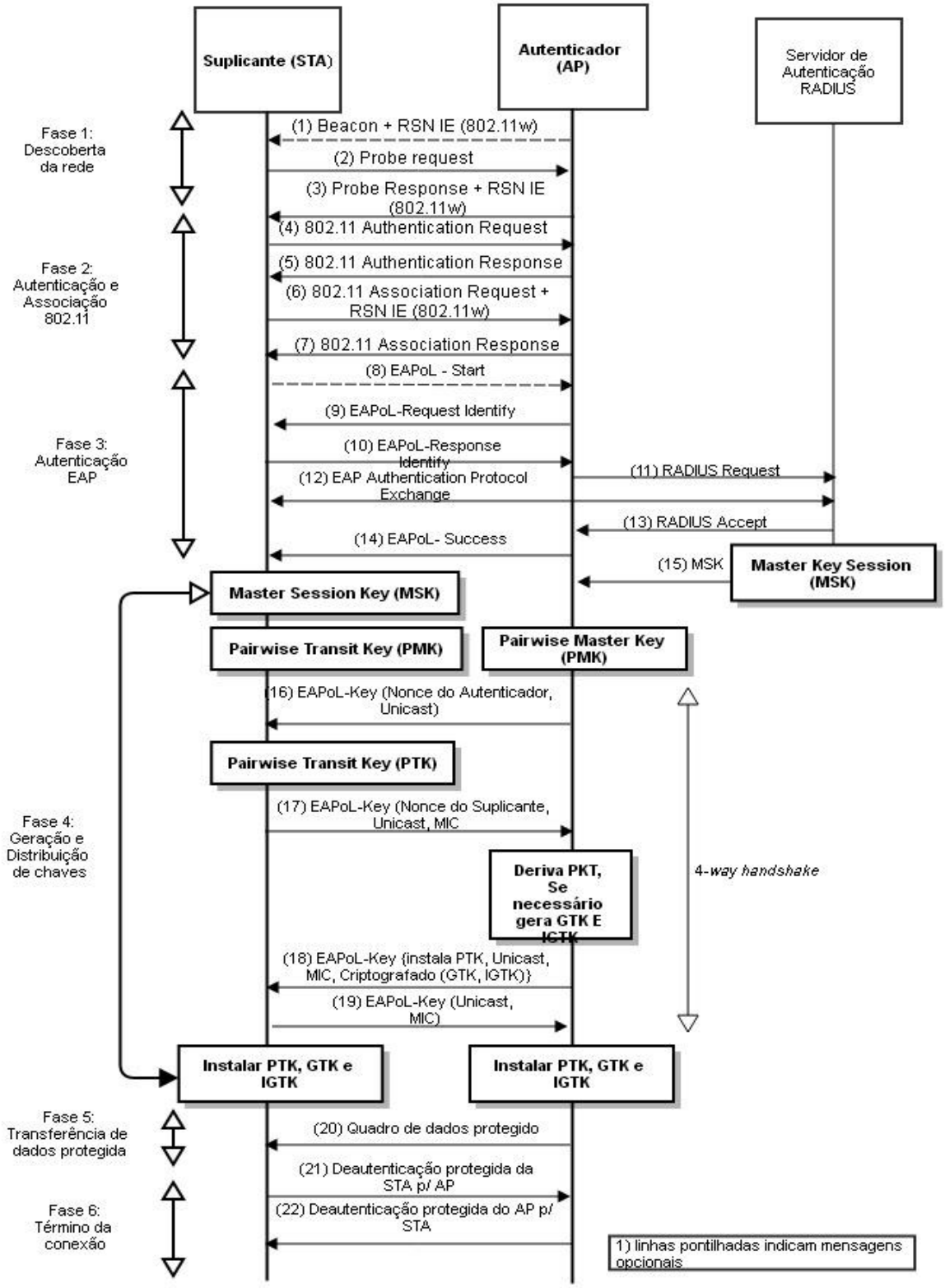
- autenticidade dos dados – a estação de destino de um quadro RM, tem a capacidade em reconhecer a estação que originou o quadro. Isto faz com que a estação reconheça se o quadro está sendo transmitido de uma estação legítima ou não, garantindo a autenticidade dos dados. Este conceito é aplicado apenas em quadros RM *unicast*; e
- detecção de repetição – a estação de destino tem a capacidade de checar se o quadro RM é repetido ou não.

O MFP é um serviço que oferece proteção a alguns quadros de gerenciamento denominados RM. Estes quadros de gerenciamento são: *deauthentication*, *diassociation* e *action*.

3.5.1 Autenticação da emenda IEEE 802.11w

A associação entre dispositivos com ementa de segurança IEEE 802.11w é parecida com o processo realizado na RSNA, diferenciando-se apenas por algumas modificações realizadas na máquina de estado. Entre essas modificações pode-se destacar a introdução de dois campos, *Management Frame Protection Required* - MFPR e *Management Frame Protection Capable* - MFPC, no campo RSN IE este informa se o dispositivo (Estação Cliente ou AP) exige ou não suporte a ementa IEEE 802.11w para que se estabeleça uma associação segura. São transmitidos pelo AP dois tipos de quadro *beacon* e *probe response*, estes são usados para anunciar as estações clientes se a associação que está sendo estabelecida suporta ou não IEEE 802.11w. Para informar a compatibilidade com a ementa IEEE 802.11w a estação transmite um quadro do tipo (*Re*)*Association request* na fase de autenticação e associação IEEE 802.11. As outras mensagens são trocadas de forma semelhante à RSNA, com exceção da mensagem (18) em que o AP encaminha o GTK junto com o IGTK para a estação e pelas mensagens (21) e (22), na qual é finalizada a conexão utilizando quadros RM protegidos. Na Figura 19 é apresentada uma RSNA em uma rede com suporte à ementa IEEE 802.11w (ARAÚJO, 2013).

Figura 19 – RSNA em uma rede WLAN com suporte a ementa IEEE 802.11w.



Fonte: Ahamad e Tadakamadla (2011).

3.5.2 Integridade e confidencialidade da emenda IEEE 802.11w

A integridade e confidencialidade de dados empregada na ementa IEEE 802.11w utiliza o modelo de hierarquia de chaves implementado no IEEE 802.11i. A inovação realizada pelo IEEE 802.11w é a geração de uma chave temporária IGTK, esta tem função de checar a integridade e detectar a repetição de quadros RM *broadcast/multicast*.

A chave IGTK é fundamentada no protocolo de integridade de mensagem *broadcast/multicast* (BIP) (INSTITUTE OF ELETRONIC AND ELETRICAL ENGINEERS, 2009), em que se utiliza o algoritmo de criptografia AES-128bits em modo operacional *block cipher based message authentication code* - CMAC. Este é usado para realizar a verificação de integridade e detecção de repetição nos quadros RM encaminhados para os suplicantes associados ao AP. As estações associadas a um AP, que tenham suporte aos IEEE 802.11w, recebem junto com o quadro RM *broadcast/multicast* um campo denominado *Management MIC Information Element* (MMIE), abrigando os subcampos IGTK, número do pacote IGTK - IPN e MIC.

3.5.3 Disponibilidade da emenda IEEE 802.11w

As redes WLANs RSN apresentam uma falha de segurança no término de uma associação segura, ocasionando problemas de disponibilidade. A ementa IEEE 802.11w implementa um processo de checagem de estado de segurança *Security Association Query* - SA *Query*, para solucionar este problema. Na qual a SA *Query* introduz dois quadros RM novos, SA *Query request*e SA *Query response*.

O quadro SA *Query request* é encaminhado pelo AP para associar o estado SA com uma estação associada. O AP encaminha um quadro SA *Query request* após receber o quadro (*Re*)*Association request* de um cliente com estado SA presente no AP. Caso a estação esteja ativa e seu estado SA seja válido, então a estação descriptografa o quadro usando o seu PTK e transmite o quadro SA Q*uery response* para o AP.

Outro avanço introduzido no IEEE 802.11w é a inclusão do campo *Time Element Information* – TEI no quadro de gerenciamento (*RE*)*association response*. O TEI tem como função anunciar para a estação comunicante que o AP está ocupado realizando o processo SA Q*uery*. Posteriormente, informa em quanto tempo o AP estará disponível para aceitar solicitações de associação da estação comunicante.

3.5.4 Vulnerabilidades da emenda IEEE 802.11w

A emenda IEEE 802.11w apresentou diversas melhorias, contudo, ainda apresenta algumas vulnerabilidades descritas a seguir:

- os quadros de controle permanecem sem proteção, possibilitando outras formas de ataques do tipo *DoS* que explorem técnicas de controle de acesso ao meio;
- problemas de atualização de *firmware* dos equipamentos com IEEE 802.11i; e
- a proteção dos quadros de gerenciamento está restrita a alguns quadros (*deauthentication, association e action*), não livrando a rede WLAN de ataques de *DoS* que afetam os quadros de controle.

3.6 AMEAÇAS E ATAQUES A REDES SEM FIO IEEE 802.11

O IEEE tem buscado implementar uma arquitetura de segurança mais robusta para redes IEEE 802.11. Porém ainda são encontradas vulnerabilidades neste padrão, as principais ameaças presentes no padrão IEEE 802.11 são (NIST, 2007):

- espionagem – devido ao meio de transmissão nas redes WLANs ser por RF, é fácil a captura do sinal transmitido. Cada atacante que esteja monitorando o meio pode captar as informações transmitidas (PLÓSZ et al., 2014);
- *man-in-the-middle* - MITE – neste tipo de ameaça o atacante se estabelece entre o usuário e o AP, desta forma consegue monitorar e obter informações referentes a autenticação deste usuário legítimo. Esta informação é utilizada pelo atacante, no qual o mesmo se personifica como se fosse o usuário vítima e autentica em outro AP (PLÓSZ et al., 2014);
- roubo de Sessão – esta ameaça é parecida com o MITE, após desconectar a estação legítima e assumir sua conexão com o AP, o atacante faz uma checagem sobre o usuário desconectado, não permitindo que ele restabeleça conexão (PLÓSZ et al., 2014);
- repetição de mensagem – o atacante intercepta mensagens ao realizar a escuta da rede, e posteriormente retransmite determinadas mensagens (PLÓSZ et al., 2014);
- acesso não autorizado – neste tipo de ameaça o atacante tenta burlar os dispositivos de segurança para conseguir se associar a WLAN. Este ataque pode ser realizado da seguinte maneira: o atacante realiza uma escuta na rede, e pelas informações obtidas cria uma lista de endereços MAC autorizada a acessar a WLAN (PLÓSZ et al., 2014);

- interceptação passiva – devido ao meio sem fio ser aberto, permite que o adversário monitore e colete dados, sem ser necessário se associar ou transmitir dados na rede WLAN (PLÓSZ et al., 2014); e
- negação de serviço – neste ataque o adversário tem como objetivo tornar os recursos ou serviços da rede indisponível. Várias técnicas utilizando este tipo de ataque podem ser empregadas, a seguir serão descritas algumas das metodologias de ataque de *DoS* utilizados em redes sem fio (PLÓSZ et al., 2014).
    - *chopchop* – neste tipo de ataque o adversário captura um quadro criptografado, logo em seguida usa uma estação para descobrir o conteúdo do quadro através da técnica de tentativas, isto se repete até que o ultimo *byte* do quadro capturado seja descriptografado (BITTAU; HANDLEY; LACKEY, 2006);
    - *fragmentation* – o adversário usa a técnica de fragmentação/montagem, esta é realizada pela estação base para desvendar a chave de fluxo usada para criptografar os quadros na WLAN (BITTAU; HANDLEY; LACKEY, 2006);
    - *deauthentication* - são inoculados na rede quadros de gerenciamento do tipo *deauthentication,* estes são enviados como pedidos fictícios de desassociação a clientes autênticos (BELLARDO; SAVAGE, 2003);
    - *duration* – o adversário encaminha quadros com o campo NAV muito elevado, desta forma impede que outras estações utilizem o meio compartilhado para transmitir (BELLARDO; SAVAGE, 2003);
    - *authentication flooding* – é transmitido pelo atacante quadros de autenticação, na tentativa de obter o reconhecimento por um endereço MAC válido presente no banco de dados cadastrado no AP. Estas solicitações falsas influenciam diretamente no processamento do AP, que por sua vez acaba negando autenticação a usuário legítimos (MITCHELL, 2005);
    - *Fake* AP – atacante cria um AP falso com o mesmo MAC e SSID do verdadeiro, para os clientes se associarem a ele (MITCHELL, 2005);
    - *Syn flooding* – o atacante envia um grande número de mensagens para um AP a uma alta taxa em que o AP não possa processá-las, isso faz com que outras estações não consigam acessar o canal (MITCHELL, 2005);
    - *RF Jamming* - Se origina através da emissão contínua de sinais de interferência de RF para ocupar o canal sem fio, bloqueando o tráfego legítimo (PLÓSZ et al., 2014);

- EAPoL-*Start* - É enviada uma carga excessiva de frames EAPOL-*Start*, isto gera uma sobrecarga no AP tirando-o de serviço (SPERTI et al., 2013);
- RTS *flood* - É executado através da técnica em que o adversário envia uma grande quantidade de *frames* RTS em um espaço de tempo curto, causando o congestionamento de reservas do canal sem fio. Que por consequência o adversário terá o controle completo do canal, negando serviço aos outros *hosts* na WLAN (LI; JOSHI; FININ, 2013); e
- *Beacon flood* - é gerada uma quantidade excessiva desses quadros, ou seja, com informações falsas do AP impossibilitando que clientes se associem ao AP verdadeiro (PLÓSZ et al., 2014).

É perceptível o esforço empregado pelo órgão responsável pelos padrões de segurança das redes sem fio. Ocorreram diversas atualizações em emendas de segurança buscando corrigir e sanar falhas. No entanto, os mecanismos de segurança propostos ainda apresentam vulnerabilidades, principalmente quando relacionada a ataques de *DoS*. Diante disto, é importante buscar ferramentas que possam auxiliar na proteção deste tipo de rede.

Foi apresentado neste capítulo a evolução das emendas de segurança propostas para redes sem fio padrão IEEE 802.11. Como também os mecanismos de proteção presentes em cada emenda de segurança e suas vulnerabilidades.

Apesar do esforço empregado para reduzir as ameaças e tornar o ambiente sem fio seguro, é possível identificar vulnerabilidades que colocam este tipo de rede em risco. Uma dessas vulnerabilidades esta presente em todas as emendas de propostas

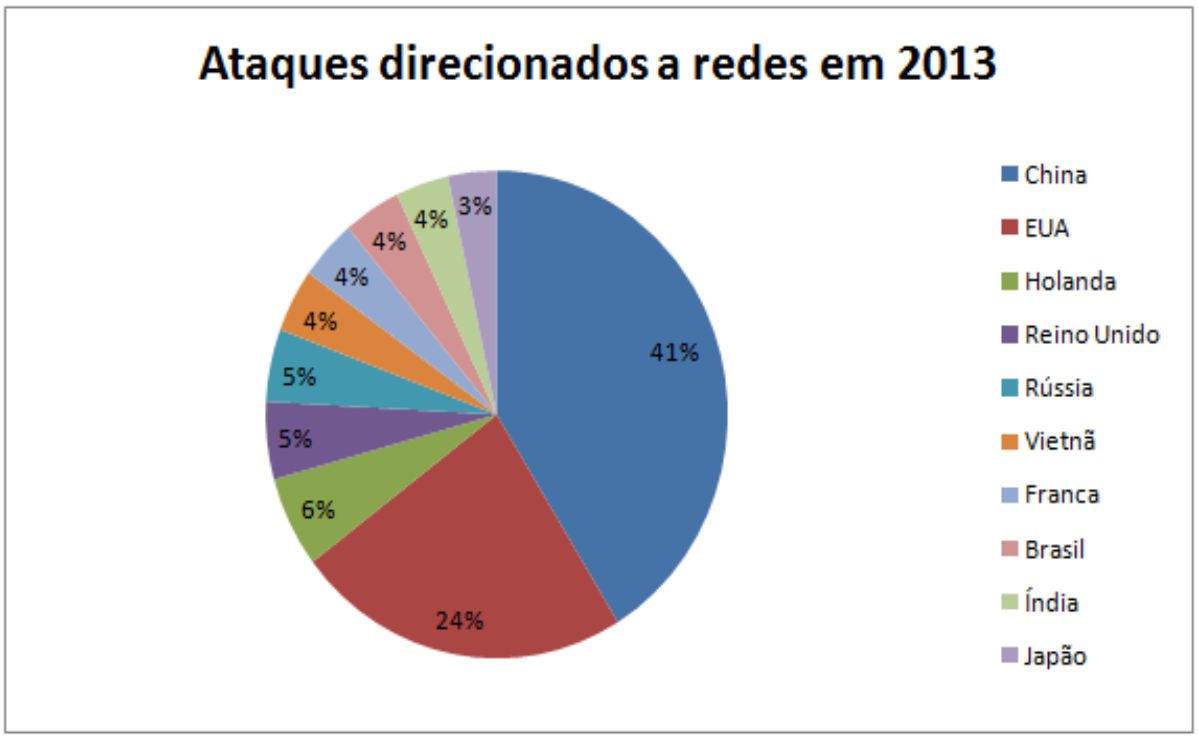
Neste capítulo foram apresentados conceitos sobre segurança em redes sem fio IEEE 802.11, e suas principais ameaças e tipos de ataques. No capítulo 4 será apresentada a contextualização sobre IDS e algumas abordagens da utilização dessas ferramentas em redes sem fio.

4 SISTEMA DETECTORES DE INTRUSÃO

As redes sem fio vêm obtendo um crescimento vertiginoso em praticamente todos os setores da sociedade. Com isto aumenta a preocupação com as vulnerabilidades apresentadas por elas, segurança tornou-se um requisito obrigatório. A Figura 20 apresenta dados obtidos pela empresa especializada em antivírus *Symantec*, nota-se que em 2013 o Brasil ocupou a oitava posição no *ranking* mundial de ataques a redes de computadores.

Esta situação evidencia a necessidade de se implementar mecanismos de proteção contra ataques as redes. Os IDS são aplicativos que se mostram eficazes para esta tarefa, atuam como uma segunda camada de defesa. Isto ajuda a reduzir a efetivação de ataques.

Figura 20 – Ataques realizados em redes de computadores.



Fonte: Symantec (2013).

O IDS é uma ferramenta capaz de avaliar o conteúdo dos pacotes transportados na rede, identificando-os como normal ou anômalo, ou ainda categorizar um ataque. O objetivo do IDS consiste em fornecer instrumentos que reduzam a possibilidade de intrusão. Isto pode ocorrer por antecipação dos ataques (HEINEN; OSÓRIO, 2005).

As métricas de detecção de intrusos preveem que os parâmetros ou comportamento apresentados por usuários legítimos são diferentes dos apresentados por um atacante. Com isto é possível reconhecer padrões das atividades realizadas no ambiente monitorado, e assim reportar os resultados do processo de detecção.

As arquiteturas para os IDS podem ser definidas em três categorias: baseada em *host*, baseada em rede e distribuída.

A arquitetura baseada em *host* consiste no monitoramento de um dispositivo, com a finalidade de identificar eventos intrusivos. Esse modelo de arquitetura define que para cada elemento monitorado deve existir um IDS. Desta forma cada dispositivo possui seu IDS baseado em *host,* não existe uma interação entre os IDS presentes nos dispositivos dispostos na rede.

A arquitetura baseada em rede consiste no monitoramento de um determinado segmento de rede, onde o IDS é posicionado de forma estratégica. Desta forma, o IDS tem a responsabilidade de monitorar e analisar todo tráfego pertencente a esta rede. Caso exista algum o IDS emite alertas.

A arquitetura distribuída permite o monitoramento modular da rede. Isto pode ser realizado através do posicionamento de diversos módulos em pontos estratégicos na rede. Os dados coletados por este módulos são direcionados para um controlador central que realiza o monitoramento e análise.

Outra característica importante presente nos IDS é o de coleta de dados. O processo de detecção de intrusos é dividido em duas etapas: coleta e análise de dados. A coleta de dados é uma etapa muito importante, um IDS necessita de informações que possibilitem o reconhecimento de eventos intrusivos (SPAFFORD; ZAMBONI, 2000). Portanto a coleta de dados é responsável por armazenar e fornecer tais informações ao IDS. O processo de formação desses conjuntos de dados consiste na captura de informações de segurança realizadas no perímetro da rede (RAJU, 2005). Conforme descreve Spafford e Zamboni (2000), o bom desempenho de um IDS esta relacionado nas informações nas quais são baseadas suas decisões.

O método de detecção utilizado por um IDS influencia diretamente em seu desempenho. O método utilizado para identificação dos eventos define como os conjuntos de dados são analisados. Os IDS podem utilizar diferentes maneiras de análise na identificação do tráfego intrusivo. Existem duas classes principais, são estes: os baseados em assinaturas e os baseados em anomalias (MAFRA et al., 2008).

Os IDS baseados em assinaturas realizam o reconhecimento de uma ação intrusiva através da associação entre os registros auditados e a caracterização pré-estabelecida do comportamento intruso. Cada evento identificado como intruso é reconhecido através de uma

assinatura, isto é uma série de atributos que o identifica. Isto torna possível que o IDS identifique ataques conhecidos de forma rápida e com uma baixa taxa de erro.

Esse método de detecção é baseado na construção e atualização de uma base de conhecimento de ataques. No entanto o comportamento de um evento intrusivo pode mudar constantemente. Isto pode ocasionar o não reconhecimento de determinadas intrusões, caso não estejam especificadas em sua base de conhecimento. Para reduzir este problema é necessário realizar a atualização constante da base. Porém esta ação é muito trabalhosa e demanda um alto custo computacional. É necessário gerar especificações que tenham o maior número de ataques previsto e não sejam associados a nenhum evento não intrusivo (SOBH, 2006).

A detecção baseada em anomalia consiste na afirmação de que todo evento intrusivo é reconhecido quando causa uma mudança no comportamento da rede. Então toda ação intrusiva apresenta características anômalas ao comportamento normal da rede (PARK, 2005). O método baseado em anomalia tem a capacidade de se adaptar as características da rede monitorada. As principais dificuldades estão em encontrar amostras anômalas na fase de treinamento (WU; BANZAHAF, 2010). Outra deficiência consiste na adaptação da mudança frequente no comportamento normal da rede.

Os resultados de desempenho apresentados por um classificador são calculados a partir de uma matriz de confusão. A matriz de confusa é uma tabela que demonstra a relação entre as classificações corretas e incorretas realizadas pelo IDS, conforme apresentado na Tabela 1.

Tabela 1- Matriz confusão.

		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: Araújo et al. (2013).

As métricas definidas para o cálculo da matriz de confusão usadas no classificador são seguintes: verdadeiro positivo (TP) indica um evento intrusivo avaliado corretamente; verdadeiro negativo (TN) indica um evento não-intrusivo avaliado corretamente; falso positivo (FP) indica um evento não-intrusivo classificado incorretamente como sendo um

intruso; falso negativo (FN) indica um evento intrusivo classificado incorretamente como sendo não-intrusivo (WU; BANZHAF, 2010).

4.1 ALGUMAS ABORDAGENS PARA A CONSTRUÇÃO DE IDS

O trabalho realizado por Ferreira et al (2011) teve como proposta o uso de transformada de *wavelets* para detecção de anomalias e classificação dos ataques através de redes neurais artificiais. O algoritmo desenvolvido identificou mudanças súbitas no comportamento da rede. Na sequência utilizou-se uma rede neural treinada para classificar os ataques detectados na fase anterior. Com isto foi possível demonstrar que a utilização de transformadas de *wavelets* junto com redes neurais artificiais pode aumentar a precisão na classificação de ataques.

O trabalho desenvolvido por Araújo (2013) utilizou conjuntos de dados representativos de uma rede sem fio, para treinar uma rede neural ARTMAP *Fuzzy* como algoritmo de detecção de intrusos. É aplicado uma *metaheurística* de otimização por enxame de partículas para determinar uma configuração de parâmetro que aumente a quantidade de identificações de ataques de *DoS* em uma rede sem fio com protocolo de segurança IEEE 802.11i habilitado.

Mafra et al (2008) desenvolveram um sistema denominado POLVO-IIDS, utilizando redes neurais *kohonen* para classificar os registros como: normal e anômalo. Além disto, empregaram redes neurais do tipo *Suporte Vector Machine* - SVM para determinar a classe dos ataques. Os autores destacam o uso de redes neurais para obter maior precisão. A base de conhecimento empregada na realização dos testes foi o KDD99.

O trabalho apresentado por Souza e Monteiro (2009), propõe a utilização de um IDS baseado em anomalia utilizando redes neurais artificiais. O objetivo do trabalho desenvolvido consistiu em buscar uma baixa taxa de erro na detecção dos padrões de ataque. Além de identificar padrões não conhecidos pela rede, porém pertencentes a mesma categoria de ataques já utilizados no treinamento da rede neural. A base de conhecimento utilizado foi o KDD99. Os autores consideraram satisfatórios os resultados obtidos, pois o classificador foi capaz de reconhecer novos ataques utilizando apenas as características por similaridade de ataque previamente conhecido.

Foi apresentado neste capítulo o conceito relacionado a sistemas de detecção de intrusão e sua importância no combate a ameaças a segurança de redes e aplicações. O emprego de IDS tem ajudado a melhorar o nível de segurança dos ambientes em que são aplicados. O número de propostas direcionadas a implementação desta ferramenta de segurança é grande, isso mostra que esta área necessita do desenvolvimento de pesquisas. A evolução das

pesquisas nesse segmento é importante para poder acompanhar as ameaças que colocam em risco o funcionamento das redes.

5 CONJUNTOS DE DADOS PARA AVALIAÇÃO DE SISTEMAS DE DETECÇÃO DE INTRUSÃO EM REDES SEM FIOIEEE 802.11

Neste capítulo é apresentada a metodologia empregada na construção dos conjuntos de dados e métricas utilizadas em sua avaliação perante alguns algoritmos de classificação e reconhecimento de padrões. É importante destacar que os conjuntos gerados neste trabalho têm como objetivo principal auxiliar o treinamento e a avaliação de sistemas de detecção de intrusão sem fio IEEE 802.11.

O processo de construção dos conjuntos foi realizado a partir da implementação três cenários de redes sem fio, as topologias de rede implantadas foram as seguintes: rede sem fio doméstica com segurança WEP/WPA habilitada; rede sem fio coorporativa com segurança IEEE 802.11i habilitada; rede sem fio acadêmica com segurança IEEE 802.11i associada a IEEE 802.11w habilitadas.

As subseções seguintes descrevem as características do ambiente, segurança, além de apresentar os métodos de coleta e o desempenho dos classificadores perante a cada conjunto gerado.

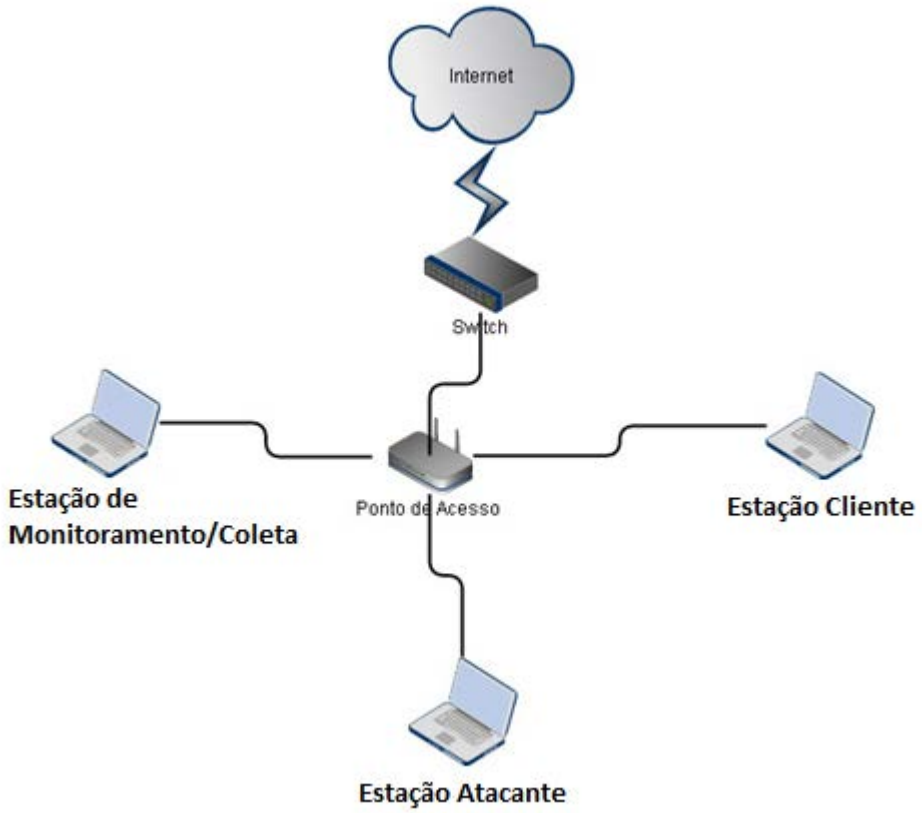
5.1 CENÁRIO 1 – UTILIZAÇÃO DE WEP/WPA

O primeiro cenário implementado possui características de rede sem fio doméstica com protocolo de segurança WEP/WPA habilitado. O protocolo WEP é considerado um mecanismo de proteção defasado e pouco implementado nas redes sem fio. Isto por que possui diversas vulnerabilidades, em especial a ausência de proteção dos quadros de gerenciamento e controle. Isto aumenta a possibilidade de os ataques apresentarem uma eficácia maior neste tipo de rede. Outros protocolos já surgiram depois do WEP apresentando melhorias em algumas das vulnerabilidades apresentadas pelo WEP. No entanto, ainda são encontradas muitas redes com este protocolo habilitado e o que se pode observar é que a maioria é proveniente de ambientes domésticos.

É importante destacar que a construção dos conjuntos de dados consiste em verificar a importância da evolução dos mecanismos de segurança empregados pelo IEEE e com isto é possível categorizar cada tipo de emenda proposta.

A topologia de rede foi baseada em um perfil básico *Basic Service Set* - BSS, e possui todos os componentes presentes em uma rede sem fio real, conforme apresenta a Figura 21. A rede é composta por: um ponto de acesso (AP); uma estação cliente; uma estação de monitoramento e coleta; uma estação atacante.

Figura 21 – Topologia de rede sem fio aplicada no cenário 1.



Fonte: Elaborado pelo autor.

A estação cliente tem a finalidade de inocular tráfego de rede normal (HTTP, FTP, SMTP, POP3 e SSH), este tipo de tráfego é comum em ambientes doméstico. A estação atacante foi configurada com sistema operacional Linux *Backtrack,* este sistema possui diversas ferramentas que permite efetuar ataques de forma automatizada. Na estação de monitoramento e coleta foi utilizado sistema operacional Linux *Ubuntu,* este sistema é baseado em *software* livre isto possibilita o uso de diversas ferramentas de monitoramento de rede gratuitas.

Os ataques realizados são os mesmos empregados no artigo de El-Khatib (2010), são ataques clássicos de *DoS* para redes sem fio. Essa diferenciação dos ataques é realizada para definir as categorias de ataques. Os ataques empregados foram: *chochop*; *deauthentication*; *fragmentation*; e *duration*.

No ataque *chopchop*, o atacante captura quadros criptografados da rede e utiliza uma estação base para decifrá-lo (BITTAU; HANDLEY; LACKEY, 2006). No ataque de *deauthentication*, o atacante envia quadros *deauthentication* fictícios para a estação de trabalho de clientes legítimos da rede, com o objetivo de desautenticá-los da rede

(BELLARDO; SAVAGE, 2003). O ataque de *fragmentation* utiliza a técnica de desmontagem/montagem para descriptografar a chave usada nos quadros de rede sem fio (EL-KATIB, 2010). Por fim, no ataque *duration*, o atacante envia quadros com valores muito grandes no campo NAV, impedindo que outras estações de usar o canal para transmitir (BELLARDO; SAVAGE, 2003).

Utilizou-se o aplicativo *airplay* (BAWISKAR; MESHRAM, 2013) para implementar todos os ataques de negação de serviço descritos. Os ataques são simples de realizar, isto permite que usuários não-avançados explorem as vulnerabilidades da rede. Com isto é possível observar o risco presente em tais redes.

Na etapa de monitoramento e coleta de dados utilizou-se aplicativo *wireshark* (LAMPING; WARNICK, 2004). Após o final da coleta dos dados utilizou-se a ferramenta *tshark* (LAMPING; WARNICK, 2004) para realizar um pré-processamento das amostras.

O pré-processamento das amostras consiste na remoção do *payload* mantendo apenas o cabeçalho MAC dos quadros. A escolha pelos dados do cabeçalho MAC ocorreu pois estes possuem características especificas das redes sem fio. Os campos utilizados dos quadros foram: *protocol version, type, subtype, to DS, from DS, more fragments, retry, Power management, more data*, WEP, *order, duration, address1, address2, address3 e sequence control*. Esta ação tem como finalidade organizar o conjunto de dados, isto facilita o uso deles pelo IDS através da definição de características.

A próxima etapa do processamento do conjunto consistiu em realizar a identificação de cada quadro. Esta ação adiciona um rótulo em cada quadro determinando se é normal ou anômalo, caso seja anômalo é descrito qual o tipo de ataque, na Figura 22 é apresentada a amostra dos dados. A inclusão do rótulo nos pacotes foi realizada através da identificação de cada pacote, isto é possível por meio da análise das características de cada pacote. Alguns campos são imprescindíveis para poder definir o tipo do pacote, são estes: *type*, *subtype* e os campos *address*.

Figura 22 – Organização do conjunto de dados.

```
0,0,12,0,0,0,0,0,0,0,0,1,2,0,0,0,Deauthentication
0,0,12,0,0,0,0,0,0,0,0,1,2,0,0,0,Deauthentication
0,0,12,0,0,0,0,0,0,0,0,1,2,0,0,0,Deauthentication
0,0,12,0,0,0,0,0,0,0,0,1,2,0,0,0,Deauthentication
0,0,12,0,0,0,0,0,0,0,0,1,2,0,0,0,Deauthentication
0,0,5,0,0,0,0,0,0,0,0,9,2,0,0,314,Normal
0,1,13,0,0,0,0,0,0,0,0,0,0,2,0,0,Normal
0,0,8,0,0,0,0,0,0,0,0,1,2,0,0,0,Normal
0,2,0,1,1,0,0,0,0,0,0,1,21,14,2,117,Normal
0,2,0,1,1,0,0,0,0,0,0,1,21,15,2,117,Normal
0,2,0,0,1,0,0,0,1,1,0,1,21,0,0,0,Normal
0,2,0,1,1,0,0,0,0,0,0,1,21,14,2,117,Normal
0,2,0,1,1,0,0,0,0,0,0,1,21,15,2,117,Normal
0,2,0,0,1,0,0,0,0,0,1,0,1,21,0,0,0,Normal
0,2,0,0,1,0,0,0,0,0,1,0,9,6,0,0,117,Normal
0,1,13,0,0,0,0,0,0,0,0,0,0,2,0,0,Normal
0,2,0,1,0,0,0,0,0,1,0,6,9,0,0,218,Normal
0,1,13,0,0,0,0,0,0,0,0,0,0,9,0,0,Normal
```

Fonte: Elaborado pelo autor.

A construção do conjunto de dados WEP/WPA foi baseado na pesquisa realizada por El-Khatib (2010). Os ataques e quantidade de amostras foram reproduzidos de forma semelhante. O total de amostras coletadas é de 24.200, estas estão organizadas em três conjuntos: treinamento, validação e teste, conforme é apresentado na Tabela 2.

O conjunto de treinamento é composto por 9600 amostras, destas 6000 são amostras originadas de tráfego normal e 3600 de tráfego anômalo. O tráfego anômalo do conjunto de treinamento foi dividido entre as quatro categorias de ataques selecionadas, com isto cada tipo de ataque originou 900 amostras. O conjunto de validação contém 6400 amostras, sendo 4000 amostras do tráfego normal e 2400 refere-se a tráfego anômalo. O tráfego anômalo do conjunto de validação seguiu os mesmo parâmetros sendo divido em 600 amostras para cada categoria de ataque. O conjunto de teste foi composto por 8200 amostras, sendo 5000 amostras originadas do tráfego normal e 3200 amostras de tráfego anômalo. Para cada tipo de ataque foram coletadas 800 amostras.

Tabela 2 - Distribuição das amostras no conjunto de dados do cenário 1.

Classe	Treinamento	Validação	Teste
Normal	6000	4000	5000
chopchop	900	600	800
deauthentication	900	600	800
Duration	900	600	800
Fragmentation	900	600	800
Total	**9600**	**6400**	**8200**

Fonte: El-Khatib (2010).

5.1.1 Avaliação de Desempenho dos classificadores de padrão para o cenário 1 (WEP / WPA)

A validação do conjunto de dados foi realizada com o emprego de algoritmos de classificação e reconhecimento de padrões, implementados na ferramenta WEKA. O WEKA é um *software* de mineração de dados amplamente utilizada em pesquisas de aprendizagem de máquina. Oferece diversas bibliotecas de classificação e agrupamento de tarefas (HALL, 2009). A escolha do *software* WEKA ocorreu pela facilidade disponibilidade de implementação de vários algoritmos de classificação e reconhecimento de padrões.

Foram utilizados algoritmos de classificação tradicionais para IDS, sendo eles: *Multilayer Perceptron* - MLP, *Radial Basis Function* - RBF e *Bayes Network* - *Bayes Net*.

O MLP é formado por um grupo de neurônios artificiais interligados por sinapses, distribuído em camadas e com comunicação sequencial (RUCK; ROGERS; KABRISKY, 1990). A opção pela rede MLP foi definida por ser eficiente na formação de representações internas das características dos dados de entrada, além disso, as redes neurais são fontes de inúmeras pesquisas, portanto é bastante utilizada como elemento de reconhecimento de muitas propostas de IDS.

As redes RBF fazem parte de uma classe de técnicas denominadas *gaussian potential functions* para classificação e aproximação de funções. As redes RBF são compostas por uma camada de entrada, uma camada intermediária onde o neurônio tem funções de ativação e uma camada de saída com ativação linear dos neurônios. A projeção e o processo de treinamento de uma RBF podem ser realizados de diversas maneiras (ORR, 1996). A RBF utiliza funções de proximidade, e este processo de aproximação também pode ser interpretado como um caso simples de rede neural. Suas principais vantagens são: aprendizado rápido, treinamento incremental e não apresenta problemas de paralisia da rede e mínimo local. Sua desvantagem é que após o treinamento se torna mais lenta para realizar a recuperação da informação, isto acontece por serem compostas de mais processadores que as MLP.

O *Bayes Net* utiliza métodos estatísticos bayesianos para organizar conjuntos de dados (FRIEDMAN; GEIGER; GOLDSZMIDT, 1997). O algoritmo *Bayes Net* cria uma rede Bayesiana completa, e a busca desta rede depende de mecanismo escolhido. Foi utilizado um Estimador simples, este é eficiente e seu aprendizado é rápido.

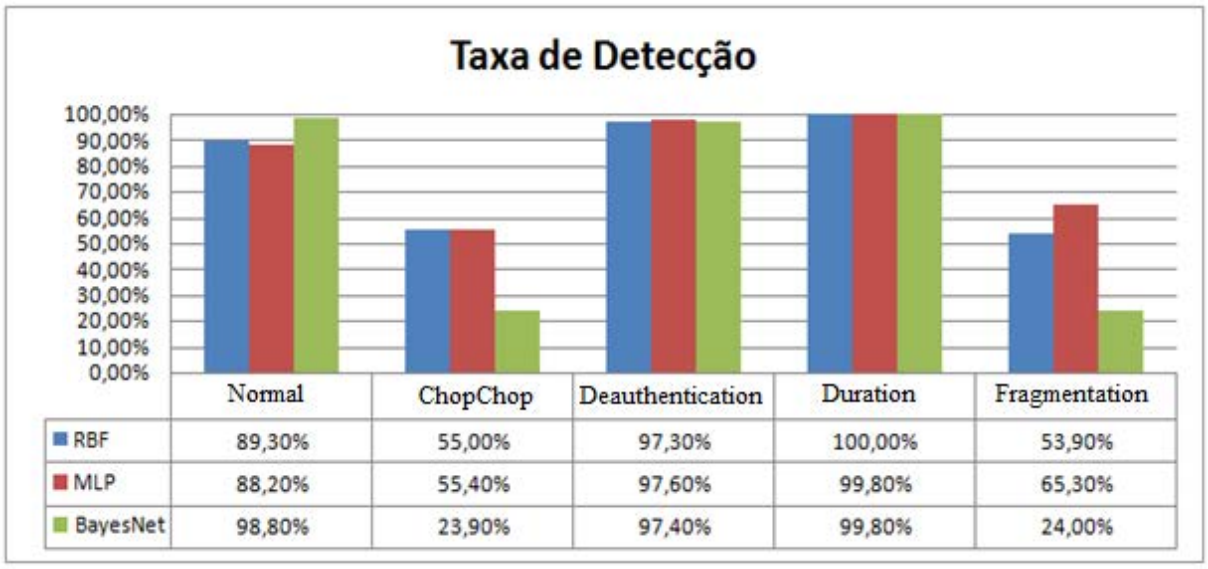
Para avaliar a capacidade de detecção do IDS perante o conjunto de dados utilizou-se a métrica de *recall* ou taxa de detecção, conforme Equação 1. Esta métrica apresenta a quantidade de eventos detectados pelo IDS como intrusão, isto não significa que estes eventos

são realmente eventos de intrusões verdadeiras. Pode-se também obter resultados falsos. Essa métrica é relativamente simples, mas é o suficiente para a avaliação. Isto por que será avaliada apenas a possibilidade de utilizar o conjunto de dados gerado como um ponto de referência para avaliar os IDS propostos. No entanto que a avaliação do IDS com outras métricas deve resultar de forma semelhante.

$$\text{Taxa de detecção} = \left(\frac{TP}{TP+FN}\right) \quad (1)$$

A Figura 23 apresenta os resultados obtidos com a utilização de algoritmos de classificação e de reconhecimento de padrões, utilizando o conjunto de dados gerado no cenário 1.

Figura 23 – Taxa de detecção do conjunto de dados WEP/WPA.



	Normal	ChopChop	Deauthentication	Duration	Fragmentation
RBF	89,30%	55,00%	97,30%	100,00%	53,90%
MLP	88,20%	55,40%	97,60%	99,80%	65,30%
BayesNet	98,80%	23,90%	97,40%	99,80%	24,00%

Fonte: Elaborado pelo autor.

O classificador *Bayes Net* apresentou melhores resultados que os outros classificadores na detecção do tráfego normal. Sua taxa de detecção foi de 98,8%, enquanto o MLP e RBF apresentaram aproximadamente 89% de reconhecimento do tráfego, conforme apresentado na Figura 23.

Os classificadores também apresentaram bons resultados na detecção dos ataques de *deauthentication* e *duration*. O ataque de *deauthentication* é realizado nos quadros de gerenciamento, as características dessa categoria de ataque são perceptíveis nos campos *type* e *subtype* do cabeçalho MAC. Enquanto que ataque de *duration* é empregado nos quadros de

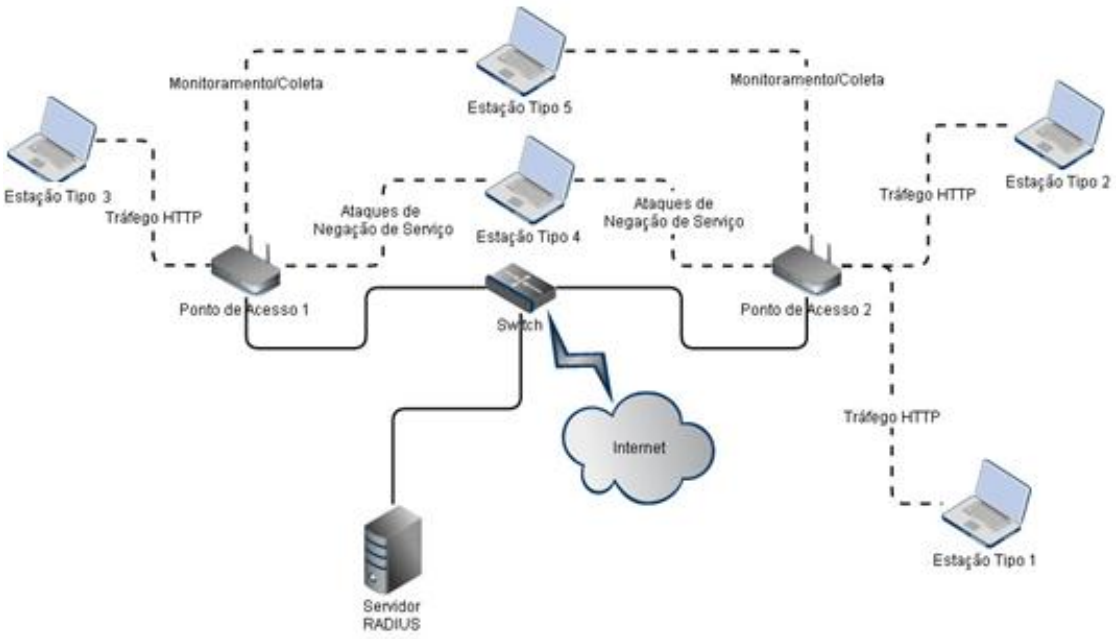
controle. Os campos que permitem diferenciar este ataque dos outros são *type*, *subtype* e *duration*.

Todos os classificadores apresentaram baixa taxa de detecção para os ataques de *fragmentation* e *chochop*, em especial o *Bayes Net* que obteve o pior resultado. A média de reconhecimento dos outros classificadores foi de 55%. Acredita-se que a baixa taxa de reconhecimentos dessas duas categorias acontece pelo fato das informações contidas nesses campos serem bem semelhantes ao tráfego normal. Apenas as informações contidas no cabeçalho MAC não são suficientes para aumentar o reconhecimento desses ataques.

5.2 CENÁRIO2 – UTILIZAÇÃO DE IEEE 802.11I

O segundo conjunto de dados foi gerado a partir da implementação de uma rede sem fio com criptografia IEEE 802.11i habilitada e associação segura. Este mecanismo é mais completo que o WEP, sendo mais utilizado em ambientes corporativos. A implementação do cenário 2 utilizou características desse tipo de ambiente, conforme demonstra Figura 24.

Figura 24 - Topologia de rede sem fio aplicada no cenário 2.



Fonte: Elaborado pelo autor.

O cenário 2 é composto por: dois pontos de acesso (AP), um servidor de autenticação responsável por controlar o acesso à rede, uma estação atacante, uma estação de monitoramento e as estações clientes.

O serviço de controle de acesso foi realizado por um servidor de autenticação RADIUS, para isto o IEEE 802.11i utiliza o *framework* IEEE 802.1x para prover a autenticação mútua e realizar o controle de acesso na rede sem fio. Esse controle é realizado para controlar o fluxo de dados entre os AP e as estações.

Como no cenário 1, as estações clientes têm como finalidade gerar o tráfego normal na rede sem fio (HTTP, FTP, SMTP e outros). A estação atacante foi configurada da mesma forma do cenário 1, com sistema operacional Linux *Backtrack.*

As categorias de ataques utilizadas para gerar o tráfego anômalo foram selecionadas por explorarem de forma efetiva as vulnerabilidades de disponibilidade presentes nas redes sem fio com IEEE 802.11i habilitada.

Os ataques empregados foram: *deauthentication*, *Fake authentication*, *Fake* AP e *syn flooding*. O ataque de *deauthentication* é similar ao efetuado no cenário 1 com criptografia WEP/WPA. O ataque de *fake authentication* o atacante envia solicitações de autenticação ao AP, isto afeta a capacidade de memória e processamento do AP. A consequência é a negação de serviços a usuário legítimos (HE; MITCHELL, 2005). No *Fake* AP o atacante cria vários perfis do AP verdadeiro, com mesmo SSID e endereço MAC. Com isto usuários acabam tentando se associar aos perfis falsos (HE; MITCHELL, 2005). O ataque de *syn flooding* o atacante envia uma carga excessiva de mensagens para o AP, de forma que ele não consiga processar. Isto faz com que outros usuários não consigam utilizar o canal de comunicação (HE; MITCHELL, 2005).

As configurações da estação de monitoramento e coleta são semelhantes às aplicadas no cenário 1. O método de coleta de dados utilizado foi *holdout test,* esse método é realizado por estimativa por amostragem (KOHAVI, 1995). A escolha pelo *holdout* ocorreu devido a este método apresentar taxa de erro no conjunto de teste próximo a taxa de erro verdadeira, isto quando submetido a uma grande quantidade de amostras. O conjunto de dados gerado foi dividido em dois grupos: treinamento e teste. O conjunto de treinamento é utilizado para treinar o sistema de classificação, já o conjunto de teste tem como finalidade exclusiva mensurar a taxa de erro do classificador. O raciocino prevê que o desempenho apresentado por um classificador no conjunto de teste seja o mesmo apresentado em seu uso real. Neste cenário não foi gerado um conjunto de validação, este é utilizado apenas como um *pseudoteste* que tem como finalidade apenas avaliar o desempenho da rede durante o treinamento.

A divisão das amostras para os conjuntos de treinamento e teste foi a seguinte: 75% para treinamento e 25% para teste. Assim foram armazenadas 10.000 amostras, sendo 7.500 pertencentes ao subconjunto de treinamento e 2.500 subconjunto de teste, conforme mostra a Tabela 3.

As 7.500 amostras do subconjunto de treinamento estão divididas assim: 4.500 amostras de tráfego normal e 750 amostras para cada categoria de ataque. O subconjunto de treino tem 2.500 amostras, sendo: 1.500 pertencentes ao tráfego normal e 250 amostras para cada categoria de ataque.

Tabela 3 - Distribuição das amostras no conjunto de dados do cenário 2.

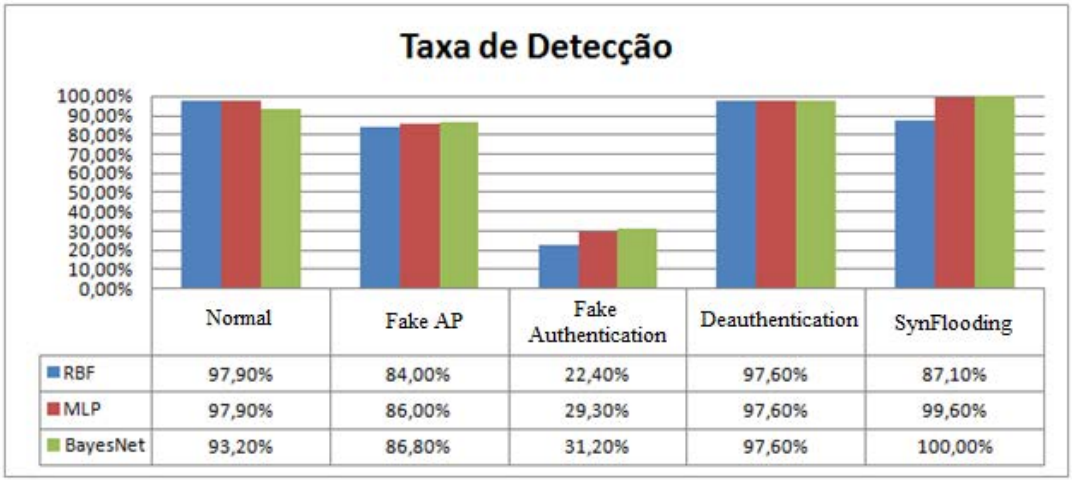
Classe	Treinamento	Teste
Normal	4500	1500
Deauthentication	750	250
FakeAuthentication	750	250
Fake AP	750	250
SynFlooding	750	250
Total	**7500**	**2500**

Fonte: Elaborado pelo autor.

5.2.1 Avaliação de Desempenho dos classificadores de padrão para o cenário 2 (IEEE 802.11i)

A Figura 25 apresenta os resultados obtidos pelos algoritmos de classificação e de reconhecimento de padrões, do conjunto de dados gerado.

Figura 25 - Taxa de detecção do conjunto de dados IEEE 802.11i.



Fonte: Elaborado pelo autor.

Os classificadores apresentaram resultados semelhantes no reconhecimento do tráfego normal. MLP e RBF apresentaram resultados semelhantes, sua taxa de detecção foi de 97,90% neste perfil de tráfego. Porém, o algoritmo *Bayes Net* obteve resultado inferior aos outros com um reconhecimento de 93,20%.

Nas categorias de ataques, o desempenho dos classificadores foi igual no reconhecimento do ataque de *deauthentication* com uma taxa de detecção de 97,60%. Conforme detalhado no cenário 1 o ataque de *deauthentication* possui características em determinados campos que facilitam seu reconhecimento. No ataque de *syn flooding* o *Bayes Net* apresentou taxa de detecção de 100%, MLP 99,60% e RBF 87,10%. Esta categoria de ataque age efetivamente nos quadros de controle RTS e CTS.

Os ataques de *fake* AP e *fake authentication* não tiveram resultados bons. O ataque de *fake* AP obteve uma média de reconhecimento de 85% e *fake authentication* 30%. Essas categorias de ataques possuem características muito próximas ao do tráfego normal, isso dificulta o reconhecimento pelos classificadores. Eles afetam os quadros gerenciamento do tipo *authentication* e *beacon*. É necessário analisar outros atributos além dos presentes no quadro MAC.

5.3 CENÁRIO 3 - UTILIZAÇÃO DE IEEE 802.11W

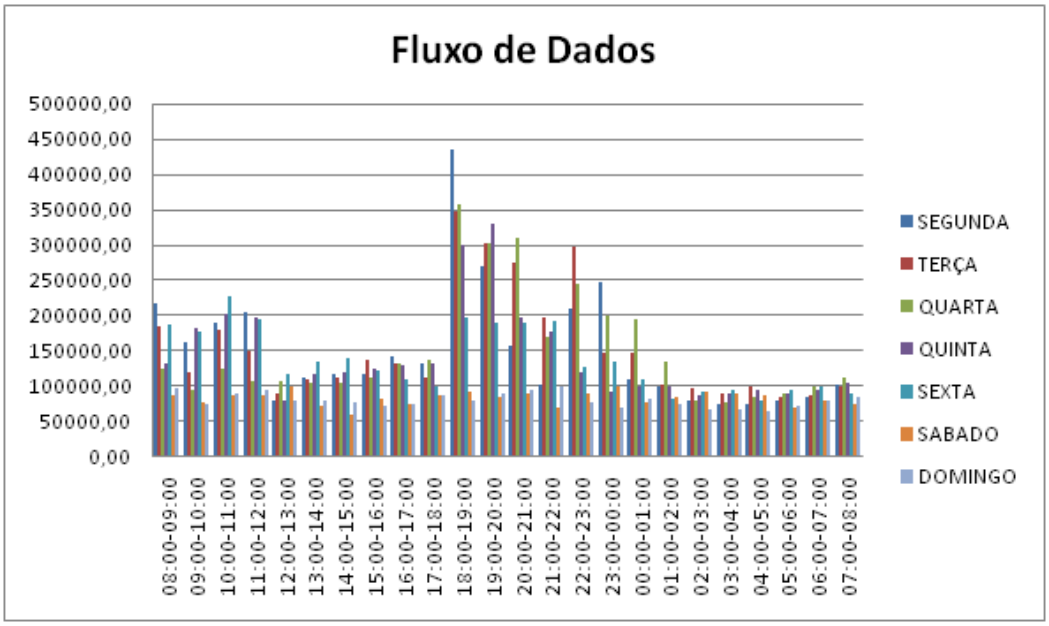
A construção do terceiro cenário foi realizado em uma ambiente acadêmico e com protocolo de segurança IEEE 802.11i associado ao IEEE 802.11w. A escolha por um cenário acadêmico ocorreu principalmente pela diversidade de dispositivos móveis presentes neste tipo de rede, grande fluxo de dado se por obter características diferentes dos cenários anteriores. A diferenciação entre os cenários propostos são importantes para categorizar cada tipo de tráfego de acordo com cada tipo de ambiente.

A construção dos conjuntos anteriores foi realizada através da coletada de dados por amostras, neste terceiro a armazenagem de dados escolhido foi temporal. A construção de um conjunto de dados temporal possibilita obter um padrão do comportamento das atividades dos usuários da rede, tais como, mudanças de comportamento da rede e analisar os períodos em que a rede tem maior fluxo de dados.

A primeira etapa realizada consiste em analisar o período em que a rede é mais acessada. Para isto realizou-se um monitoramento prévio de sete dias. Esse período é o suficiente para definir o padrão de utilização da rede sem fio. A Figura 26 demonstra o monitoramento

realizado. Constatou-se que o período entre as dezoito horas e dezenove horas a rede possui maior volume de dados trafegados.

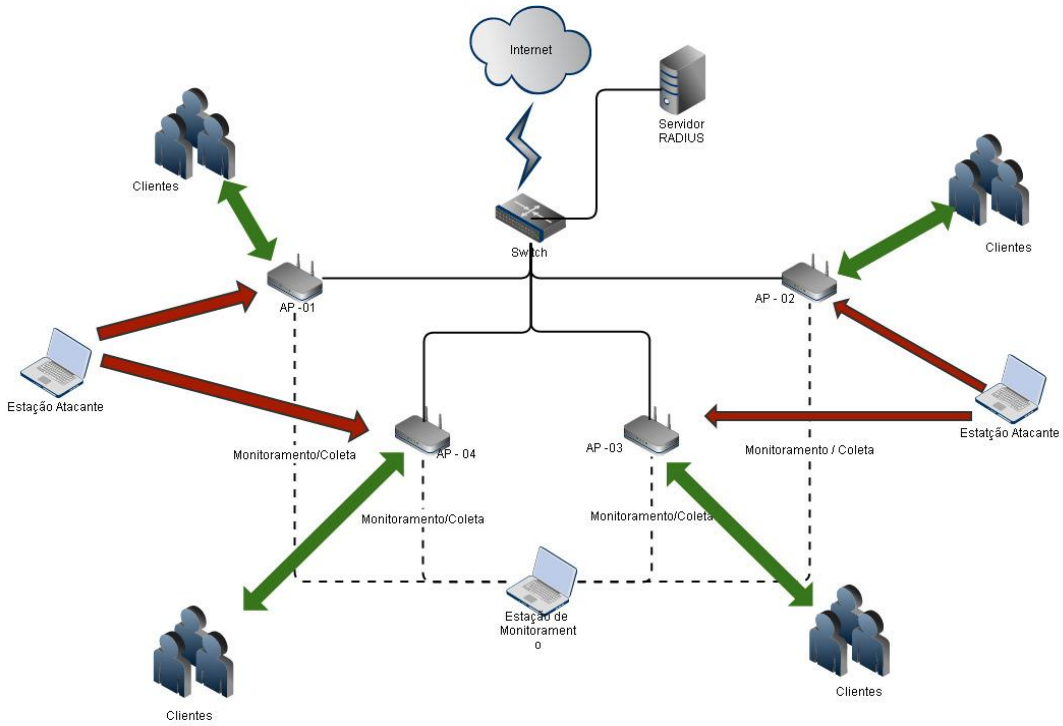
Figura 26 – Fluxo de dados da rede sem fio (IEEE 802.11w).



Fonte: Elaborado pelo autor.

A Figura 27 apresenta a topologia de rede implantada no cenário 3.

Figura 27 - Topologia de rede sem fio aplicada no cenário 1.



Fonte: Elaborado pelo autor.

Sua composição possui: quatro pontos de acesso (AP); um servidor RADIUS; duas estações de ataque; uma estação de monitoramento; e clientes da rede.

Todo o perímetro do ambiente selecionado possui cobertura de sinal de rádio, isto é feito pelos quatros pontos de acesso. Os pontos de acesso estão todos interligados, isso permite que todos os usuários estejam conectados em uma rede única. A diversidade de dispositivos e vários perfis de usuários gera variados tipos de tráfego categorizados como normal. O monitoramento realizado na fase anterior não identificou nenhum tipo de tráfego anômalo. O monitoramento assim como nos cenários anteriores foi realizado por uma estação sem fio, com sistema operacional Linux *Ubuntu* e auxilio do *software Wireshark*. Os ataques foram empregados por duas estações sem fio, as estação não estavam associadas a rede. Foram alocadas em locais estratégicos para obter apenas sinal de rádio frequência. As estações inocularam tráfego anômalo, o Quadro 5 apresenta os ataques empregados.

Foram executados quatro tipos de ataque, sendo dois empregados nos quadros de gerenciamento, um no quadro de gerenciamento e dados e outro no quadro de controle. Estes ataques são técnicas comuns muito empregadas em redes sem fio. A escolha por tipos de ataques diferentes é necessária, pois cada um possui um tipo de característica. Os ataques empregados ocorrerem da seguinte maneira: um ataque por dia no período de maior fluxo, no quinto dia os ataques foram empregados de forma simultânea.

Quadro 5 – Tipos de ataques.

Ataque	**Tipo Quadro**
Deauthentication	Gerenciamento
BeaconFlood	Gerenciamento
EAPOL-Start	Gerenciamento\Dados
RTS-Flood	Controle

Fonte: Elaborado pelo autor.

Os ataques empregados nos quadros de gerenciamento foram: *deauthentication* e *beacon flood*. O ataque de *deauthentication* consiste no envio de quadros do tipo *deauthentication*, no entanto os quadros enviados são fictícios e buscam desautenticar clientes legítimos pertencentes à rede (BELLARDO; SAVAGE, 2003). Para empregar o ataque, foi inoculada uma sequência de cem quadros falsos, em seguida foram enviados mil quadros e por último foi inoculado uma sequência ininterrupta de quadros *deauthentication* falsos. A análise obtida com este ataque mostra que os quadros fictícios enviados pela estação atacante foram ignorados pelo ponto de acesso, não afetando a disponibilidade dos serviços. Os *beacons* são quadros enviados pelo AP com informações da sua capacidade naquele momento. No ataque

de *beacon flood* é gerada uma quantidade excessiva desses quadros, ou seja, com informações falsas do AP impossibilitando que clientes se associem ao AP verdadeiro. Mesmo com o emprego da emenda IEEE 802.11w o ataque surtiu efeito, pois o ataque é direcionado aos clientes da rede.

O ataque direcionado aos quadros de gerenciamento e dados foi o EAPOL-*Start.* O ataque de EAPOL-*Start* tem como propósito afetar a disponibilidade do ponto de acesso, para isto envia quadros EAPOL a fim de parar os recursos internos do rádio.

O ataque de RTS *Flood* é direcionado aos quadros de controle. Para realizar o ataque de RTS *Flood* foi instalado o *metasploid-framework*. Através deste foram transmitidos quadros RTS no meio de comunicação, esses quadros tiveram o campo de duração alterado para um valor maior. Isto é visa ocupar o canal por períodos de tempo maiores.

A quantidade de pacotes armazenados, durante o período de monitoramento, foi de 12.297.571. A distribuição dos pacotes durante o tempo de monitoramento é apresentado na Tabela 4. O mesmo pré-processamento realizado nos outros conjuntos foi realizado neste.

Tabela 4 - Distribuição das amostras no conjunto de dados do cenário 3.

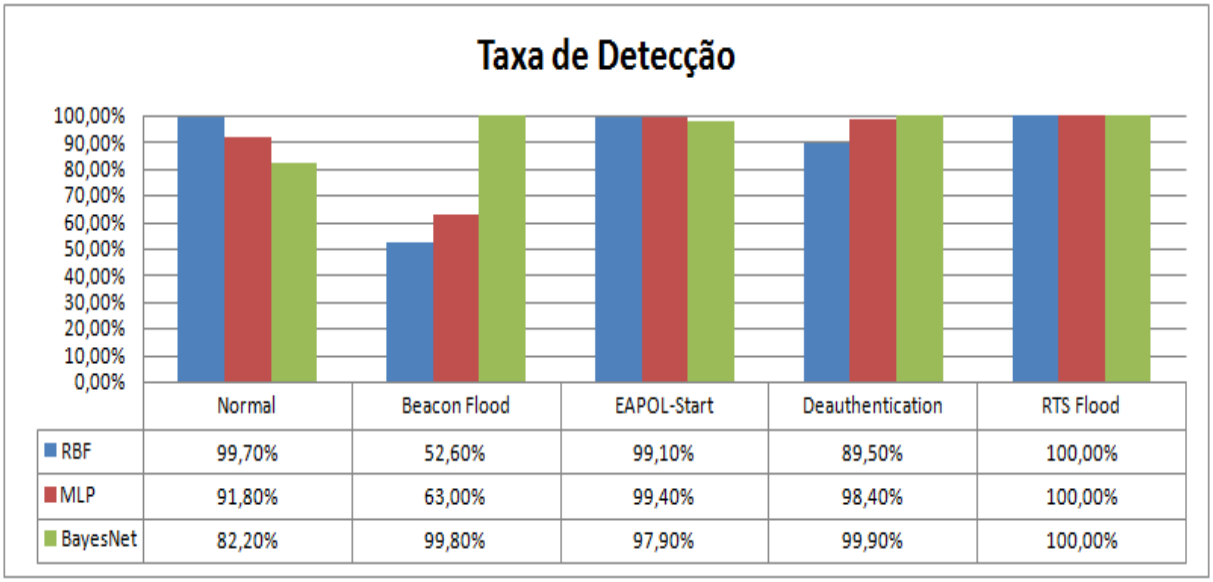
Classe	Conjunto de dados
Normal	10886309
deauthentication	323976
Beaconflood	545481
EAPOL-*Start*	539692
RTS *flood*	2113
Total	**12297571**

Fonte: Elaborado pelo autor.

5.3.1 Avaliação de Desempenho dos classificadores de padrão para o cenário3 (IEEE 802.11w)

A Figura 28 apresenta os resultados obtidos com a utilização de algoritmos de classificação e de reconhecimento de padrões, no conjunto de dados do cenário 3.

Figura 28 - Taxa de detecção do conjunto de dados IEEE 802.11w.



	Normal	Beacon Flood	EAPOL-Start	Deauthentication	RTS Flood
RBF	99,70%	52,60%	99,10%	89,50%	100,00%
MLP	91,80%	63,00%	99,40%	98,40%	100,00%
BayesNet	82,20%	99,80%	97,90%	99,90%	100,00%

Fonte: Elaborado pelo autor.

O algoritmo RBF obteve taxa de detecção de 99,70%, MLP apresentou 91,80% e *Bayes Net* apresentou o pior desempenho para o tráfego normal. No ataque de *deauthentication* os classificadores apresentaram resultados similares, essa categoria de ataque explora os quadros de gerenciamento. O ataque de RTS *flood* obteve taxa de detecção de 100% por todos os classificadores. Este tipo de ataque é empregado no quadro de controle do tipo RTS. O reconhecimento desse ataque se torna fácil pelo classificador, pois possui valores muito diferentes do tráfego normal. Isto pode ser notado no campo *duration* que possui um valor muito alto. O ataque de EAPOL-*Start* apresentou resultados próximos com uma taxa de detecção de aproximadamente 98%. Esse ataque é empregado no quadro de gerenciamento de *authentication* e no quadro de dados. A taxa de detecção para o ataque de *Beacon Flood* não foi muito boa, RBF apresentou 52,60%, MLP 63% e *Bayes Net* obteve o melhor resultado com 99,80%. As características desse ataque se assemelham muito com o tráfego normal. Apenas os atributos presentes no cabeçalho MAC não foram suficientes para se ter uma boa taxa de detecção.

5.4 COMENTÁRIOS E DISCUSSÕES

Foi apresentado neste capítulo o relato da construção de três conjuntos de dados formados por tráfego de rede sem fio, normal e anômalo. Essa proposta utilizou a aplicação das emendas de segurança WEP, IEEE 802.11i e IEEE 802.11w para cada cenário implementado.

Os conjuntos de dados foram submetidos a avaliações de alguns algoritmos de classificação e reconhecimento de padrões, tal procedimento foi executado para avaliar o comportamento do conjunto de dados. Os resultados alcançados pelos classificadores empregados na avaliação permitem concluir que a abordagem proposta é bastante promissora. A diversificação dos cenários e tipos de ataques permitiu categorizar vários tipos de tráfego, tanto normal quanto anômalo.

As diferenças encontradas nas taxas de detecção dos classificadores estão relacionadas a aspectos intrínsecos dos algoritmos de classificação, o que é considerado normal, pois os algoritmos são baseados em mecanismos diferentes. Além disso, como o objetivo principal desta pesquisa é a construção dos conjuntos de dados, os parâmetros utilizados nos algoritmos de classificação e reconhecimento de padrões não foram otimizados, como acontece em pesquisas cujo objetivo é o estudo destes algoritmos.

6 CONCLUSÕES

Existe um grande número de propostas de IDS para redes, porém a avaliação justa entre as diversas abordagens é uma árdua tarefa, afinal, é muito difícil reproduzir o mesmo cenário empregado pelo autor da proposta, principalmente com o perfil de comportamento dos usuários. Uma maneira de realizar a comparação é através da aplicação do IDS em um conjunto de dados. Porém, a maioria dos conjuntos de dados são oriundos de dados de simulação ou de redes cabeadas. Assim, não é viável o emprego destes conjuntos de dados na avaliação de IDS para redes sem fio em função das diferenças significativas entre as redes.

Durante esta pesquisa foi produzido um conjunto de dados oriundo do funcionamento de uma rede sem fio real, baseado no padrão IEEE 802.11, com três cenários distintos e bastante utilizado atualmente: cenário com criptografia WEP, cenário com mecanismo de segurança IEEE 802.11i e o terceiro baseado na ementa IEEE 802.11i associado ao IEEE 802.11w.

Com o emprego de alguns algoritmos de classificação e reconhecimento de padrões, obteve-se bons resultados na identificação de ataques de negação de serviços. Pode-se concluir que os campos do cabeçalho da camada MAC foram suficientes para detecção. Os campos *type, subtype, duration* e *address* tiveram contribuição significativa neste processo, principalmente na identificação dos ataques *deauthentication*, duração, *syn flood*, RTS *flood* e EAPOL-*Start*. O cenário não se repetiu com outros tipos de ataques: fragmentação*, beacon flooding*, autenticação falsa, AP falso e *chopchop*. A contribuição destes campos não foi importante, aliás, a detecção destes ataques foi ruim.

Os diferentes resultados permitem-se concluir que alguns campos do cabeçalho MAC são mais significativos para alguns tipos de ataques. Portanto, é importante a captura de todos os campos do cabeçalho e sua utilização no conjunto de dados. E para aumentar a precisão da detecção, dados oriundos de outras camadas podem ser utilizados.

Porém, nas avaliações realizadas no cenário em que foi empregado a emenda IEEE 802.11w, bons resultados foram obtidos, principalmente em função do campo *duration*, que auxiliou a identificação dos ataques.

A continuação desta pesquisa, com trabalhos futuros, pode ser realizada através de:

- inserir novas categorias de ataques com finalidade de gerar outros perfis de tráfego anômalo;
- comparar avaliações com outras metodologias de detecção de intrusos;
- verificar campos de outras camadas (aplicação, transporte, rede e física) de rede que podem ser representativas no cenário de uma rede sem fio; e

- criação e análise de repositórios para avaliação de algoritmos de detecção de intrusão para outros tipos de redes, como de telefonia móvel.

REFERÊNCIAS

AHMAD, M. S.; TADAKAMADLA, S. Short paper: security evaluation of IEEE 802.11 w specification. In: THE ACM CONFERENCE ON WIRELESS NETWORK SECURITY, 4., 2011, Hamburgo. **Proceedings ...** New York: ACM, 2011. p. 53-58.

ARAÚJO, N. S. V.; SHINODA, A. A.; OLIVEIRA, R. de; FERREIRA, E. T.; NASCIMENTO, V. E. 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, 18., 2013, Brasília. **Anais...** Brasília: SBRC, 2013. p. 119-130.

BAWISKAR, A.; MESHRAM, B. B. Survey of attacks on wireless network**. International Journal of Innovative Research in Computer and Communication Engineering,** Mumbai, v. 1, p. 90-100, 2013.

BELLARDO, J; SAVAGE, S. IEEE 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In: CONFERENCE ON USENIX SECURITY SYMPOSIUM, 12., 2003, Washington. **Proceedings...** Washington: Usenix, 2003. p. 15-28.

BITTAU, A; HANDLEY, M; LACKEY, J. The final nail in WEP's. In: IEEE SYMPOSIUM ON SECURITY AND PRYVACY, 2006, Berkeley. **Proceedings…** Piscataway: IEEE, 2006. p. 386-400.

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.

FENG, P. Wireless LAN security issues and solutions. In: IEEE SIMPOSIUM ON ROBOTICS AND APPLICATIONS- ISRA, 2012, Kuala Lumpur. **Proceedings…** Kuala Lumpur: IEEE, 2012. p. 921-924. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6219343>. Acesso em: 22 dez. 2014.

FERREIRA, E. T; CARRIJO, G. A; OLIVEIRA, R. de; DE SOUZA, N. V . Intrusion detection system with wavelet and neural artifical network approach for networks computers. **Latin America Transactions, IEEE (Revista IEEE America Latina)**, São Paulo, v. 9, n. 5, p. 832-837, 2011.

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, 1997.

FRIEDMAN, N; GEIGER, D; GOLDSZMIDT, M. Bayesian network classifiers. **Machine Learning**, Netherlands. v. 29, n. 2-3, p. 131-163, 1997.

GAST, M. **IEEE 802.11 wireless networks:** the definitive guide. Sebastopol: O'Reilly Midia, 2005.672 p.

GILL, R. S. **Intrusion detection techniques in wireless local area networks**. 2009. 264 f. Thesi (Doctor of Philosophy)– Faculty de Information Technology, Queensland university of technology, Queesnland, 2009.

HALL, M.; FRANK, E.; HOLMES, E.; PFAHRINGER, B.; REUTMAANN, P.; WITTEN, I. H. The WEKA datamining software: na update. **ACM SIGKDD Explorations Newsletter**, New York, v. 11, n. 1, p. 10-18, 2009.

HE, C.; MITCHELL, J.C. Security analysis and improvements for IEEE 802.11i. In: PROCEEDINGS OF THE ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM- NDSS, 12., 2005, New York. **Proceedings…** New York: IEEE, 2005. p. 90–110.

HEINEN, M. R.; OSÓRIO, F. S. Autenticação de assinaturas utilizando algoritmos de aprendizado de maquina. In: CONGRESSO DA SOCIEDADE BRASILEIRA DA COMPUTAÇÃO, 25., 2005, São Leopoldo. **Anais…** São Leopoldo: Unisinos, 2005. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/enia/2005/053.pdf>. Acesso em: 23 dez. 2014.

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. (Specification, 1999).

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.

INSTITUTE OF ELETRICAL AND ELETRONICS ENGINEERS – IEEE. **Std IEEE 802.11i™ – 2004**: wireless LAN medium access control (MAC) and physical layer (PHY): medium access control (MAC) security enhancements. Piscataway: IEEE, 2004. 175 p.

INSTITUTE OF ELETRICAL AND ELETRONICS ENGINEERS – IEEE. **IEEE Std IEEE 802.11w™ – 2009**: wireless LAN medium access control (MAC) and physical layer (PHY): Protected Management Frames. Piscataway: IEEE, 2009. 91 p.

KATZ, F. H. WPA vs. WPA2: Is WPA2 really an Improvement on WPA? In: COMPUTER SECURITY CONFERENCE- CSC, 4., 2010, Coastal Carolina. **Annual...** Coastal Carolina: University, 2010. Disponível em: <http://infotech.armstrong.edu/katz/katz/Frank_Katz_CSC2010.pdf>. Acesso em: 23 dez. 2014.

KOHAVI, R**.** A study of cross-validation and bootstrap for accuracy estimation and model selection. In: INTERNETIONAL JOINT CONFERENCE ON ARTIFICIAL

INTELLIGENCE- IJCAI, 2., 1995, Stanford. **Conference…** Stanford: [s.n.],1995. p. 1137-1145.Disponível em: <http://www.cs.iastate.edu/~jtian/cs573/Papers/Kohavi-IJCAI-95.pdf>. Acesso em: 23 dez. 2014.

LAMPING, U.; SHARPE, R.; WARNICKE, E. Wireshark user's guide. **Interface**, Chicago, v. 4, p. 6, 2004.

LI, W.; JOSHI, A.; FININ, T. Cast: context-aware security and trust framework for mobile ad-hoc networks using policies. **Distributed and Parallel Databases**, New York. v. 31, n. 2, p. 353-376, 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 802.11 w.** Recife: UFPE, 2012. Disponível em: <http://www.cin.ufpe.br/~pasg/gpublications/LiGo06.pdf>. Acesso em: 23 dez. 2014.

LIPPMANN, R. Pattern classification using neural networks. **IEEE communication Magazine**, Piscataway, v. 27, n. 11, p. 47-62, 1989.

MAFRA, P. M.; FRAGA, J. S.; MOLL, V.; SANTIN, A. POLVO-IIDS, um sistema de detecção de intrusão inteligente baseado em anomalias. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 8., 2008, Curitiba. **Anais…**Curitiba: UFP, 2008. p. 201-214, 2008.

MOHANABHARATHI, R.; KALAIKUMARAN, M. T.; KARTHI, S. Feature selection for wireless intrusion detection system using filter and wrapper model. **International Journal of Modern Engineering Research (IJMER)**, Warszawa, v. 2, n. 4, p. 1552-1556, 2012. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=6BC676B8AC8BFC7D05DE277838BD0B0C?doi=10.1.1.416.9367&rep=rep1&type=pdf>.Acesso em: 22 dez. 2014

NASR, K.; EL KALAM, A. A.; FRABOUL, C. Generating representative attack test cases for evaluating and testing wireless intrusion detection systems. **International Journal of Network Security & Its Applications (IJNSA)**, Australia, v. 4, n. 3, p. 1-19, 2012. Disponível em: <http://airccse.org/journal/nsa/0512nsa01.pdf>. Acesso em: 23 dez. 2014.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. **Establishing wireless robust security networks:** a guide to IEEE 802.11i. Gaithersburg: [s.n.], 2007.

ORR, M, J, L. **Introduction to radial basis function networks**. Edinburg:[s.n.], 1996. Disponível em: <http://www.cc.gatech.edu/~isbell/tutorials/rbf-intro.pdf>. Acesso em: 22 dez. 2014.

PARK, Y. **A statistical process control approach for network intrusion detection.** 2005. 128 f. Thesi (Doctor of Philosophy)– School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, 2005.

PELECHRINIS, K.; ILIOFOTOU, M.; KRISHNAMURTHY, S. V. Denial of service attacks in wireless networks: the case of jammers. **Communications Surveys &Tutorials, IEEE**, Riverside, v. 13, n. 2, p. 245-257, 2011.

PEREIRA, C. M. **Segurança em redes de comunicações de área local não-cabladas IEEE IEEE 802.11.** 2005. 242 f. Dissertação (Mestrado)– Universidade de Aveiro, Aveiro, 2005. Disponível em: <http://ria.ua.pt/bitstream/10773/1994/1/2009000696.pdf>. Acesso em: 23 dez. 2014.

PLÓSZ, S.; FARSHAD, A.; TAUBER, M.; LESJAK, C.; RUPRECHTER, T.; PEREIRA, N. Security vulnerabilities and risks in industrial usage of wireless communication. In: IEEE INTERNATIONAL CONFERENCE ON EMERGING TECHNOLOGY AND FACTORY AUTOMATION, 19., 2014, Barcelona. **Proceedings …** Barcelona: IEEE, 2014. Disponível em: <http://www.researchgate.net/publication/264436422_SECURITY_VULNERABILITIES_AND_RISKS_IN_INDUSTRIAL_USAGE_OF_WIRELESS_COMMUNICATION >. Acesso em: 23 dez. 2014.

RAJU, P. N. **State-of-the-art intrusion detection:** technology, challenges, and valuation. 2005. 85 f. Dissertation (Mestrado em Information Theory Division)- Dept of Electrical Engineering, Linköping University, Linköping, 2005.

RUBINSTEIN, M. G.; REZENDE, J. F. Qualidade de serviço em redes IEEE 802.11. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 20., 2002, Búzios. **Anais…** Rio de Janeiro: UFRJ, 2002.

RUCK, D.; ROGERS, S.; KABRISKY, M. Feature selection using a multilayer perceptron. **Journal of Neural NetworkComputing,** Warren, v. 2, p. 40–48, 1990. Disponível em: <http://www.researchgate.net/publication/2430790_Feature_Selection_Using_a_Multilayer_Perceptron>. Acesso em: 23 dez. 2014.

SAKIB, A. K. M. N.; AHMED, S; RAHMAN, S.; MAHMUD, I.; BELALI, H. WPA 2 (Wi-Fi Protected Access 2) Security enhancement: analysis and improvement. **Global Journal of Computer Science and Technology**, Daka, v. 12, n. 6, 2012.

SANDSTRÖM, H. **A survey of the denial of service problem**. Luleå: Department of Computer Science and Electrical Engineering, Luleå University of Technology, 2001. Disponível em: <http://www.sm.luth.se/gradschool/pdf/Papers/p03.pdf >. Acesso em: 23 dez. 2014.

SHIRAVI, A.; SHIRAVI, H.; TAVALLAEE, M. GHORBANI, A. A. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. **Computers & Security**, New Brunswick, Canada, v. 31, n. 3, p. 357-374, 2012.

SINGH, S. K.; SINGH, M. P.; SINGH, D. K.A survey on network security and attack defense mechanism for wireless sensor networks. **International Journal of Computer Trends and**

Technology, India, p. 1-9. 2011. Disponível em: <http://ijcttjournal.org/Volume1/issue-2/ijcttjournal-v1i2p2.pdf>. Acesso em: 23 dez. 2014.

SOBH, T. S. Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. **Computer Standards & Interfaces**, Cairo, v. 28, n. 6,p. 670-694, 2006.

SOMMER, R.; PAXSON, V. Out side the closed world: on using machine learning for network intrusion detection. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP), 2010, Berkeley. **Symposium...** Berkeley: IEEE, 2010. p. 305-316.

SOUZA, E. P.; MONTEIRO, J. A. S. Estudo sobre sistema de detecção de intrusão por anomalias, uma abordagem utilizando redes neurais. In: WORKSHOP DE GERÊNCIA E OPERAÇÃO DE REDES E SERVIÇOS-WGRS, 14., 2009, Recife. **Anais...** Recife: Sociedade Brasileira de Redes de Computadores – SBRC, 2009. p. 84-97. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/wgrs/2009/007.pdf>. Acesso em: 23 dez. 2014.

SPAFFORD, E. H.; ZAMBONI, D. Intrusion detection using autonomous agents. **Computer Networks**, Amsterdam, v. 34, n. 4, p. 547-570, 2000.

SPERTI, L.; MOLLO, M. J.; FROSALI, F.; FREGUGLIA, G. **Method and system for detecting attacks in wireless data communications networks**.U.S. Patent n. 8, 369, 830, 5 fev. 2013.

TANENBAUM, A. **Rede de computadores.** 5. ed. São Paulo: Pearson Education,2011.

TEWS, E. **Attacks on the wep protocol**. Alemanha: IACR cryptology e print archive, 2007. p. 471, 2007. Disponível em: <http://eprint.iacr.org/2007/471.pdf>. Acesso em: 22 dez. 2014.

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, p. 1-35, 2010.

APÊNDICE A - ARTIGOS PUBLICADOS E ACEITOS RELACIONADOS AO PRESENTE TRABALHO

VILELA, D. W. F. L et al. Construção de bases 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- ENACOMP**,** 10., 2013, Goiás. **Encontro...** Goiás: [s.n.], 2013. PUBLICADO.

VILELA, D. W. F. L; FERREIRA, E. T.; SHINODA, A. A.; ARAÚJO, N. construção de uma base de dados para auxiliar a avaliação de sistemas de detecção de intrusos com criptografia IEEE 802.11i e IEEE 802.11w habilitada. In: JORNADA DE PESQUISA E EXTENSÃO DO IFMT, 2013, Mato Grosso. **Jornada....** Mato Grosso: [s.n.], 2013. PUBLICADO.

FERREIRA, E. T.; SHINODA, A. A.; ARAÚJO, N. V. S.; NASCIMENTO, V. E; VILELA, D. W. Construção e uso de base de dados sobre o funcionamento de uma rede sem fio para contribuir no ensino nos cursos de computação e engenharia**.** In: CONGRESSO BRASILEIRO DE EDUCAÇÃO EM ENGENHARIA- COBENGE, 41., 2013, Rio Grande do Sul. **Congresso...** Rio Grande do Sul: [s.n.], 2013. PUBLICADO.

VILELA, D. W. F. L.; FERREIRA, E. T.; SHINODA, A. A.; ARAÚJO, N. Construção de uma base de dados para auxiliar a avaliação de sistemas de detecção de intrusos com criptografia IEEE 802.11i e IEEE 802.11 w habilitada. In; WORKSHOP DE PESQUISA E INOVAÇÃO DO IFMT, 2., 2013, Mato Grosso. **Workshop…** Mato Grosso: [s.n.], 2013. PUBLICADO.

VILELA, D. W. F. L. et al. A dataset for evaluating intrusion detection systems in IEEE 802.11 wireless networks. In: IEEE COLOMBIAN CONFERENCE ON COMMUNICATIONS AND COMPUTING- COLCOM**,** 2014**. Conference…** Colombia: IEEE, 2014. p. 1-5. PUBLICADO.