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

DOUGLAS WILLER FERRARI LUZ VILELA

DESENVOLVIMENTO DE IDS BASEADO NO MODELO DE RNA ARTMAP *FUZZY* COMO FERRAMENTA DE SEGURANÇA EM REDES *WI-FI*

Ilha Solteira
2021

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

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

DOUGLAS WILLER FERRARI LUZ VILELA

DESENVOLVIMENTO DE IDS BASEADO NO MODELO DE RNA ARTMAP *FUZZY* COMO FERRAMENTA DE SEGURANÇA EM REDES *WI-FI*

Tese apresentada à Faculdade de Engenharia de Ilha Solteira – UNESP como parte dos requisitos para obtenção do título de Doutor em Engenharia Elétrica.
Área de Conhecimento: Automação.

Orientadora: Anna Diva Plasencia Lotufo

Ilha Solteira

2021

FICHA CATALOGRÁFICA
Desenvolvido pelo Serviço Técnico de Biblioteca e Documentação

Vilela, Douglas Willer Ferrari Luz.
V699d Desenvolvimento de IDS baseado no modelo de RNA ARTMAP Fuzzy como ferramenta de segurança em redes wi-fi / Douglas Willer Ferrari Luz Vilela. -- Ilha Solteira: [s.n.], 2021
67 f. : il.

Tese (doutorado) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de conhecimento: Automação, 2021

Orientador: Anna Diva Plasencia Lotufo
Inclui bibliografia

1. Sistema de detecção de intrusão. 2. Redes sem fio IEEE 802.11. 3. Rede Neural ARTMAP Fuzzy. 4. Cibersegurança. 5. Conjunto de dados. 6. Classificação de padrões.

João Josué Barbosa
Serviço Técnico de Biblioteca e Documentação
Diretor Técnico
CRB 8-5642

unesp

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de Ilha Solteira

CERTIFICADO DE APROVAÇÃO

TÍTULO DA TESE: Desenvolvimento de IDS baseado no modelo de RNA ARTMAP Fuzzy como ferramenta de segurança em redes Wi-Fi.

AUTOR: DOUGLAS WILLER FERRARI LUZ VILELA
ORIENTADORA: ANNA DIVA PLASENCIA LOTUFO

Aprovado como parte das exigências para obtenção do Título de Doutor em ENGENHARIA ELÉTRICA, área: Automação pela Comissão Examinadora:

Profª. Drª. ANNA DIVA PLASENCIA LOTUFO (Participaçao Virtual)
Departamento de Engenharia Elétrica / Faculdade de Engenharia de Ilha Solteira - UNESP

Prof. Dr. CARLOS ROBERTO DOS SANTOS JÚNIOR (Participaçao Virtual)
Campus de Hortolândia / Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP

Profª. Drª. MARA LUCIA MARTINS LOPES (Participaçao Virtual)
Departamento de Matemática / Faculdade de Engenharia de Ilha Solteira - UNESP

Prof. Dr. BENEDITO ISAIAS LIMA FULY (Participaçao Virtual)
Instituto de Engenharia de Sistemas e Tecnologias da Informação / Universidade Federal de Itajubá - UNIFEI

Prof. Dr. GELSON DA CRUZ JUNIOR (Participaçao Virtual)
Escola de Engenharia Elétrica e de Computação / Universidade Federal de Goias - UFG

Ilha Solteira, 27 de julho de 2021

DEDICATÓRIA

A Deus

A minha mãe Loraine e minha irmã Luiza

A minha esposa Isabela e meus filhos Maria Fernanda e Davi

AGRADECIMENTOS

Agradeço à minha família, pela compreensão e apoio durante os 04 anos de doutoramento. Foram momentos difíceis, as vezes longe fisicamente, mas não de coração;

À minha esposa Isabela, pela paciência, carinho, amor e incentivo durante essa trajetória. Aos meus filhos Maria Fernanda e Davi, por serem fonte de inspiração para esta jornada acadêmica.

À professora Anna Diva por me aceitar como orientando de doutorado e integrante do grupo de pesquisa SINTEL. Sou muito grato pela amizade, ensinamentos, compreensão, respeito e confiança depositada em meu trabalho.

Aos professores membros do Laboratório SINTEL: Prof. Dr. Carlos Roberto Minussi e Profa. Dra. Mara Lopes.

Aos colegas do laboratório SINTEL, e em especial ao amigos Carlos Roberto dos Santos Júnior e Thays Abreu.

Ao meu amigo Prof. Dr. Lucas Ramalho pelas dicas, companheirismo, conselhos e por me ajudar sempre que possível.

À minha amiga Cássia Correa pela companhia nas viagem de Cuiabá a Ilha Solteira e parceria nas disciplinas.

Agradeço a todos amigos de Cuiabá e Ilha Solteira que diretamente ou indiretamente contribuíram com meu aprendizado durante a elaboração desta Tese de Doutorado.

Ao IFMT pela concessão do meu afastamento para o desenvolvimento de meus trabalhos, em especial a professora Suzana e professor Deiver Teixeira, dos quais sempre tive total apoio nesta empreitada.

Especiais agradecimentos à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

“Tudo posso naquele que me fortalece”

(Filipenses 4:13)

RESUMO

As redes de comunicação sem fio IEEE 802.11 possuem diversas vulnerabilidades, e os ataques de negação de serviço são considerados uma das suas principais ameaças. A primícias básica do ataque de negação de serviço pauta-se pela indisponibilidade dos recursos e serviços da rede. A maioria das técnicas aplicadas no ataque de negação de serviço em redes sem fio exploram a falta de proteção dos quadros de gerenciamento e controle do quadro MAC do IEEE 802.11. Garantir a segurança absoluta de um ambiente de rede sem fio não é possível, porém pode-se adicionar camadas extras de proteção para redução do risco de incidentes de segurança. Os sistemas de detecção de intrusão (IDS, do inglês *Intrusion Detection System*) são ferramentas utilizadas no monitoramento do tráfego da rede e identificação de eventos anômalos. No entanto, um dos grandes gargalos dos sistemas de detecção de intrusão é encontrar conjuntos de dados públicos que caracterizem o funcionamento normal e anômalo de uma rede sem fio. Com objetivo de mitigar as vulnerabilidades das redes sem fio e sanar o problema de caracterização do comportamento da rede, foi desenvolvido nesta pesquisa um algoritmo de detecção de intrusão baseado no modelo de rede neural artificial ARTMAP *Fuzzy*. O trabalho foi realizado em quatro etapas: seleção da rede sem fio IEEE 802.11; avaliação da rede IEEE 802.11; construção, padronização e pré-processamento do conjunto de dados; e resultados gerados pelo algoritmo de detecção de intrusão. Os resultados obtidos demostram que o IDS possui alta capacidade de detecção de intrusão em redes sem fio e utiliza poucos recursos computacionais para processar os dados. A taxa média de detecção foi de 98,9% e a taxa de falso positivo foi menor que 1,2%. A seleção de um cenário de rede sem fio real e com características heterogêneas, foi fundamental para construção de um conjunto de dados com atributos representativos do comportamento normal e criação de assinaturas anômalas. A rede neural ARTMAP *Fuzzy* confirmou a eficiência do IDS, atestando as características da estabilidade e plasticidade.

Palavras-chave: segurança da informação; redes sem fio; sistema de detecção de intrusão; rede neural artificial. ARTMAP *fuzzy;* aprendizagem de máquina.

ABSTRACT

IEEE 802.11 wireless communication networks have several vulnerabilities, and the attacks called denial of service are the principal threat. The bases of this kind of attack are the unavailability of the resources and network services. Most of the techniques applied to the denial of service in wireless networks explore the lack of protection in management and control of IEEE 802.11 MAC. Absolute security in wireless environment is difficult to assure, however extra protection layers can be added to reduce the risk of security incidents. The IDS (Intrusion Detection System) contains tools that monitor the traffic in the network and identify anomalous events. Nonetheless, the great difficulty of the IDS is to find public dataset that characterize the normal and anomalous operation of wireless network. To mitigate the vulnerabilities of the wireless network and solve the problem of characterizing the network behavior, this research develops an algorithm of intrusion detection based on Fuzzy ARTMAP Artificial Neural Network. Results show that the IDS has high capacity of detecting intrusions in wireless networks with few computational resources to process the data. The medium detection rate is 98.9% and false positive rate is less than 1.2%. The selection of a wireless scenery with heterogeneity characteristic is fundamental to build a dataset with representative attributes of normal and anomalous behavior. The Fuzzy ARTMAP neural network confirms the efficiency of IDS proving its proprieties of stability and plasticity.

Key words: information security; wireless network; intrusion detection system; artificial neural network; *fuzzy* ARTMAP; machine learning.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

AES	*Advanced Encryption Standard*
AP	*Access Point* (Ponto de Acesso)
ART	*Adaptive Resonance Theory* (Teoria da Ressonância Adaptativa)
AS	*Source Address*
AUC	*Area Under The Curve*
CCMP	*CCM Mode Protocol*
CRC	*Cyclic Redundancy Check*
CTS	*Clear to Send*
DA	*Destination Address*
DL	*Deep Learning*
DOS	*Denial of Service*
DS	*Distribution System* (Sistema de Distribuição)
EAP	*Extensible Authentication Protocol*
ESS	*Extended Service Set*
FCS	*Frame Check Sequence*
GTK	*Group Temporal Key*
IBSS	*Independent Basic Service Set*
IDS	*Intrusion Detection Systems* (Sistema de Detecção de Intrusão)
IEEE	*Institute of Electrical and Electronic Engineers*
IGTK	*Integrity Group Temporal Key*
IOT	*Internet of Things* (Internet das Coisas)
IV	*Initialization Vector* (Vetor de Inicialização)
KNN	*K-Nearest Neighbor*
KRACK	*Key Reinstallation Attacks*
LLC	*Logical Link Control*
MAC	*Media Access Control* (Controle de Acesso ao Meio)
MIC	*Message Integrity Code*
ML	*Machine Learning* (Aprendizagem de Máquina)
NIST	*National Institute of Standards and Technology*
PCA	*Principal Component Analysis*
PMK	*Pairwise Master Key*
PSO	*Particle Swarm Optimization*

PTK	*Pairwise Transit Key*
RA	*Receiver Address*
RC4	*Ron Rivest 4*
RF	*Radio Frequency* (Radio Frequência)
RNA	Rede Neural Artificial
ROC	*Receiver Operating Characteristic*
RSN	*Robust Secure Network*
RSNA	*Robust Security Network Associations*
RTS	*Request to Send*
SSID	*Service Set Identifier*
TA	*Transmitter Address*
TIC	Tecnologia da Informação e Comunicação
TKIP	*Temporal Key Integrity Protocol*
WCAN	*Wireless Campus Area Network*
WEP	*Wired Equivalent Privacy*
WI-FI	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WPA	*WLAN Protected Access*

SUMÁRIO

1 INTRODUÇÃO

A evolução das Tecnologias da Informação e Comunicação (TIC) são fundamentais para o desenvolvimento tecnológico na área acadêmica, científica, industrial, social e corporativa (MOORE, 1965). A *Internet* das Coisas (IOT, do inglês *Internet of Things*) é uma das tecnologias emergentes que contribuem para ascensão de novos paradigmas, principalmente no âmbito das redes de comunicação. A primícia básica de um sistema IOT é prover a infraestrutura de rede com protocolos de comunicação interoperáveis que possibilitem conectar diferentes dispositivos e/ou objetos inteligentes, com a *internet* (AAZAM *et al.*, 2016). Em 2019, a Universidade de *Stanford* e a Empresa de segurança *Avast* realizaram um estudo que prospectou a existência de aproximadamente 50 bilhões de dispositivos inteligentes conectados à *internet* (KUMAR *et al*., 2019). O aumento exponencial das redes de comunicação compostas por dispositivos inteligentes é um agravante no âmbito da cibersegurança. Garantir os princípios básicos da segurança da informação (disponibilidade, integridade e confidencialidade) tornou-se um grande desafio para os administradores de rede (Jing *et al.*, 2014).

Neste cenário, as redes sem fio, em especial as advindas do padrão IEEE 802.11 são muito utilizadas em ecossistemas IOT (ČOLAKOVIĆ; HADŽIALIĆ, 2018). Segundo os pesquisadores Pahlavan e Krishnamurthy (2021), as primeiras redes locais sem fio (WLAN, do inglês *Wireless Local Area Network*) (surgiram no mercado na década de 1990, logo após a inserção da *internet* nas residências. A redução do preço dos equipamentos utilizados nas redes sem fio e o aporte de bilhões de dólares investidos na tecnologia, foram fundamentais para a popularização da tecnologia nos anos 2000 (PAHLAVAN; KRISHNAMURTHY, 2021). Desde a homologação da primeira especificação (IEEE, 1999), as WLANs são amplamente difundidas. Porém, existe a preocupação com os mecanismos de segurança empregados pelo padrão IEEE 802.11, devido a diversas vulnerabilidades apresentadas desde a sua homologação. As especificações dos mecanismos de segurança das redes sem fio IEEE 802.11 evoluíram, assim como a tecnologia. No entanto, algumas de suas principais vulnerabilidades permanecem até a atualidade.

O primeiro protocolo de segurança apresentado foi o *Wired Equivalent Privacy* (WEP), este provou ser ineficaz, principalmente pelas fragilidades do seu algoritmo criptográfico *Ron´s Code 4* (RC4). No ano de 2003 foi apresentado um novo protocolo

de segurança chamado *Wi-Fi Protected Access* (WPA), sendo substituído no ano seguinte pelo WPA2 ou também conhecido como padrão IEEE 802.11i. As principais características do WPA2 incidem sobre a autenticação e criptografia, buscando garantir em especial a confidencialidade, autenticidade e integridade dos dados em uma WLAN. Para isto, foram empregados o algoritmo criptográfico *Advanced Encryption Standard* (AES) e o conceito de Rede de Segurança Robusta (RSN, do inglês *Robust Security Network*). Outra modificação é a implementação do protocolo do IEEE 802.1x (IEEE, 2001), utilizado para realizar o controle de acesso. Apesar das novas funcionalidades de segurança inseridas pelo protocolo WPA2, as melhorias concentraram-se apenas nos quadros de dados presentes no protocolo de controle de acesso ao meio (MAC, do inglês *Medium Access Control*). Desta forma, os quadros de gerenciamento e controle que também compõem o protocolo MAC permaneceram sem nenhuma proteção. A ausência de mecanismos de proteção para esses quadros possibilita suscetíveis a ataques inoculados na camada MAC de uma WLAN. Em 2009 foi homologado o padrão IEEE 802.11w, esta nova especificação assegura a proteção de alguns quadros de gerenciamento e controle. Esforços foram realizados para melhorar os mecanismos de segurança do padrão IEEE 802.11, porém este tipo de rede ainda é permissível a alguns tipos de ataques, em especial os que afetam a disponibilidade da rede.

O ataque de negação de serviço (DoS, do inglês *Denial of Service*) é uma das principais ameaças as segurança das redes IEEE 802.11, pois exploram justamente a falta de proteção dos quadros de gerenciamento e controle do protocolo MAC (BICAKCI; TAVLI, 2009). Para mitigar incidentes de segurança em WLANs é necessário empregar controles de proteção extra, essas ferramentas funcionarão em consonância com os mecanismos de segurança já existentes no protocolo IEEE 802.11. Sistemas de Detecção de Intrusão (IDS, do inglês *Intrusion Detection Systems*) são ferramentas muito utilizadas por administradores de rede no monitoramento e identificação de eventos anômalos em ambientes de rede. Porém, monitorar uma rede sem fio é uma tarefa complexa, visto que não existem limitadores físicos. A transmissão é realizada através de rádio frequência (RF). O processo de seleção de um IDS que seja funcional para uma rede WLAN precisa levar em consideração a precisão, eficiência e capacidade de processamento do IDS. Muitas soluções de IDS comercializadas não possuem uma caracterização específica para detecção de anomalias em redes sem fio (CHAKRABARTI; CHAKRABORTY;

MUKHOPADHYAY, 2010). Por outro lado, pesquisadores tem explorado o uso de técnicas de aprendizagem de máquina, redes neurais artificiais, algoritmos genéticos e aprendizagem profunda (DL, do inglês *Deep Learning*) para desenvolver sistemas de detecção de intrusão mais precisos e eficazes.

Para superar os principais problemas de segurança encontrados nas redes sem fio, foi desenvolvido nesta tese um algoritmo de identificação e classificação de atividades normais e anômalos. A ferramenta desenvolvida monitora especificamente o comportamentos dos campos presentes no quadro MAC IEEE 802.11 e atua em consonância com os mecanismos de segurança habilitados. O método de detecção adotado é baseado em um modelo híbrido, pois realizou a combinação do método de detecção por assinatura e anomalia. Apesar de muitas técnicas de aprendizagem de máquina conseguirem reduzir as altas taxas de falsos positivos e aumentar a precisão dos modelos de detecção por anomalia, ainda possuem dificuldade em lidar com grandes conjuntos de dados.

O algoritmo de aprendizagem de máquina utilizado na pesquisa baseou-se no modelo de Rede Neural Artificial ARTMAP *Fuzzy*. A escolha do algoritmo deu-se principalmente por sua resposta ao problema da estabilidade (capacidade de manter o conhecimento prévio devido aos ajustes de peso) e plasticidade (capacidade de se adaptar e criar novos padrões sem perda de conhecimento prévio) (CARPENTER *et al.*, 1992). As características da RNA ARTMAP *Fuzzy*, foram essenciais para validar o algoritmo desenvolvido, e também sanar problemas comuns em IDS como, tempo de aprendizado e classificação eficaz de grandes conjuntos de dados. O conjunto de dados utilizado na avaliação da eficiência e precisão do IDS foi gerado em uma rede sem fio real e em funcionamento em uma instituição de ensino. Os dados foram obtidos através do monitoramento de todo tráfego transmitido na rede durante um período de sete (07) dias e posteriormente pré-processados e padronizados. As métricas de avaliação foram dadas pela matriz de confusão.

1.1 OBJETIVOS E CONTRIBUIÇÕES

Esta tese de doutorado tem por objetivo e contribuições:

- Desenvolver um algoritmo de detecção de intrusão para redes sem fio IEEE 802.11 baseado na rede neural artificial ARTMAP *Fuzzy*;

- Selecionar um cenário de rede sem fio IEEE 802.11 real e com grande fluxo de dados;
- Realizar uma análise preditiva do fluxo de dados trafegado na rede sem fio escolhida para dimensionar o conjunto de dados de treinamento e teste aplicado na pesquisa;
- Reestruturar o conjunto de dados utilizado como base de conhecimento no aprendizado e teste do IDS ARTMAP *Fuzzy*. Pré-processar e padronizar os dados em consonância com a variação do tráfego analisado no período de 2019;
- Apresentar os resultados do IDS ARTMAP *Fuzzy*, para assim, validar a eficiência e precisão do algoritmo de classificação desenvolvido; e
- Contribuir com o desenvolvimento de uma ferramenta de segurança para redes sem fio, com a perspectiva de mitigar ameaças que exploram vulnerabilidades presentes nos quadros de gerenciamento e controle do protocolo IEEE 802.11.

1.2 ORGANIZAÇÃO DO TEXTO

Esta tese de doutorado está organizada em sete capítulos como segue:

- **Capítulo 1:** Introdução, objetivos, contribuições e organização do texto;
- **Capítulo 2:** Revisão bibliográfica de artigos relevantes para abordagem de IDS para redes sem fio;
- **Capítulo 3:** Fundamentação teórica sobre o padrão IEEE 802.11, protocolos de segurança, ameaças existentes e ferramenta de segurança para redes sem fio IEEE 802.11;
- **Capítulo 4:** Embasamento teórico sobre o modelo de aprendizagem de máquina baseado na família ART, concentrando-se na RNA ARTMAP *Fuzzy*;
- **Capítulo 5:** Descrição do cenário de rede utilizado na pesquisa, metodologia de seleção da rede sem fio escolhida, avaliação da rede sem fio selecionada, construção e estruturação do conjunto de dados utilizado pelo IDS e avaliação do algoritmo de detecção de intrusão

para redes sem fio baseado no modelo de rede neural artificial ARTMAP *Fuzzy*;

- **Capítulo 6:** Conclusão e sugestões para trabalhos futuros; e
- **Capítulo 7:** Referências bibliográficas.

2 TRABALHOS RELACIONADOS

Sistemas de detecção de intrusão são amplamente utilizados em muitas organizações para identificação de ataques em redes. Um IDS eficiente e preciso deve possuir uma capacidade de detecção elevada, assegurar que os alertas emitidos correspondam à atividade sinalizada, velocidade na emissão de alertas e baixo custo computacional.

A pesquisa desenvolvida por Tama e Rhee (2016) utilizou o modelo de aprendizagem de máquina *Rotation Forest* como Sistema de Detecção de Intrusão para redes sem fio. No treinamento e teste do IDS foi utilizada a base de dados GPRS (VILELA *et al*., 2014), e como métrica para avaliação foi empregado o cálculo da derivada da curva Característica de Operação do Receptor (ROC, do inglês *Receiver Operating Characteristic*) denominada de área sob a curva (AUC, do Inglês *Area Under the Curve*). O conjunto GPRS foi subdividido em dois, o primeiro é baseado em uma topologia de rede com modo de operação infraestruturado e com o protocolo de segurança WEP/WPA habilitado. O segundo, também é baseado em uma rede com modo de operação infraestruturado e protocolo de segurança WPA2 habilitado. O método de análise de componentes principais (PCA, do inglês *Principal Component Analysis*) foi utilizado para pré-processar os conjuntos de dados e extrair atributos significativos. O conjunto de dados que antes possuía cinco classificações, foi reestruturado para apenas duas classificações (normal e anômala). Em resultados preliminares, o IDS apresentou baixa eficiência. Ao associar o algoritmo *Rotation Forest* com o algoritmo *Decision Tree* (Árvore de Decisão) o classificador de detecção de intrusão apresentou desempenho satisfatórios em relação ao conjunto de dados WEP/WPA e WPA2.

No trabalho desenvolvido por Araújo *et al.* (2013) a RNA ARTMAP *Fuzzy* foi utilizada como IDS. O desempenho do classificador foi avaliado por meio das métricas dada pela matriz de confusão e coeficiente *Kappa*. O *Kappa* foi utilizado para medir a proporção de concordância observada entre as classes de comportamento existentes (classe real) e as preditas (classe prevista). O conjunto de dados utilizado na avaliação foi o KDD99 e aplicado o método de validação cruzada em 10 subconjuntos com 1.000 amostras cada. A ferramenta de optimização por enxame de partículas (PSO, do inglês *Particle Swarm Optimization*) foi utilizada para seleção dos parâmetros da rede neural. Embora os resultados apresentados demonstrem viabilidade de integração do

Kappa com a RNA ARTMAP *Fuzzy* para o problema de detecção de intrusão, o conjunto de dados empregado é antigo e não engloba ataques específicos para redes sem fio.

No artigo intitulado “Detecção de intrusão em redes 802.11: avaliação empírica de ameaças e um conjunto de dados público”, os pesquisadores Kolias *et al.* (2015) realizaram a construção de um conjunto de dados denominado de AWID. Posteriormente utilizaram uma série de algoritmos de aprendizagem de máquina presentes no *software Weka* para avaliar o conjunto de dados AWID. O algoritmo *J48* obteve o melhor desempenho em comparação aos outros algoritmos avaliados, sua taxa de detecção foi de (99,98%) e a taxa de alarmes falsos foi de (4,37%). Porém demonstrou-se lento durante o treinamento, o algoritmo levou 3.921,68 segundos para aprender apenas 20 instancias do conjunto de treinamento. Os algoritmos *Random Forest* e *OneR* também obtiveram desempenho satisfatório, o *Random Forest* apresentou taxa de detecção de (95,58%), taxa de alarmes falsos de (4,41%) e o tempo gasto no treinamento do algoritmo foi de aproximadamente 829 segundos. Já o algoritmo *OneR* obteve uma taxa de detecção de (94,57%), taxa de alarmes falsos de (5,42%) e aproximadamente 157 segundos no treinamento.

Os autores Agarwal *et al*.(2016) propuseram uma arquitetura de sistema de detecção de intrusão em tempo real. A proposta teve como objetivo identificar apenas o ataque de negação de serviço denominado de *PS-Poll DoS*. O quadro *PS-Poll* é responsável pelo gerenciamento do modo de economia de energia do ponto de acesso (AP, do inglês *Access Point*), e pode ser utilizado por uma estação maliciosa para que ela assuma perante ao AP a identidade de uma estação legítima. Este ataque explora a ausência de proteção nos quadros controle e só é passível de ataques pela falta de autenticação dos quadros *PS-Poll*. O modelo de IDS que foi proposto apresentou bons resultados na detecção do ataque *PS-Poll DoS*, porém a ferramenta não foi testada na detecção de outras classes de ataques. Existem outros pontos da pesquisa que também são passíveis de questionamento, como a configuração trivial do ambiente de rede definido. A rede sem fio projetada foi configurada em um ambiente de teste e com um número ínfimo de equipamentos (ativos) de rede, destoando de uma rede disposta em um cenário real. A origem das atividades anômalas foram geradas de uma única origem, isso influência diretamente no padrão de comportamento da rede. E por fim, o tempo de realização dos testes foram curtos, sendo de apenas três (03) horas.

O trabalho desenvolvido por Chudasma (2020) avaliou os algoritmos de aprendizagem de máquina *Decision Tree* (Árvore de Decisão), *K-Nearest Neighbor* (KNN), *Logistic Regression* (Regressão Logística) e *Naive Bayes* aplicados ao problema de detecção de intrusão. O trabalho utilizou como métrica de avaliação a precisão, acurácia, *recall* (sensibilidade) e F-*measure* presentes na matriz de confusão. A pesquisa dividiu-se em duas etapas: IDS baseado no modelo de detecção por anomalia e aprendizagem profunda. Os métodos de classificação *Decision Tree*, KNN, Logistic *Regression* e *Naive Bayes* foram usados para identificar os eventos anômalos, e a técnica aprendizagem profunda empregou uma abordagem baseada em RNA para classificar os ataques detectados pelo IDS. O algoritmo *Decision Tree* apresentou a acurácia de (99,49%) e precisão de (100%). O modelo KNN obteve (99,16%) de acurácia e (99,00%) de precisão. O algoritmo *Logistic Regression* apresentou a acurácia de (95,54%) e (95,00%) de precisão. O algoritmo *Naive Bayes* apresentou os piores resultados, apenas (90,67%) de acurácia e (88,00%) de precisão. Já o modelo baseado em uma RNA (96,22%) de acurácia e (97,00% de precisão). Ao comparar os resultados o algoritmo *Decision Tree* foi o que obteve melhor desempenho.

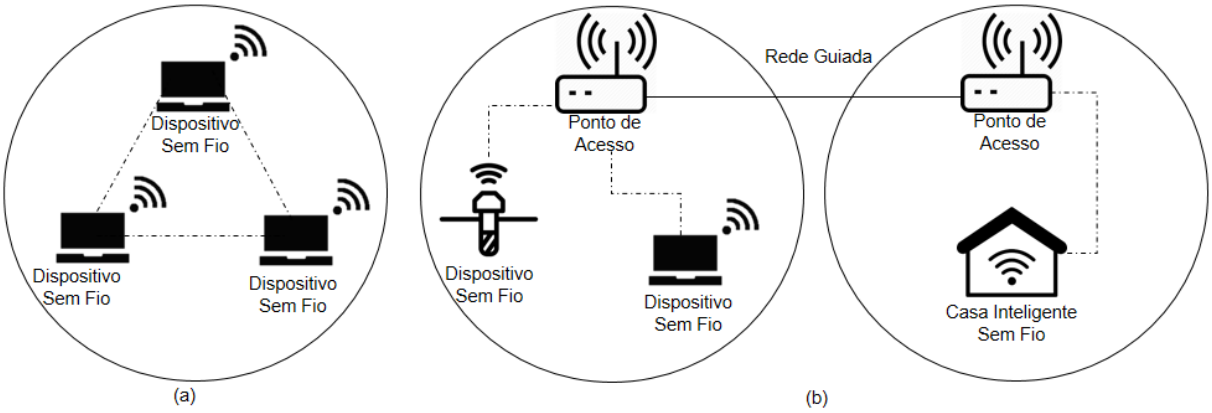
O IDS proposto nesta tese, visa identificar e classificar em especial ataques que afetam o funcionamento das redes IEEE 802.11. O IDS funcionará em consonância aos mecanismos de segurança habilitados na rede.

3 VISÃO GERAL DO PADRÃO IEEE 802.11

O padrão IEEE 802.11, também popularmente conhecido como *Wi-Fi* (*Wireless Fidelity*), estabelece a arquitetura e as especificações das redes sem fio. A topologia do padrão IEEE 802.11 possibilita interoperabilidade entre dispositivos de rede garantindo mobilidade e transparência a protocolos de camadas superiores. Em 1999, a primeira especificação de rede sem fio IEEE 802.11 foi homologada (IEEE, 1999b). Novas versões surgiram com os avanços da tecnologia, proporcionando melhorias na velocidade, segurança e outros. O padrão IEEE 802.11 suporta duas topologias: conjunto de serviço básico independente (IBSS, do inglês *Independent Basic Service Set*); e conjunto de serviço estendido (ESS, do inglês *Extended Service Set*). A rede formada por um IBSS não possui *backbone*, normalmente é composta por duas ou mais estações sem fio. O ESS, por outro lado, possui uma infraestrutura de *backbone*,

permitindo a comunicação entre estações de rede sem fio com estações de rede guiadas. A arquitetura do padrão IEEE 802.11 define duas formas de funcionamento para uma WLAN: *ad-hoc* e infraestruturado (KUROSE; ROSS, 2010), representado na Figura 01.

Figura 01 – Arquitetura *Ad-Hoc* (a) e Infraestruturado (b).



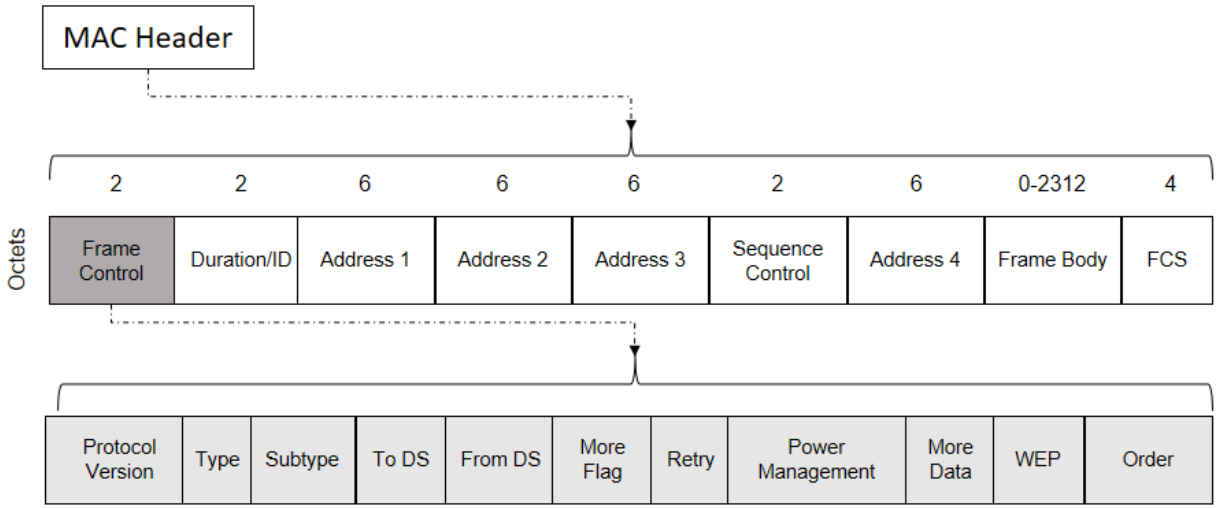
Fonte: Adaptado de Kurose e Ross (2010).

Na arquitetura de rede *ad-hoc*, a comunicação é estabelecida sem uma estrutura pré-definida, onde cada estação se comunica com outras estações, desde que estejam dentro da área de cobertura um do outro. Os nós são organizados em uma rede e cada um realiza o roteamento e transmissão dos dados para os outros nós da rede sem a presença de um AP. O modo insfraestruturado é composto por uma ou mais células de comunicação gerenciadas por pontos de acesso sem fio que controlam o tráfego de dados gerado. O AP também pode ser usado para estabelecer comunicação entre o meio sem fio e o meio guiado.

3.1 ARQUITETURA LÓGICA DO IEEE 802.11

O padrão IEEE 802.11 atua nas Camadas Física e de Enlace. A camada física é responsável pelos sinais de radiofrequência, modulação para transmissão e recepção. A camada de enlace é dividida em duas subcamadas: Controle Lógico de Enlace (LLC, do inglês *Logic Link Control*) e Controle de Acesso ao Meio (MAC, do inglês *Media Access Control*). A subcamada LLC faz interface da camada de enlace com as camadas superiores, enquanto a subcamada MAC controla o acesso ao meio compartilhado e também especifica o formato do quadro na comunicação, conforme ilustrado na Figura 02.

Figura 02 – Organização básica do quadro MAC do protocolo IEEE 802.11.



Fonte: Adaptado de IEEE (1999).

O primeiro campo é o *Frame Control* (controle de quadros), este campo possui **(2 *bytes*)**. Este campo é responsável por carregar onze subcampos como:

- *Protocol Version* (Versão do protocolo) – Informa a versão do protocolo IEEE 802.11 em uso;
- *Type* (Tipo) – Define o quadro, para cada tipo de quadro o campo recebe um valor: gerenciamento (00), controle (01), dados (10) e (11) indica que está reservado;
- *Subtype* (Subtipo) - Informa a função, se valor do campo for 0000 indica solicitação de associação, se for 1000 é um quadro de *beacon*, etc;
- *To DS* - Informa que o quadro de destino é para um sistema de distribuição (DS, do inglês *Distribution System*);
- *From DS* – Informa quando o quadro é originário de um DS;
- *More Flag* (Especificações de Fragmentação) – Informa que o quadro é acompanhado por outros fragmentos;
- *Retry* (Retransmissão) – Informa se o quadro atual é proveniente de uma retransmissão;
- *Power Manager* (Gerenciamento de Energia) – informa o estado da estação após a transmissão de um quadro. Se o campo for definido como (1), a estação entra no modo de economia de energia. Se o campo for definido como (0), a estação permanece ativa;

- *More Data* – Informa ao receptor que o remetente tem mais dados para serem enviados. Geralmente é utilizado pelo AP para indicar se uma estação que está em modo de economia de energia, e que mais pacotes serão armazenados em *buffer*;
- *WEP* – Informa qual protocolo de segurança está habilitado no padrão IEEE 802.11; e
- *Order* – Informa quais quadros recebidos devem ser processados rigorosamente na ordem.

O segundo é o campo *Duration* (Duração), este possui **(2 *bytes*)** e é responsável por informar o tempo de transmissão. Os campos seguintes são: *Address* (endereço MAC), possuem **(6 *bytes* cada)** e identificam endereço de origem (AS, do inglês *Source Address*), endereço de destino (DA, do inglês *Destination Address*), endereço do transmissor (TA, do inglês *Transmitter Address*), endereço do receptor (RA, do inglês *Receiver Address*) e o campo Identificador de BSS (BSSID, do inglês *BSS Indentifier*). O campo *Sequence Control* (Controle de Sequência) possui (**2 *bytes*)**, e suporta a retransmissão de mensagens para evitar pacotes duplicados. O Corpo do Quadro (*Frame Body*) pode possuir de **(0-2312 *bytes*)**, por isso seu tamanho é variável. Nele são armazenadas as informações recebidas das camadas superiores ou conteúdo dos quadros de gerenciamento à serem transmitidos. Finalmente, o Quadro de Controle de Verificação Sequência (FCS, do inglês *Frame Check Sequence*) que possui **(4 *bytes*)**, e contém o resultado do protocolo *Cyclic Redundancy Check* 32(CRC-32) aplicado no cabeçalho e corpo da mensagem.

3.2 ESPECIFICAÇÕES DE SEGURANÇA DO PADRÃO IEEE 802.11

A evolução das especificações dos protocolos de segurança do IEEE 802.11 deram-se da seguinte forma: Protocolo WEP, protocolo WPA, IEEE 802.11i (WPA2) e IEEE 802.11w.

3.2.1 Protocolo WEP

Apesar de atualmente o protocolo WEP não ser mais utilizado, quando homologado em (1999) ele tinha como primícias garantir o mesmo nível de segurança que em uma rede guiada. No entanto várias falhas de segurança foram identificadas, a maioria das vulnerabilidades eram advindas do seu algoritmo criptográfico *Rivest Cypher 4* (RC4) e do vetor de inicialização (IV, do inglês *Initialization Vector*) (REDDY

et al., 2010). O algoritmo RC4 do protocolo WEP tornou-se suscetível a ataques de dicionário, pois seu tamanho é reduzido, sua chave é estática e poderia ser reutilizada. O IV do protocolo WEP é considerado pequeno e era transmitido em texto simples, facilitando a sua decodificação por ferramentas de varredura de rede (*sniffers*). Outra ameaça ao protocolo WEP são os ataques de negação de serviço, este tipo de ataque explorava a ausência de proteção nos quadros de gerenciamento e controle do IEEE 802.11. As principais técnicas de ataque de negação de serviço inoculadas no protocolo WEP são: *chop-chop*, *deauthentication* (desautenticação), *Fake* AP (AP falso), *Fake Authentication*, etc. O ataque *chop-chop* explora as vulnerabilidades do mecanismo de detecção de erros. Não há verificação de ordem de quadros, portanto, o invasor pode interceptá-los e indexá-los novamente quantas vezes quiser. O ataque de *deauthentication* envia quadros falsos para desconectar algum *host* associado à rede. No ataque de *Fake AP*, vários SSIDs falsos são gerados e quando usuários legítimos tentam se conectar na rede falsa seus dados capturados.

3.2.2 Protocolo WPA

Na tentativa de sanar as principais vulnerabilidades encontradas do protocolo de segurança WEP, o IEEE homologou em 2003 o protocolo de segurança WPA. Como melhoria o protocolo WPA implementou um protocolo de integridade de chave temporal (TKIP, do inglês *Temporal Key Integrity Protocol*), o TKIP tem como função criptografar a mensagem transmitida. Além disto, o TKIP utiliza o Código de Integridade de Mensagem (MIC, do inglês *Message Integrity Code*) para embaralhar o conteúdo da mensagem original e realizar a verificação de erros (LIU; JIN; WANG, 2010). O tamanho do IV foi alterado de 24 *bits* para 48 *bits*, porém, se a complexidade da chave for baixa ainda é passível de decodificá-la. Os quadros de controle e gerenciamento da subcamada MAC permanecem sem nenhuma proteção, com isto, ficam ainda vulneráveis a ataques de negação de serviço.

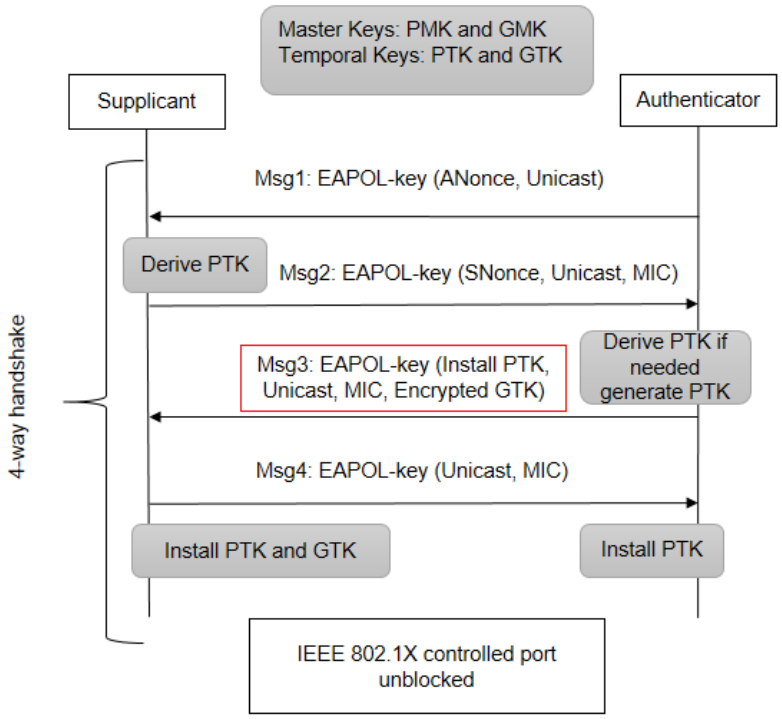
3.2.3 Protocolo IEEE 802.11i/WPA2

O IEEE 802.11i, também conhecido como WPA2, foi homologado em 2004 e está em funcionamento até a atualidade. O protocolo implementa o conceito RSN, a RSN adota critérios de alto nível de segurança para assegurar a privacidade de dados, controle de acesso e gerenciamento de autenticação (IEEE, 2004). O algoritmo RC4 foi substituído pelo *Counter-Mode* / *Cipher Block Chaining Message Authentication*

Code Protocol (CCMP) visando garantir a confidencialidade, integridade e autenticidade das mensagens transmitidas. O CCMP é baseado no Padrão de Encriptação Avançado (AES, do inglês, *Advanced Encryption Standard*), a sua chave criptográfica é de 128 *bits*. Outra mudança importante foi a implementação do Protocolo de Autenticação Extensível (EAP, do inglês *Extensible Authentication Protocol*), que usa a Associação de Rede com Segurança Robusta (RSNA, do inglês *Robust Security Network Associations*) entre o *host* e AP. O processo é executado pelo protocolo IEEE 802.1x RADIUS adicionado ao *framework* para garantir autenticação bilateral e controle de acesso (IEEE, 2001).

Apesar dos avanços obtidos pelo protocolo de segurança WPA2, a falta de proteção dos quadros de gerenciamento e controle do quadro MAC ainda deixa as redes sem fio vulneráveis a ameaças que afetam sua disponibilidade. A pesquisa realizada por Vanhoef e Piessens (2017) identificou uma nova vulnerabilidade nas redes IEEE 802.11, explorada por ataques de reinstalação de chaves (KRACK, do inglês *Key Reinstallation Attacks).* O ataque KRACK é baseado na técnica *man-in-the-middle*, cuja primícias consistem em interceptar passivamente os dados transmitidos. Na sequência, o atacante manipula as mensagens interceptadas e injeta as mensagens manipuladas durante a execução da terceira etapa do 4-*way handshake*. É instalado no *host* o *Pairwise Transient Key* (PTK), com isto, o *host* necessariamente precisa reiniciar sua conexão e transmitir os novos quadros para todos os clientes da rede e assim capturar seus PTKs e explorar ataques de negação de serviço (VANHOEF; PIESSENS, 2017). A Figura 03 resume o funcionamento da fase 4 do estabelecimento de uma RSNA, é nesta etapa que se realiza a geração e distribuição de chaves do 4-*way handshake*.

Figura 03 – Funcionamento simplificado do *4-way handshake*.



Fonte: Adaptado de IEEE (2004).

As etapas de funcionamento do *4-way handshake* é resumida da seguinte forma:

- Na primeira etapa, o AP envia ao *host* um valor arbitrário definido aleatoriamente utilizando o parâmetro (*Nonce*);
- Na segunda etapa, o cliente realiza a derivação da PTK e concatena com pares a chave mestre (PMK, do inglês *Pairwise Master Key*), com o parâmetro *Nonce* e endereço MAC enviado pelo AP, com o seu próprio *Nonce* e endereço MAC. Na sequência, é enviado através do algoritmo a mensagem ao AP, assegurando a integridade e autenticidade da mensagem;
- Na terceira etapa, o AP encaminha um grupo de chave temporal (GTK, do inglês *Group Temporal Key*) através de pacotes *broadcast* e *multicast* para o *host*. Nesta fase o cliente realiza a instalação da chave PTK e GTK; e
- Na quarta etapa, o cliente confirma o recebimento do GTK para o AP. As duas últimas etapas podem se repetir durante a conexão, em virtude da mudança do GTK.

Neste processo, tanto o AP quanto cliente possuem conhecimento das chaves utilizadas na comunicação. A etapa que define as chaves é realizado na terceira fase, e é a vulnerabilidade encontrada por Vanhoef e Piessens (2017) que deu origem ao ataque de reinstalação de chaves (KRACK).

3.2.4 Protocolo IEEE 802.11w

A especificação do protocolo IEEE 802.11w foi homologada em 2009, e teve como objetivo principal aumentar a segurança da transmissão dos quadros na camada física. A principal melhoria apresentada na ementa é a inclusão de proteção para os seguintes quadros de gerenciamento: *Disassociation*, *Deauthentication* e *Robust Action*. Os mecanismos habilitados para proteger estes quadros de gerenciamento, não criptografam os dados, somente asseguram que as mensagens transmitidas sejam oriundas de fontes legítimas. Para isto, foi introduzido o elemento de checagem da integridade das mensagem (MIC, do inglês *Message Integrity Check*). Inicialmente, apenas as mensagens *unicast* eram verificadas, posteriormente as mensagens de *broadcast* e *multicast* passaram a ser verificadas com a instalação de uma Chave Temporal do Grupo de Integridade (IGTK, do inglês *Integrity Group Temporal Key*). No entanto, se os quadros de gerenciamento forem transmitidos antes da instalação da chave criptográfica estarão desprotegidos (IEEE, 2009).

As medidas de proteção adotadas na ementa IEEE 802.11w mitigam ataques de negação de serviço do tipo *deauthentication* (desautenticação), que tinham como primícias injetar quadros falsos para desassociar clientes legítimos da rede, após habilitação deste protocolo de segurança está vulnerabilidade foi sanada. No entanto, os ataques que exploram a ausência de proteção dos quadros de controle como EAPOL-*Logoff*, BIP, SA *Query manipulation*, Association *Starvation* e RF-*jamming* ainda são ameaças em potencial para as rede IEEE 802.11 (AHMAD; TADAKAMADLA, 2011).

3.3 AMEAÇAS A SEGURANÇA EM IEEE 802.11

O quantitativo de redes sem fio padrão IEEE 802.11 tem crescido exponencialmente, quase na mesma proporção aumenta o número de ameaças a esse tipo de rede. Primeiro, porque a maioria dos ataques inoculados em uma rede sem fio pode ser empregado sem que o atacante tenha que invadir o espaço físico da rede. Segundo, porque muitas técnicas de ataques são amplamente divulgadas na

internet, assim como, existem ferramentas pré-configuradas disponíveis para o uso de agentes maliciosos. O Instituto Nacional de Padrões e Tecnologia (NIST, do inglês *National Institute of Standards and Technology*) disponibilizou um guia com as principais ameaças para redes sem fio IEEE 802.11, os principais são:

- Espionagem – está ameaça utiliza técnicas para reconhecer o cenário que será atacado. É considerado um ataque fácil de ser empregado nas redes sem fio, devido ao meio transmissão ser difundido através de sinais de RF;
- *Man-in-the-middle* – neste tipo de ameaça o atacante posiciona-se estrategicamente entre o AP e o *host*, com objetivo de interceptar informações de rede, e posteriormente manipulá-las/falsificá-las;
- *Eavesdropping* - este ataque é semelhante à técnica *man-in-the-middle*. O atacante coleta os dados da rede sem autorização, porém não os modifica e nem os transmite. O objetivo é apenas roubar informações;
- Acesso não autorizado – este ataque explora técnicas de espionagem para obter informações da rede que auxiliem a burlar os mecanismos de segurança, e obter acesso indevido. Uma das principais vulnerabilidades advém da configuração errada de dispositivos de entrada; e
- Negação de serviço – esta ameaça afeta a disponibilidade dos recursos e serviços da rede. Existem várias técnicas de ataques de negação de serviço, como (CHATZOGLOU; KAMBOURAKIS; KOLIAS, 2021):
    - RF-*Jamming* – esta técnica é aplicada na camada física da sem fio e tem como primícias causar interferência no espectro de RF da rede.
    - *Deauthentication* – nas redes sem fio IEEE 802.11 qualquer *host* não autenticado pode empregar este tipo de ataque. Basta utilizar uma ferramenta para gerar uma sequência de quadro de *deautentication* falsos para o AP da rede na tentativa de desassociar usuários legítimos.
    - *Request to Send* (RTS)/*Clear to Send* (CTS) *flood* – neste ataque é realizada a inundação do canal de comunicação da rede com várias solicitações de transmissão (RTS) em um curto período, e obrigando a vítima a responder cada solicitação com um CTS. A técnica explora a interação dos quadros na camada MAC para realizar um congestionamento no canal e tornar o serviço indisponível para o *host*.

- *Beacon Flood* - por padrão, o AP envia vários quadros de *beacon* para informar sua presença. No ataque de *beacon*, quando um *host* procurar uma rede disponível, receberá vários quadros de *beacon* falsos, dificultando a identificação da rede verdadeira.

É notório que os padrões de segurança especificados não protegem completamente a comunicação sem fio, e necessita de mecanismos auxiliares de defesa como o IDS.

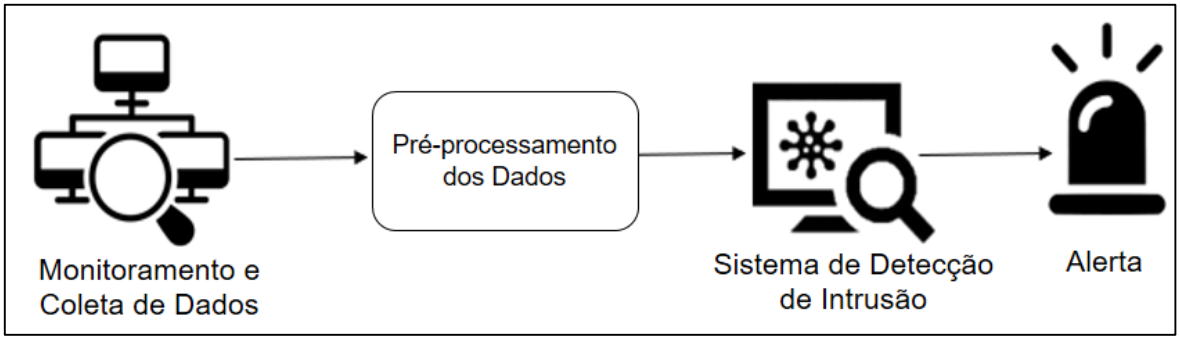
3.4 FERRAMENTA DE SEGURANÇA PARA REDES SEM FIO PADRÃO IEEE 802.11

Com o aumento dos incidentes de segurança nas redes sem fio, torna-se essencial o uso de mecanismos de proteção para garantir a segurança cibernética nessas redes de comunicação. Existem diversas ferramentas que auxiliam no controle e proteção, como *firewalls* e *softwares* antivírus e outros *frameworks* de segurança (CHOO, 2011). Os sistemas de detecção de intrusão representam uma outra área da segurança cibernética, e têm sido uma ferramenta muito utilizada por gestores de redes de computadores, principalmente nas redes de alto desempenho e com grande fluxo de tráfego de dados. O IDS concentra-se no monitoramento e análise do tráfego de rede para identificar eventos anômalos, sem comprometer o funcionamento normal da rede (LIAO *et al*., 2013).

3.4.1 Sistema de Detecção de Intrusão

O funcionamento básico de um IDS ocorre da seguinte forma: monitoramento, coleta, processamento e identificação/classificação das atividades normais ou anômalas. A Figura 04 mostra o funcionamento básico de um IDS.

Figura 04 – Funcionamento básico de um IDS.



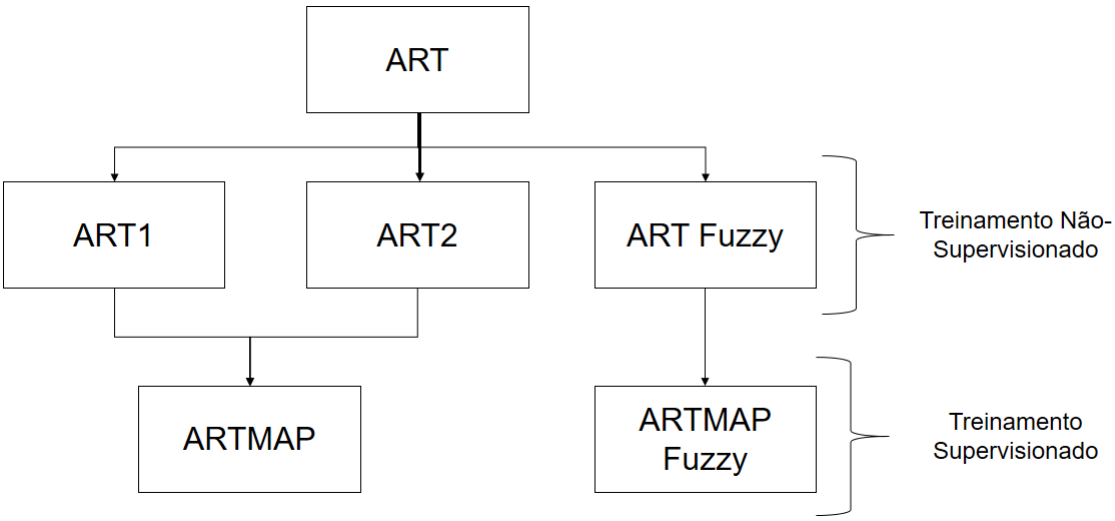
Fonte: Elaborado pelo Autor.

Há várias propostas de IDS, porém, os mais utilizados são categorizados em dois grupos: detecção por assinatura e detecção por anomalia. O modelo de detecção por assinatura utiliza conjuntos de dados que contêm amostras rotuladas de cada tipo de atividade anômala. Caso o funcionamento da rede apresente comportamento semelhante às assinaturas do conjunto de dados, então o alerta é encaminhado ao gestor da rede. Se a atividade anômala não estiver no conjunto de dados, o IDS não enviará o alerta (SOBH, 2006). Outra desvantagem do IDS por assinatura é o desempenho, conforme a quantidade de comparações aumenta, o processamento se torna mais demorado (WU; BANZHAF, 2010). O método de detecção por anomalias define um comportamento normal, e o IDS irá emitir alertas para qualquer atividade que seja diferente da considerada normal (AGRAWAL; AGRAWAL, 2015). O conjunto de dados ainda se faz necessário, pois aumentará o desempenho do IDS. As principais técnicas empregadas para esse modelo de IDS são: Aprendizado de Máquina (ML, do inglês *Machine Learning*), IDS baseado em métodos estatísticos e IDS baseado no conhecimento (AGRAWAL; AGRAWAL, 2015). Inicialmente, as técnicas de ML utilizam conjuntos de dados como base de conhecimento para aprender como a rede se comporta. Posteriormente, o sistema usa novas informações para aprender a generalizar o padrão de funcionamento.

4 TEORIA DA RESSONÂNCIA ADAPTATIVA

O estudo da teoria da ressonância adaptativa (ART, do inglês *Adaptive Resonance Theory*) teve início em 1976, o pesquisador Grossberg apresentou um novo modelo de RNA em resposta ao dilema da estabilidade/plasticidade (GROSSBERG, 1976a, 1976b). A plasticidade é a capacidade da rede adaptar-se a novos padrões de reconhecimento, e manter o conhecimento adquirido anteriormente e ao mesmo tempo armazenar novas informações. A estabilidade, assegura que todos elementos serão agrupados em categorias criadas pela RNA (LOPES, 2005). Posteriormente Carpenter e Grossberg desenvolveram outros modelos de RNA baseados na arquitetura ART, conhecidos como família ART. As principais características das redes da família ART são: aprendizado rápido, auto-organização, incrementação e estabilidade (SANTOS JÚNIOR, 2017). A Figura 05 mostra os principais modelos que fazem parte da família ART.

Figura 05 – Família ART.



Fonte: Adaptado de Lopes (2005).

Em 1987 foi apresentado por Carpenter e Grossberg o modelo de RNA ART1 (CARPENTER; GROSSBERG, 1987a). As características da rede ART1 são: treinamento não-supervisionado e capacidade de agrupar padrões de entrada binário. No mesmo ano foi apresentado o modelo ART2 (CARPENTER; GROSSBERG, 1987b), as características da rede ART2 são: treinamento não-supervisionado e capacidade de agrupar padrões de entrada binários e analógicos.

Em 1991 os pesquisadores anunciaram a rede ARTMAP. A ARTMAP que é composta por dois módulos da ART1, denominados ARTa e ARTb e um módulo *inter-*

ART (CARPENTER *et al.*, 1991a). Suas características são: treinamento supervisionado, auto organizável e reconhece padrões de entradas binários. Também em 1991 foi anunciada a rede ART *Fuzzy* (CARPENTER *et al*., 1991b). Suas características, são: treinamento não-supervisionado e arquitetura de cálculos baseados na lógica *Fuzzy*. Em 1992 foi apresentada a RNA ARTMAP *Fuzzy* (CARPENTER *et al*., 1992). A RNA ARTMAP *Fuzzy* possui treinamento supervisionado, assim como, a ARTMAP. Seus cálculos são embasados na lógica *Fuzzy* (Carpenter et al., 1992).

4.1 RNA ART

As redes baseadas na arquitetura ART possuem treinamento não-supervisionado, rápido e estável. Os padrões de entrada são classificados em categorias utilizadas no reconhecimento. É realizada uma combinação em conformidade com o nível de semelhança. A entrada é comparada com a categoria selecionada, caso nenhuma das categorias ressoem, é criada uma nova categoria. O parâmetro de vigilância é responsável pela checagem, e seu valor é definido preliminarmente, porém pode ser ajustado durante o treinamento. Isso possibilita alterar o grau de semelhança dos padrões correspondentes as categorias (CARPENTER; GROSSBERG, 1987).

A rede ART é formada por dois subsistemas: subsistema de atenção e subsistema de orientação (CARPENTER; GROSSBERG, 1991c).

- Subsistema de Atenção - possui dois campos de neurônios, F1 responsável pelo processamento dos dados de entrada, e F2 agrupa os padrões em categorias de reconhecimento. Cada campo pode conter diversas camadas de neurônios interligados por conexões não-recorrentes de (F1 a F2) e recorrentes (F2 a F1). São encarregados de armazenar as informações do processo de escolha da categoria, critério de equalização e treinamento; e
- Subsistema de Orientação - é estabelecido caso o padrão de entrada seja vinculado a uma categoria existente, esse processo é chamado de ressonância e estabelecido pelo parâmetro de vigilância (ρ). Os neurônios da camada F2 representam a categoria de reconhecimento, os neurônios podem ser dos seguintes tipos: comprometidos ou descomprometidos (CARPENTER; GROSSBERG, 1991c).

Os neurônios da camada de entrada F0 são responsáveis por realizar o pré-processamento dos vetores de entrada. Esta fase é chamada de codificação, sua função é normalizar e realizar o complemento dos dados, fazendo com que todos os vetores de entrada tenham a mesma dimensão. Na sequência os valores de F0 são encaminhados à camada F1 para realização do treinamento ART. A classificação da rede ART possui quatro fases essenciais: reconhecimento, comparação, escolha e treinamento (CARPENTER; GROSSBERG, 1991c).

Na fase de reconhecimento cada neurônio da camada de entrada F1 realiza conexões não-recorrentes com todos os neurônios da camada F2, os pesos são associados de baixo para cima. Na conexão recorrente é realizado o processo inverso, todos os neurônios de F2 se conectam a um neurônio de F1. Na sequência é realizado o cálculo de atividade, o resultado do vetor é comparado com todos os vetores de pesos armazenados na memória da rede para identificar aquele que mais se aproxima do padrão de entrada atual. O neurônio da camada F2 selecionado como candidato é aquele que possui o maior valor de índice.

Na fase de comparação são realizados ajustes, esse processo faz o teste de paridade entre o vetor de entrada e o vetor de comparação. O vetor de comparação é o resultado da atividade calculada em F1 por meio do modelo apresentado em F2. A comparação é realizada pelo parâmetro de vigilância (ρ), ele define se o padrão pode ou não ser atribuído a uma categoria existente. Caso o valor de comparação seja maior que o valor atribuído para o parâmetro de vigilância (ρ) o padrão de entrada é aceito e incluso a uma categoria ativa, se for menor, a rede realiza uma nova busca.

No treinamento ART é realizada a procura por um neurônio candidato em F2. Após a seleção, o neurônio é comparado ao padrão de entrada atual para checagem do grau de similaridade. Este processo é refeito até identificar um neurônio de saída que se assemelhe com o padrão de entrada apresentado. Caso nenhum neurônio obtenha a similaridade estabelecida pelo parâmetro de vigilância (ρ), o vetor de entrada é considerado como uma categoria desconhecida. Como não é feito nenhum vínculo com as categorias existentes, ele é considerado uma classe de origem desconhecida.

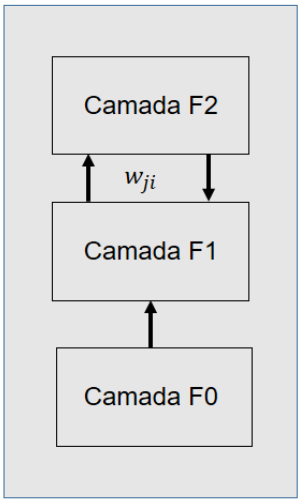
Resumindo, o subsistema de atenção é responsável por definir a classe vencedora e o subsistema de orientação em aceitar ou indicar a busca por uma nova classe. O treinamento da rede ART é realizado por um algoritmo de aprendizado não-

supervisionado, e pode ser habilitado a qualquer instante, possibilitando o aprendizado da rede de forma continua.

4.2 RNA ART *Fuzzy*

A rede ART *Fuzzy* é uma generalização da rede ART1, são agregados cálculos da teoria dos conjuntos *Fuzzy* possibilitando o processamento de dados analógicos compreendidos entre 0 e 1. O aprendizado da RNA ART é não-supervisionado, no entanto, pode ser ativado a qualquer instante, possibilitando o aprendizado de novos padrões de forma continua. Na ART *Fuzzy* o operador de interseção (∩) utilizado no ART1 é substituído pelo operador *Fuzzy* min(∧) (CARPENTER; GROSSBERG, 1991b). O agrupamento das entradas é feito em “clusters”, cada cluster é uma categoria representada na forma de hiper-retângulos. A composição das categorias é realizada pelo método de aprendizagem baseado na similaridade (*match*), são estabelecidas diretrizes que fazem a generalização dos padrões (LOPES, 2005). A Figura 06 apresenta a arquitetura da RNA ART *Fuzzy*.

Figura 06 – RNA ART *Fuzzy*.



Fonte: Adaptado de Lopes (2005).

A rede ART *Fuzzy* possui o subsistema de atenção e subsistema de orientação, similares aos apresentados na ART1. O subsistema de atenção é formado por três camadas (F0, F1, F2), conforme apresentado na Figura 06.

- F0 - faz o tratamento do vetor de entrada. Realiza normalização e codificação preservando a amplitude do valor de entrada. A saída de F0 é feita pelo vetor de atividade I em direção a camada superior F1;

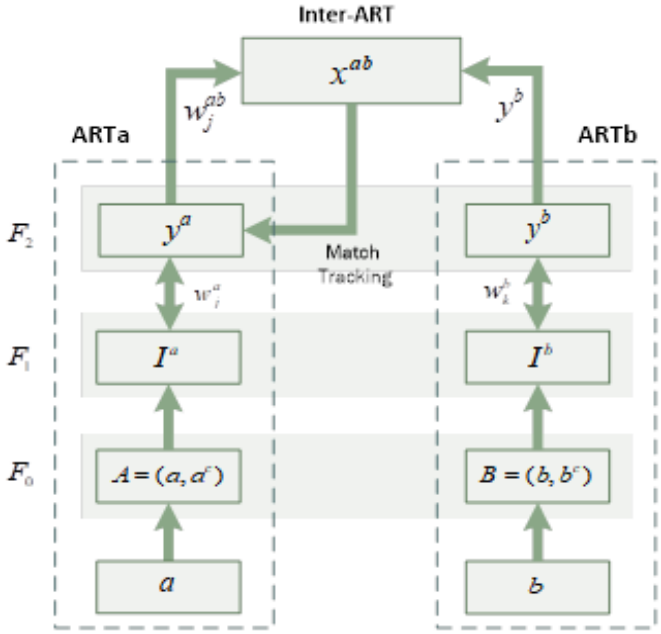
- F1 - a camada F1 também pode ser chamada de camada de comparação. F1 recebe as entrada de F0 (baixo para cima) e F2 (de cima para baixo) e realiza o teste de vigilância. O teste de vigilância indica se houve ressonância, se não ocorrer o processo é reiniciado (*reset*) e é iniciada a procura por uma nova categoria; e
- F2 - a camada F2 também pode ser chamada de camada de reconhecimento. Em F2 é realizada a classificação dos padrões de treinamento em categorias de reconhecimento. Nela estão localizados os pesos que serão atualizados e armazenados os resultados.

4.3 RNA ARTMAP *Fuzzy*

Os modelos de ML são utilizados em diversas tipos de aplicações. No que diz respeito à detecção de intrusão, as RNAs são utilizadas principalmente devido às características de adaptabilidade, escalabilidade e aprendizado de novos tráfegos de rede anômalos que possam surgir. Embora o modelo ARTMAP *Fuzzy* não tenha sido utilizado com frequência na detecção de intrusão, seu algoritmo apresenta várias vantagens em relação a outros modelos. A RNA FAM é baseada na teoria da ressonância adaptativa (ART) e carrega como propriedades: aprendizado rápido, auto-organização, incrementação e estabilidade (CARPENTER *et al*., 1992). Essas propriedades vêm do dilema plasticidade-estabilidade. A plasticidade é a capacidade de se adaptar a novos padrões de classificação e a estabilidade consiste na preservação dos conhecimentos adquiridos anteriormente (CARPENTER *et al*., 1992).

A RNA ARTMAP *Fuzzy* possibilita a utilização do treinamento supervisionado com base na rede ART não supervisionada existente (CARPENTER; GROSSBERG, 1987). Sua arquitetura é composta por três módulos: módulos *Fuzzy* ARTa e *Fuzzy* ARTb, interligados pelo módulo *Inter*-ART. Os padrões de entrada são recebidos pelo ARTa, que envia suas previsões como entradas para o módulo ARTb. Ambos os módulos são conectados por *Inter*-ART que possui o mecanismo *Match-Tracking* para identificar as categorias ativas. A Figura 07 apresenta a arquitetura de uma RNA ARTMAP *Fuzzy* (SANTOS JÚNIOR, 2017).

Figura 07 – Arquitetura ARTMAP *Fuzzy*



Fonte: SANTOS JUNIOR (2020).

O algoritmo ARTMAP *Fuzzy* possui as seguintes etapas (CARPENTER *et al*., 1992):

1) Leitura do vetor de entrada (A) e vetor de saída (B).

$$\mathrm{A} = [\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_\mathrm{n}] \text{ and } \mathrm{B} = [\mathrm{b}_1, \mathrm{b}_2, \ldots, \mathrm{b}_\mathrm{n}] \quad (1)$$

Sendo:

n: número de padrões de entrada

2) Normalização do vetor de entrada (A) e vetor de saída (B).

$$\bar{a} = \frac{\mathrm{a}}{|\mathrm{a}|} \text{ e } \bar{b} = \frac{\mathrm{b}}{|\mathrm{b}|} \quad (2)$$

3) Codificação complementar dos vetores (A) e (B). Esta etapa é realizada preliminarmente para manter as informações de amplitude.

$$\bar{a}_\mathrm{i}^\mathrm{c} = 1 - \mathrm{a}_\mathrm{i} \text{ e } \bar{b}_\mathrm{i}^\mathrm{c} = 1 - \mathrm{b}_\mathrm{i} \quad (3)$$

4) Vetor de entrada (A) e Vetor de saída (B) normalizados e complementados.

$$\mathrm{I}^\mathrm{a} = [\mathrm{a}\ \bar{a}] \text{ e } \mathrm{I}^\mathrm{b} = [\mathrm{b}\bar{b}] \quad (4)$$

Sendo:

I^a: vetor de entrada da camada de entrada F_0^a;

I^b: vetor de saída da camada de entrada F_0^b.

5) Inicialização da matriz de peso. O peso começa com o valor 1, inativando todas as categorias;

$$w_j^a = 1;\ w_j^b = 1;\ w_j^{ab} = 1; \tag{5}$$

6) Definição dos parâmetros aplicados ao treinamento RNA FAM.

α: parâmetro de escolha (α), sendo (α> 0);

β: parâmetro da Taxa de treinamento (β), sendo (β ϵ [0,1]) ;

ρa: parâmetro de vigilância do módulo ARTa (ρa ϵ [0,1]);

ρb: parâmetro de vigilância do módulo ARTb (ρb ϵ [0,1]);

ρab: parâmetro de vigilância do módulo inter-ART (ρab ϵ [0,1]);

ε: incremento do parâmetro (ρa).

7) Leitura dos parâmetros;

$$\alpha, \beta, \rho a, \rho b, \rho ab, \varepsilon; \tag{6}$$

8) Categorias escolhidas dos módulos ARTa e ARTb: Caso haja mais de um neurônio ativo, seleciona-se o índice de ordem menor.

a) Cálculo das Funções (T_k^b) e (T_j^a):

$$T_k^b(I^b) = \frac{|I^b \wedge\ w_k^b|}{\alpha + |w_k^b|};\quad T_j^a(I^a) = \frac{|I^a \wedge\ w_j^a|}{\alpha + |w_j^a|} \tag{7}$$

b) Escolha de categoria (K) para ARTb *Fuzzy* e (J) para ARTa *Fuzzy*:

$$T_K^b = \{T_k^b : k = 1, \dots, N_b\};\ \ T_j^a = \{T_j^a : j = 1, \dots, N_a\}; \tag{8}$$

c) Verificação da correspondência do parâmetro de vigilância para ARTb *Fuzzy* e ARTa *Fuzzy*. A ressonância ocorre quando o critério de vigilância é satisfeito. Caso contrário, uma pesquisa é realizada para encontrar um novo índice (*reset*). O processo de busca se repete até que o critério de vigilância seja satisfeito.

$$\left|x^b\right| = \frac{|I^b \wedge\ w_K^b|}{|I^b|} \geq \rho b;\ |x^a| = \frac{|I^a \wedge\ w_j^a|}{|I^a|} \geq \rho a \tag{9}$$

Se ARTb não for satisfeito: Reinicia-se $T_K^b = 0$;

Se o critério de vigilância for satisfeito:

- Realiza-se ressonância adaptativa dos pesos para ARTb *Fuzzy*:

$$w_K^{novo} = \beta\left(I^b \wedge w_K^{velho}\right) + (1-\beta) w_K^{velho} \quad (10)$$

- Calcular o vetor de atividade em F_2:

$$y_K^b = \left[y_1^b, y_2^b, \ldots, y_N^b\right];\ y_j^a = \left[y_1^a, y_2^a, \ldots, y_N^a\right] \quad (11)$$

9) O *Match-Tracking* verifica o critério de vigilância no módulo *Inter*-ART.

$$\left|x^{ab}\right| = \frac{|y^b \wedge w_J^{ab}|}{|y^b|} \geq \rho ab \quad (12)$$

Se o critério não for satisfeito, incrementa o parâmetro de vigilância:

$$\rho a = \frac{|y^b \wedge w_J^{ab}|}{|I^e|} + \varepsilon; \quad \text{Reset: } T_j^a = 0 \quad (13)$$

Se o critério for satisfeito:

- Executa ressonância e adaptação de pesos para o módulo ARTa *Fuzzy*:

$$w_J^{novo} = \beta\left(I^a \wedge w_J^{velho}\right) + (1-\beta) w_J^{velho} \quad (14)$$

- Atualização de pesos para o módulo Inter-ART:

$$W_{JK}^{ab} = \left[y_1^{ab}, y_2^{ab}, \ldots, y_N^{ab}\right] \quad (15)$$

Sendo:

$$y_{jk}^{ab} = \{1, \text{if } j = J$$

$$k = K\ 0, \text{if } j \neq J$$

$$k \neq K \quad (16)$$

- Repetir até que todos os pares estejam treinados.

5 DESCRIÇÃO DO CENÁRIO DE TESTE

A metodologia de desenvolvimento da pesquisa foi realizada em quatro etapas. A primeira etapa descreve a metodologia empregada para seleção da rede sem fio IEEE 802.11 utilizada na pesquisa. Na segunda etapa foi realizada a avaliação da rede IEEE 802.11 selecionada, a métrica utilizada para validar o ambiente deu-se através do estudo preditivo do tráfego de dados gerado na rede. A terceira etapa detalha a construção, padronização e pré-processamento do conjunto de dados utilizado na pesquisa. Por fim, a quarta etapa detalha o funcionamento do algoritmo utilizado como ferramenta de detecção de intrusão em redes IEEE 802.11, as métricas de avaliação empregadas e os resultados obtidos pelo IDS.

5.1 SELEÇÃO DA REDE IEEE 802.11

Os critérios de escolha do cenário de rede sem fio utilizado na pesquisa foram: diversidade de dispositivos, interoperabilidade entre dispositivos e rede de comunicação sem fio, amplo volume de dados trafegados, protocolo de segurança IEEE 802.11w habilitado e características advinda de um sistema baseado na *internet* das coisas (IOT, do inglês *Internet of Things*). Também foi levado em consideração o desempenho, escalabilidade e a adaptabilidade da rede sem fio.

- Desempenho da rede – para avaliar o desempenho da rede considerou-se a taxa de transferência de dados na rede em períodos de sessenta (60) minutos. A taxa de transferência é uma medida importante para estimar a capacidade de desempenho necessário do IDS durante a análise do tráfego de rede.

- Escalabilidade da rede - esta métrica considera a capacidade de expansão da rede a nível de desempenho, número de usuários, serviço e dispositivos.

- Adaptabilidade da rede - esta métrica considera a adaptação da rede sem fio a inserção de novos perfis de usuário, serviços, aplicações e dispositivos.

Segundo Liu (2016), para um sistema de comunicação possa ser classificado como um Campus Inteligente, é necessário atender os critérios e métricas elencados acima. Além disso, deve garantir ambientes de estudo e pesquisa integrados e interoperáveis com aplicação IOT (LIU, 2016).

Neste sentido, o ambiente mais indicado foi o de uma instituição federal de ensino profissional e tecnológico. O Campus da instituição é localizado em Cuiabá, no estado de Mato Grosso, e oferece formação tecnológica nas áreas de saúde, controle industrial, alimentos, TIC, entre outras áreas. Além disso, o campus está dentro de uma área de proteção ambiental de setenta mil metros quadrados. A Figura 8 mostra uma visão panorâmica do Campus.

Figura 08 - Visão panorâmica do campus Bela Vista do Instituto Federal de Mato Grosso.

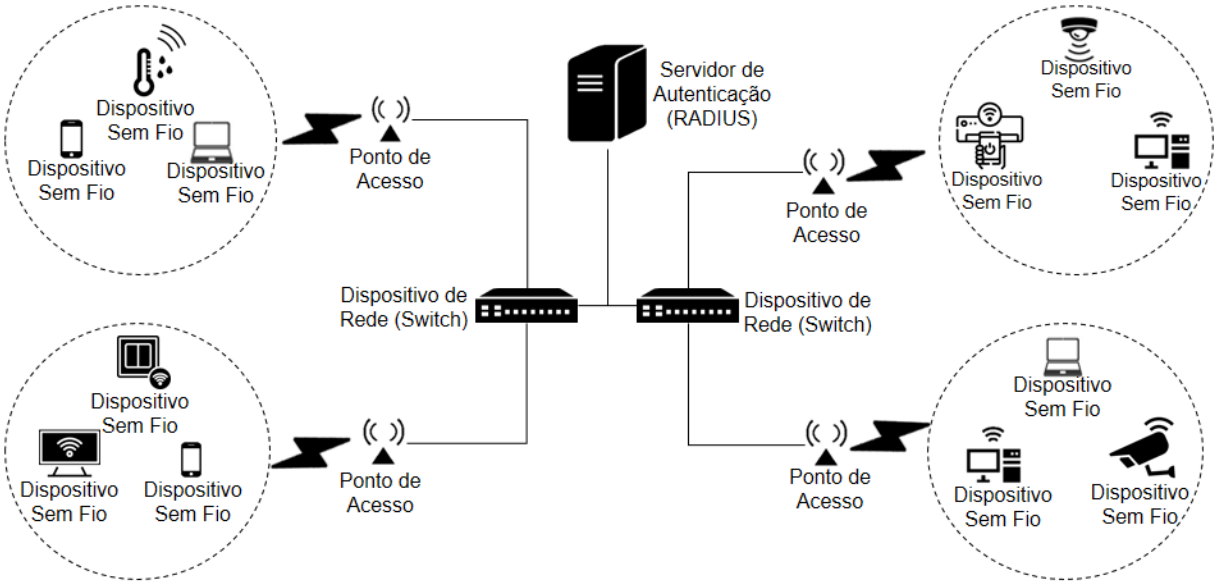
Fonte: Adaptado de Google Earth (2021).

A estrutura organizacional do ambiente selecionado é composta por diversos colaboradores, que são dispostos da seguinte forma: funcionários administrativos e docentes (±140 usuários); e estudantes (±2500 usuários) matriculados em cursos regulares com oferta presencial e ensino a distância. A estrutura organizacional evidencia diferentes perfis de usuários que utilizam a rede de comunicação sem fio. A heterogeneidade do cenário o caracteriza como ótimo, pois comtempla vários padrões de comportamento dentro de cada perfil de usuário. A rede sem fio está segmentada em três perfis de funcionamento: Administrativo, Professores e Alunos.

A rede sem fio é composta por diversos dispositivos, como: computadores, *notebooks*, *smartphones*, impressoras, *smart tv*, câmeras inteligentes, ar condicionados e sensores. Os dispositivos estão conectados à rede através de vários

pontos de acesso, os APs foram distribuídos estrategicamente para cobrirem todo perímetro do campus. A caracterização geográfica da rede é dada por um rede sem fio Campus (WCAN) que funciona no modo de operação infraestrutura e em topologia estrela, conforme mostrado na Figura 09.

Figura 09 - Topologia da rede sem fio IEEE 802.11 selecionada.



Fonte: Elaborado pelo Autor.

O cenário escolhido já foi objeto de estudo do autor (VILELA, 2014). No entanto, a estrutura física e lógica da rede passou por mudanças. A área de cobertura da rede foi expandida, para isto foram instalados novos pontos de acesso. Anteriormente eram 17 APs, e na atualidade são 25 APs. O protocolo de segurança habilitado na atualidade é o IEEE 802.11w, esta mudança foi realizada principalmente para garantir a proteção dos quadros de gerenciamento. Também foi alocado na estrutura da rede um servidor RADIUS, que tem como função prover a autenticação segura por meio do *framework* IEEE 802.1x.

5.2 AVALIAÇÃO DA REDE IEEE 802.11

Nesta etapa foi realizada uma análise preditiva do tráfego de dados gerado na rede sem fio no ano de 2019. Este estudo teve como objetivo analisar a volumetria do tráfego de dados corrente e realizar um comparativo com um estudo similar realizado em 2014 por Vilela, e assim, diagnosticar o aumento de dados trafegados no período, sazonalidade, tendência e previsão de crescimento. No estudo realizado em 2014 foram coletados dados da rede durante um ciclo semanal (07 dias). O processo de

coleta foi realizado de forma automatizada, sendo salvo um pacote de dados no formato PCAP *Next Generation* (.PCAP) a cada intervalo de sessenta (60) minutos. Durante todo período de coleta foram gerados cento e sessenta e oito (168) arquivos, e cada um dos registros contém os pacotes transmitidos durante aquele intervalo de tempo (60 minutos). No período de coleta de dados para a avaliação da rede sem fio não foi realizado ataques na rede e também não foi observado nenhum evento anômalo (incidente), propiciando um padrão de comportamento regular da rede.

A metodologia de coleta de dados empregada no estudo realizado em 2019 foi semelhante a de 2014. Os dados coletados para análise foram capturados por um computador móvel, que foi disposto em um ponto de cobertura global da rede. Para diagnosticar qual o melhor ponto de cobertura do sinal de rádio frequência foi realizada uma análise do *spectro*. O equipamento utilizado foi configurado com sistema operacional Linux (Kali Linux), e para poder escutar todo o tráfego da rede sem fio a interface da placa de rede *wireless* foi habilitada em modo monitor. Para esta tarefa foi desenvolvido um *script* que chama o comando *airmon-ng* da ferramenta *Aircrack-ng* (AIRCRACK-NG, 2019). Na sequência foi utilizado o analisador de protocolos (*Wireshark*) para realização da coleta dos dados transmitido na rede sem fio tráfego (SANDERS, 2017). A metodologia utilizada para capturar apenas os dados da rede em estudo utilizou os filtros da própria ferramenta *wireshark*, sendo eles: SSID, origem e destino.

A Tabela 01 mostra os registro coletados em 2014 e a Tabela 02 contém a distribuição do número de registros coletados em 2019. O lapso temporal entre os estudos foi de cinco (05) anos.

Tabela 01 – Registros do tráfego de dados da rede sem fio IEEE 802.11 (2014).

Período	Registros coletados por período											
[1 – 12]	217.439	184.311	126.006	133.206	188.576	88.671	96.394	162.828	120.356	95.410	182.058	177.654
[13 – 24]	77.822	74.969	190.381	178.957	124.700	201.624	227.097	88.378	89.419	203.898	149.238	106.887
[25 – 36]	198.389	195.930	88.197	95.703	80.512	91.109	107.740	78.865	118.021	99.991	80.690	113.021
[37 – 48]	110.792	105.687	117.544	134.652	73.241	81.121	118.568	112.470	103.919	121.036	140.211	61.089
[49 – 60]	78.418	117.201	137.843	111.721	124.034	121.348	82.067	73.623	142.311	132.830	132.082	128.903
[61 – 72]	109.919	75.909	74.595	131.691	111.947	137.883	133.433	99.008	87.405	88.318	434.912	347.439
[73 – 84]	357.601	298.993	198.034	93.426	81.032	271.104	302.221	302.987	328.769	190.151	84.824	89.008
[85 – 96]	158.157	274.812	310.988	198.723	189.755	89.114	94.066	101.675	197.350	169.399	177.234	192.345
[97 – 108]	70.074	99.075	211.209	297.331	245.967	119.045	128.599	90.010	78.039	246.261	147.341	200.803
[109 – 120]	92.456	134.579	99.810	70.093	110.600	147.343	195.126	101.238	109.316	78.418	82.143	100.531
[121 – 132]	102.297	134.568	99.219	82.326	85.788	74.541	80.434	97.354	80.209	88.067	93.218	93.665
[133 – 144]	67.677	75.414	89.775	77.429	90.040	95.509	91.033	68.098	73.788	99.864	84.521	93.943
[145 – 156]	81.063	87.809	65.567	80.456	85.678	90.349	89.129	94.244	71.244	72.022	85.467	87.540
[157 – 168]	100.982	95.754	99.210	80.604	81.112	102.903	99.751	111.306	104.544	90.222	75.663	83.991

Fonte: Elaborado pelo Autor.

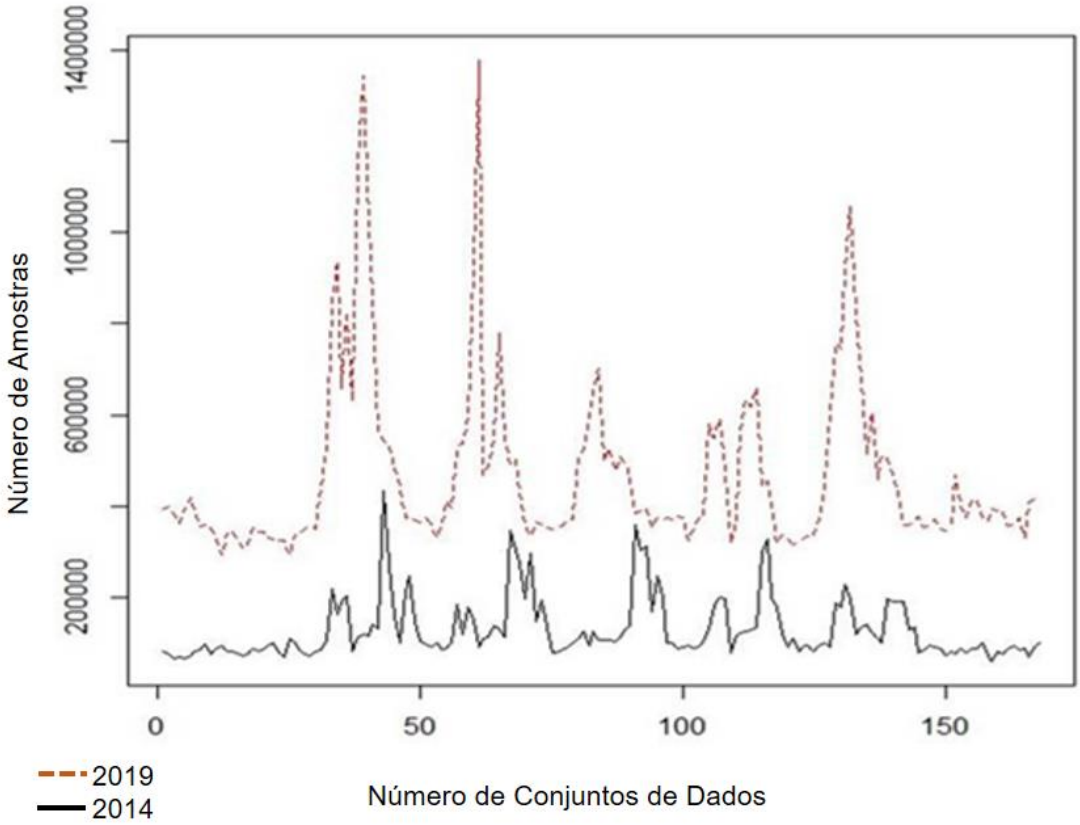
Tabela 02 – Registros do tráfego de dados da rede sem fio IEEE 802.11 (2019).

Período	Registros coletados por período											
[1-12]	393.376	399.367	383.782	363.318	397.737	418.341	392.875	357.290	359.850	352.471	334.448	294.456
[13-24]	341.757	345.192	330.137	308.388	316.754	351.772	342.238	342.475	331.882	326.562	325.293	323.852
[25-36]	294.245	335.940	344.746	349.830	356.166	349.050	443.090	533.330	842.349	937.045	657.225	825.651
[37-48]	629.890	1.144.808	1.341.204	1.019.419	855.576	564.300	544.922	528.726	483.734	439.823	373.596	377.142
[49-60]	369.422	365.663	374.770	363.124	332.436	359.654	412.715	397.659	529.566	534.848	592.080	921.310
[61-72]	1.376.559	468.811	486.483	543.241	779.833	547.522	492.320	501.288	429.815	365.291	335.265	363.706
[73-84]	359.394	353.116	348.177	351.634	355.315	371.190	372.877	505.937	524.748	596.162	644.464	702.856
[85-96]	498.936	526.802	477.217	508.225	493.838	461.796	384.661	390.918	393.400	353.222	377.931	367.745
[97-108]	373.945	372.718	376.191	375.111	325.880	349.847	373.378	374.177	579.108	547.303	588.690	471.014
[109-120]	316.932	369.629	567.112	632.769	616.998	658.358	442.830	455.293	406.856	317.358	337.591	327.408
[121-132]	314.747	322.341	330.660	335.430	334.753	369.790	449.871	607.788	755.910	744.696	913.698	1.057.161
[133-144]	820.720	672.442	510.351	603.890	458.468	507.621	508.789	474.750	433.027	359.099	358.864	366.907
[145-156]	379.027	353.370	359.088	371.442	350.427	347.765	360.360	468.112	402.558	373.735	415.330	410.800
[157-168]	374.025	368.195	391.748	389.027	385.601	355.206	360.013	374.573	330.827	407.328	414.177	409.611

Fonte: Elaborado pelo Autor.

A primeira análise identificou que o tráfego de dados na rede aumentou cerca de 260% no período. Uma das possíveis causas foi a expansão da área de cobertura da rede, bem como, o aumento do número de usuários e dispositivos de rede. A Figura 10 apresenta um comparativo do tráfego de dados de 2014 e 2019. O perfil de funcionamento segue o mesmo padrão, e assim como em 2014 pode-se observar que de segunda-feira a sexta-feira ocorre um aumento do tráfego no período de 19 horas as 20 horas. A provável causa dessa disparidade pode estar relacionada a troca de turnos (vespertino e noturno).

Figura 10 - Fluxo evolutivo do tráfego de dados da rede sem fio IEEE 802.11 nos anos de 2014 e 2019.



Fonte: Elaborado pelo Autor.

Na análise seguinte, foi realizada a predição comportamento do fluxo de tráfego da rede. A métrica aplicada foi baseada na série temporal aditiva de Holt-Winters. O padrão estatístico de Holt-Winters gera estimativas aproximadas da realidade, e para isso utiliza a amplitude da variação sazonal. O modelo é baseado em equações balizadoras que identificam nível, tendência e sazonalidade. As equações básicas do modelo aditivo de Holt-Winters estão descritas nas Equações 17, 18, 19 e 20.

Nível: $$L_t = \alpha\,(Z_t - S_{t-s}) + (1-\alpha)(L_{t-1} + T_{t-1}) \quad (17)$$

Tendência: $$T_t = \beta\,(L_t - L_{t-1}) + (1-\beta)T_{t-1} \quad (18)$$

Sazonalidade: $$S_t = \gamma\,(Z_t - L_t) + (1-\gamma)S_{t-s} \quad (19)$$

Previsão: $$Z_{t+k} = L_t + T_{t-k} + S_{t-s+k} \quad (20)$$

Sendo:

- t – Período de tempo;
- s - Tamanho da sazonalidade;

- k – Períodos à frente;
- L – Nível estimado da série;
- T –Tendência estimada da série;
- S - Sazonalidade estimada da série;
- Z_{t+k} - Previsão para k períodos à frente;
- $\hat{Z}$- Previsão de demanda;
- Z - Valor real observado na série;
- n – Quantidade de observações associadas as previsões; e
- α, β, γ - constantes de suavização do nível, da tendência e da sazonalidade (intervalos entre 0 e 1);

A análise preditiva do padrão de caracterização foi realizada pela ferramenta estatística R (R-STUDIO, 2020). Os Valores de entrada definidos para as constantes de suavização do modelo aditivo de *Holt-Winters* estão listados na Tabela 03.

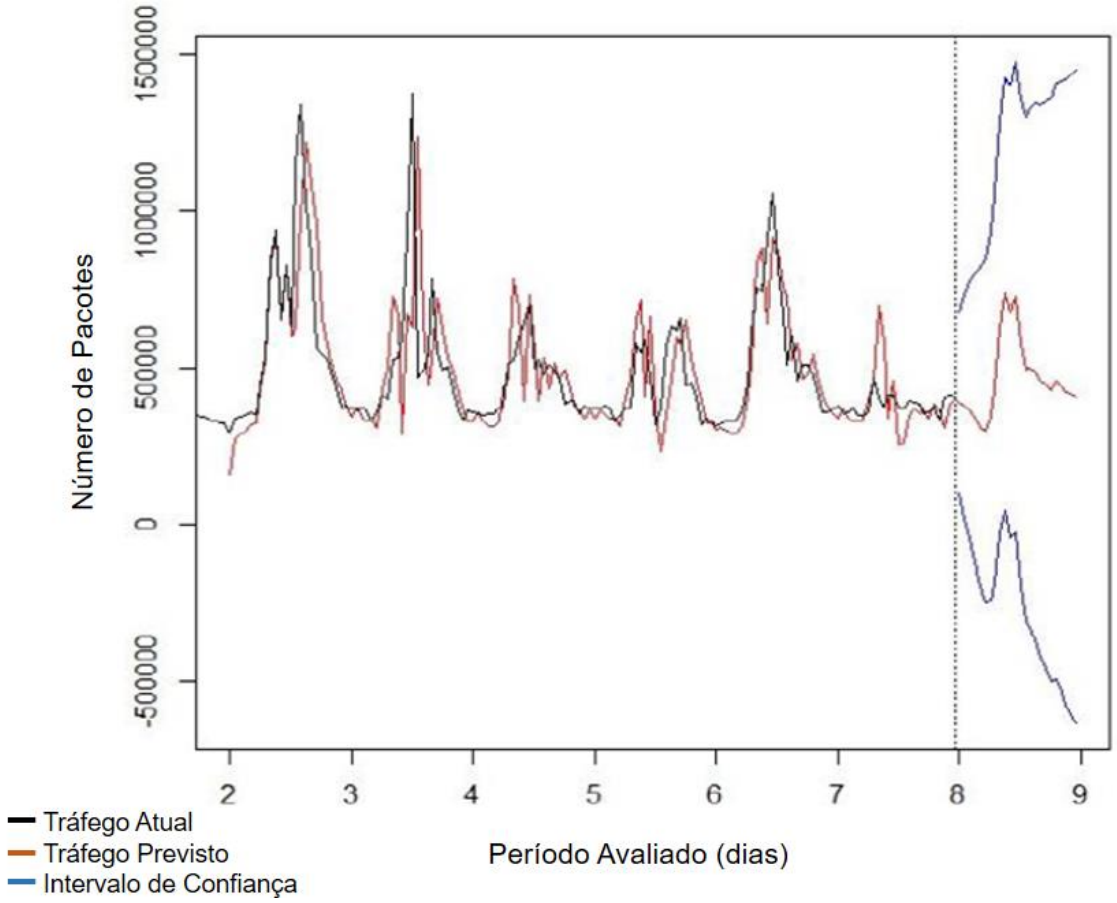
Tabela 03 – Valores de entrada definidos para as constantes de suavização do modelo aditivo de *Holt-Winters*.

	α	β	γ
Modelo Aditivo	0.7	0	0.4

Fonte: Elaborado pelo Autor.

Os valores de entrada foram escolhidos empiricamente, e os efeitos aditivos apresentaram sazonalidade pela período matutino e quando há o aumento do tráfego de dados na rede (18 horas as 19 horas). A constante β é igual a zero e mostra que os parâmetros unitários de tendência foram bem definidos, e não precisam ser atualizados para encontrar o erro quadrático médio. Ou seja, o padrão permanecerá no futuro. A análise apresentada evidencia a eficiência do método de Suavização Exponencial de Holt-Winters, A Figura 11 mostra a previsão do tráfego de dados da rede IEEE 802.11 apresentada pelo modelo aditivo de Holt-Winters.

Figura 11 - Previsão do tráfego de dados da rede IEEE 802.11 apresentada pelo modelo aditivo de Holt-Winters.



Fonte: Elaborado pelo Autor.

A avaliação do funcionamento e análise do tráfego da rede sem fio em estudo foi essencial para dimensionar o fluxo de informações trafegadas, bem como prever sua escalabilidade. O diagnóstico é necessário para implementação de soluções baseadas em rede, pois infere no dimensionamento de recursos computacionais que serão estabelecidos.

5.3 CONSTRUÇÃO E ESTRUTURAÇÃO DO CONJUNTO DE DADOS

Encontrar conjuntos de dados que representem o tráfego normal e anômalo de uma rede sem fio corporativa, e com registros oriundos de um ambiente real não é uma tarefa fácil. Na maioria das vezes, as vulnerabilidades de segurança de uma rede não devem serem expostas publicamente. Além disso, existem os dados privados que não podem ser compartilhados. Neste caso, por muitas das vezes ao remover determinados campos do conjunto de dados, acarreta na perda de atributos fidedignos da rede e destoando do real. Os conjuntos de dados são fundamentais para treinar,

validar e testar a eficiência de um sistema de detecção de intrusão. Como alternativa, vários pesquisadores de IDS têm utilizado conjuntos de dados simulados, e isto por vezes limita a estimativa de desempenho do IDS se comparado a um conjunto de dados real (BUCZAK; GUVEN, 2015). Nesta pesquisa, foi gerado um conjunto de dados que foi usado como base de conhecimento para o treinamento, validação e teste do IDS desenvolvido. O conjunto de dados foi gerado a partir da captura do tráfego de dados de uma rede sem fio IEEE 802.11 real em funcionamento em um campus de uma instituição de ensino.

O conjunto de dados foi gerado a partir da coleta de informações do quadro MAC da rede sem fio IEEE 802.11 selecionada. O processo de captura foi realizado por um computador móvel disposto em um ponto estratégico da rede, de modo que captasse todos sinais de rádio frequência transmitidos na área de cobertura global da rede. O diagnóstico para escolha do ponto de coleta foi dado pela análise do espectro de rádio frequência dos pontos de acesso da rede. O computador móvel foi configurado com sistema operacional Linux (Kali Linux) e demais ferramentas necessárias para coleta. Para poder escutar todo o tráfego da rede sem fio a interface da placa de rede *wireless* foi habilitada em modo monitor. Utilizou-se o mesmo *script* desenvolvido na fase de avaliação da rede e também foi utilizada a ferramenta de análise de protocolos (*Wireshark*).

Durante o período de uma (01) semana foram coletados registros de tráfego de rede normal e anômalos. A captura iniciou-se domingo no período matutino e encerrou-se no período noturno de sábado. O *software wireshark* foi configurado para armazenar a cada intervalo de sessenta (60) minutos todos os dados transmitidos na rede. Os sete (07) dias de coleta resultaram em um grande conjunto de dados formado por cento e sessenta e oitos subconjuntos. Como a rede sem fio funcionava em modo infraestruturado, todas informações transmitidas são gerenciadas pelos pontos de acesso. Isso possibilitou que fosse aplicado um filtro em todo conteúdo que passava pelos pontos de acesso, para que somente fossem armazenadas informações direcionadas a rede sem fio estudada. No período de coleta, além das atividade consideradas normais foram realizados quatro (04) tipos de ataques na rede para produzir eventos anômalos. Os ataques empregados são de negação de serviço, a Tabela 04 mostra as técnicas realizadas e o tipo de quadro afetado pelo ataque.

Tabela 04 - Ataques realizados na rede sem fio IEEE 802.11.

Ataque	**Quadro Afetado**
Deauthentication	Gerenciamento
Beacon Flood	Gerenciamento
EAPOL-Start	Gerenciamento/Dados
RTS-Flood	Controle

Fonte: Elaborado pelo Autor.

Apesar dos ataques inoculados no ambiente serem baseados em técnicas de negação de serviço, cada um possui uma característica específica e exploram vulnerabilidades distintas nos quadros do cabeçalho MAC da rede sem fio IEEE 802.11. Os ataques foram realizados empiricamente durante todos os dias da coleta de informações para construção do conjunto de dados. Foram utilizados na inoculação dos ataques equipamentos distintos, para que não se caracterizasse a origem ou um padrão de saída. A descrição de funcionamento de cada ataque realizado está listada baixo:

- *Deauthentication* (Desautenticação) – o ataque de *deauth* afeta o quadro de gerenciamento, e possui como primícias o envio atenuado de quadros fictícios do tipo *deauthentication* forçando o dispositivo a se desconectar da rede (AHMAD; TADAKAMADLA, 2011). Para realização deste ataque foi utilizado a ferramenta *aireplay-ng* incluída no pacote *aircrack-ng* (AIRCRACK-NG, 2019);
- *Beacon* Flood - o ataque de *beacon* afeta o quadro de gerenciamento, seu funcionamento é dado pelo envio massivo de milhões de pacotes com vários SSIDs falsos no espectro de RF da rede, confundindo os usuários que tentarem se conectar ao ponto de acesso (AHMAD; TADAKAMADLA, 2011). A ferramenta utilizada para realização deste ataque foi o MDK3 (MDK3, 2019);
- EAPOL-*Start* – o ataque EAPOL-*Start* afeta os quadros de gerenciamento e controle. Este ataque tem como finalidade realizar uma inundação de pacotes EAPOL com vários pedidos de autenticação EAP provocando a negação de serviço entre AP e servidor de autenticação (IEEE 802.1x) (AHMAD; TADAKAMADLA, 2011); A ferramenta utilizada para realização deste ataque foi o MDK3 (MDK3, 2019);

- RTS *Flood* – o ataque de RTS Flooding afeta o quadro de controle. Neste ataque é realizado o envio excessivo de quadros RTS em um curto período de tempo, provocando o congestionamento do canal (HEŠÍK, 2013).

O total de registros coletados para construção do conjunto de dados foi de aproximadamente doze milhões e trezentos mil (12.300.000) amostras. A distribuição das amostras do conjunto de dados é mostrado na Tabela 05.

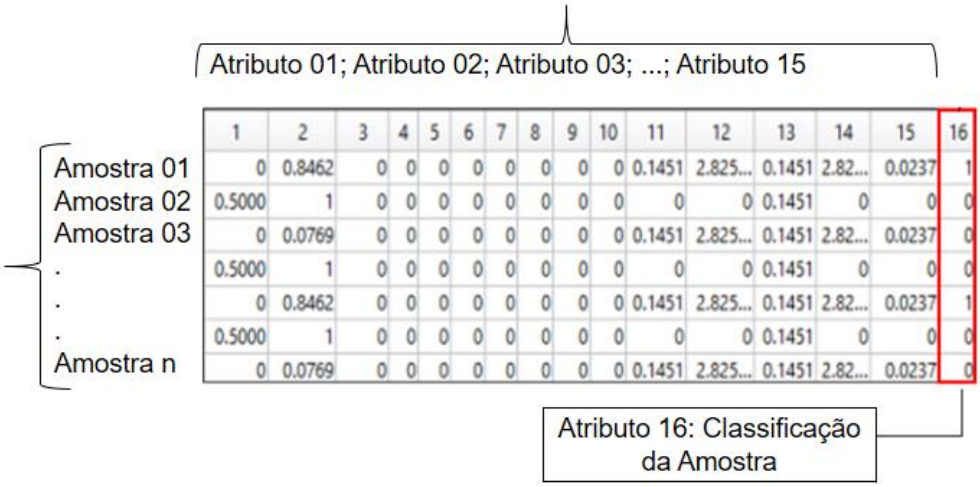
Tabela 05 – Distribuição das amostras do conjunto de dados utilizado no treinamento e teste do IDS.

Tipo da amostra	**Número de amostras**
Normal	10.886.309
Deauthentication	323.976
Beacon Flood	545.481
EAPOL-Start	539.692
RTS Flood	2.113
Total de amostras	**12.297.571**

Fonte: Elaborado pelo Autor.

A próxima etapa foi a de estruturação do conjunto de dados, a primeira tarefa realizada foi a rotulação das amostras. Cada registro recebeu um rótulo (*ticket*) que o identificava como normal ou anômalo, as amostras anômalas foram classificadas de acordo com o tipo de ataque que ela representa. A rotulação completa do conjunto foi balizada pela origem dos ataques e tipo de quadro, posteriormente estes campos foram anonimizados para não influenciarem no aprendizado do IDS. Outra parte da estruturação do conjunto de dados foi a extração dos campos do cabeçalho MAC do quadro IEEE 802.11. O pré-processamento foi realizado pela ferramenta T-shark, e os campos extraídos foram: *protocol version* (versão do protocolo), *type* (tipo), *subtype* (subtipo), *to ds*, *from ds*, *more flag* (especificações de fragmentação), *retry* (retransmissão), *power manager* (gerenciamento de energia), *more data* (mais dados), *order*, *duration* (duração), *address* (endereço mac) e *sequence control* (controle de sequência). A representação do conjunto de dados pré-processado pode ser observada na Figura 12.

Figura 12 - Fragmento do conjunto de dados gerado para o treinamento do IDS.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Amostra 01	0	0.8462	0	0	0	0	0	0	0	0	0.1451	2.825...	0.1451	2.82...	0.0237	1
Amostra 02	0.5000	1	0	0	0	0	0	0	0	0	0	0	0.1451	0	0	0
Amostra 03	0	0.0769	0	0	0	0	0	0	0	0	0.1451	2.825...	0.1451	2.82...	0.0237	0
.	0.5000	1	0	0	0	0	0	0	0	0	0	0	0.1451	0	0	0
.	0	0.8462	0	0	0	0	0	0	0	0	0.1451	2.825...	0.1451	2.82...	0.0237	1
.	0.5000	1	0	0	0	0	0	0	0	0	0	0	0.1451	0	0	0
Amostra n	0	0.0769	0	0	0	0	0	0	0	0	0.1451	2.825...	0.1451	2.82...	0.0237	0

Fonte: Elaborado pelo Autor.

5.4 NORMALIZAÇÃO DO CONJUNTO DE DADOS E DEFINIÇÃO DO PARÂMETROS DO ALGORITMO ARTMAP *FUZZY*

A RNA ARTMAP *Fuzzy* recebe padrões de entrada analógicos entre zero (0) e um (1) e binários, por isso foi necessário realizar a normalização e codificação dos vetores da camada de entrada e saída do conjunto de dados. A identificação das amostras do conjunto de dados do vetor de saída foram divididas em 5 classes, com valores de saída entre 0 e 1:

- S1 - amostra classificada como normal. A identificação dessa amostra recebeu valor zero (0);
- S2 – amostra classificada como anômala oriunda do ataque RTS *Flood.* A identificação dessa amostra recebeu valor zero (0,25);
- S3 - amostra classificada como anômala oriunda do ataque EAPOL-*Start.* A identificação dessa amostra recebeu valor zero (0,50);
- S4 - amostra classificada como anômala oriunda do ataque de *Deauthentication.* A identificação dessa amostra recebeu valor zero (0,75); e
- S5 - amostra classificada como anômala oriunda do ataque *Beacon Flood*. A identificação dessa amostra recebeu valor zero (1)

A Tabela 06 mostra como foi identificada cada amostra do vetor de saída.

Tabela 06 – Classificação das amostras do vetor de saída.

Classificação dos Dados	Classe	Vetor de saída *b*
Normal	S1	0
RTS *Flood*	S2	0,25
EAPOL-*Start*	S3	0,50
Deauthentication	S4	0,75
Beacon Flood	S5	1

Fonte: Elaborado pelo autor.

Na sequência, os vetores A e B foram codificados os vetores para que a amplitude das informações fossem preservadas (CARPENTER *et al*., 1992). Nesta etapa, também foram realizados os ajustes de parâmetros da RNA ARTMAP *Fuzzy*. Os parâmetros foram definidos para o treinamento e teste do IDS são mostrados na Tabela 07.

Tabela 07 - Definição dos parâmetros utilizados para treinamento e teste do classificador ARTMAP *Fuzzy*.

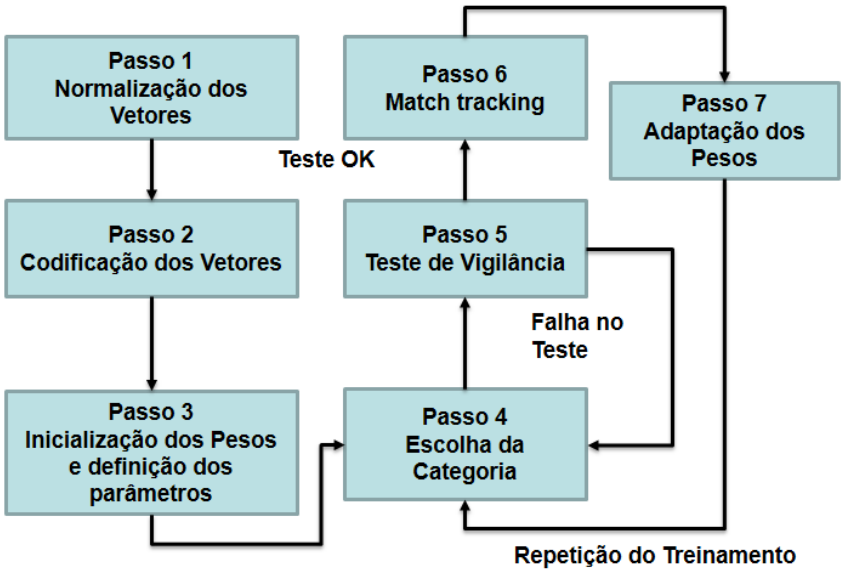
Parâmetros	Valor
Parâmetro de escolha ($\propto$)	0,001
Taxa de treinamento (β)	1
Parâmetro de vigilância da do módulo ARTa (ρ_a)	0,9
Parâmetro de vigilância da do módulo ARTb (ρ_b)	0,8
Parâmetro de vigilância da do módulo inter-ART (ρ_{ab})	0,9

Fonte: Elaborado pelo autor.

- Parâmetro de escolha - O valor foi definido empiricamente;
- Taxa de treinamento - O valor definido foi (01), pois visa um treino mais rápido e com menos ciclos de aprendizagem para a atualização dos pesos; e
- Parâmetro de vigilância de ARTa, ARTb e módulo *inter*-ART - O valor ajustado foi mantido próximo a um (01), para garantir a sensibilidade do classificador (HUANG; GEORGIOPOULOS; HEILEMAN, 1995).

O funcionamento do algoritmo da RNA ARTMAP *Fuzzy* está ilustrado na Figura 13.

Figura 13 – Fluxo de funcionamento do algoritmo da RNA ARTMAP *Fuzzy*.



Fonte: Elaborado pelo Autor.

O algoritmo utilizado como IDS para redes sem fio IEEE 802.11 foi desenvolvido no *software* MATLAB (MATLAB, 2015), os resultados obtidos foram considerados promissores quando avaliados junto ao conjunto de dados construído na pesquisa.

5.5 AVALIAÇÃO DO SISTEMA DE DETECÇÃO DE INTRUSÃO BASEADO NA RNA ARTMAP FUZZY

A performance do algoritmo de detecção de intrusão foi medida de acordo com a sua capacidade de classificação exata das atividades normais e anômalas e o tempo gasto no processamento. Os parâmetros usados na avaliação do IDS foram especificadas por uma matriz de confusão (WU; BANZHAF, 2010). Para obtenção de resultados mais fidedignos foi realizada a convergência de todos os resultados obtidos pelo IDS, possibilitando uma avaliação completa da ferramenta.

A matriz de confusão dada para o problema de detecção de intrusão considera os eventos normais como negativos (a classe que o sistema não está procurando e não aciona nenhum alarme). Por outro lado, os eventos anômalos são os positivos. A Tabela 08 mostra as taxas da matriz de confusão para o problema de detecção de intrusão.

Tabela 08 – Matriz de confusão.

		Classe Prevista	
		Classe Negativa (Normal)	Classe Positiva (Anomalia)
Classificação Real	Classe Negativa (Normal)	Verdadeiro Negativo (VN)	Falso Positivo (FP)
	Classe Positiva (Anomalia)	Falso Negativo (FN)	Verdadeiro Positivo (VP)

Fonte: Wu; Banzhaf (2010).

As métricas avaliativas da matriz de confusão são as seguintes:

- Verdadeiro Negativo (VN) - Atividade normal classificada corretamente pelo IDS. Dentro do contexto, o Verdadeiro Negativo é a detecção correta do tráfego normal da rede;
- Verdadeiro positivo (VP) - Atividade anômala corretamente classificada pelo IDS. Dentro do contexto, o Verdadeiro Positivo é a detecção correta de tráfego de rede anômalo causado por um ataque;
- Falso negativo (FN) - Atividade anômala classificada pelo IDS como atividade normal. Dentro do contexto, o Falso Negativo é a detecção incorreta do tráfego de rede normal como um ataque; e
- Falso positivo (FP) - atividade normal classificada pelo IDS como atividade anômala. Dentro do contexto, o Falso Positivo é a detecção incorreta de um ataque como atividade normal;

A eficiência do IDS avaliada pelos resultados obtidos a partir das taxas geradas pela matriz de confusão. As principais métricas são:

Exatidão Global: $$\left(\frac{\mathrm{VN+VP}}{\mathrm{VP+FP+VN+FN}}\right) \quad (21)$$

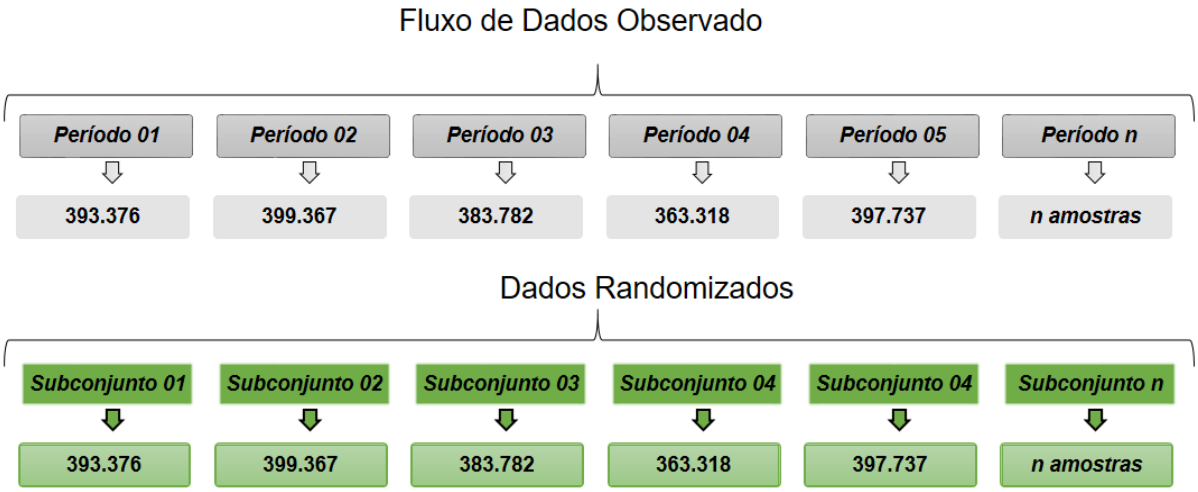
Taxa de detecção: $$\left(\frac{\mathrm{VP}}{\mathrm{VP+FN}}\right) \quad (22)$$

Taxa de falso positivo: $$\left(\frac{\mathrm{FP}}{\mathrm{VN+FP}}\right) \quad (23)$$

A taxa de exatidão global corresponde as predições classificadas corretamente pelo IDS. O cálculo desta métrica é a razão entre as previsões corretas e o total de observações. A taxa de detecção é a proporção das atividades anômalas classificadas corretamente. A taxa de falso positivo é a parte das atividades normais classificadas incorretamente como anômalas.

A metodologia utilizada para quantificar o número de amostras processadas pelo IDS durante o treinamento e teste foi em conformidade com o quantitativo de registros observados durante a etapa de análise da rede em 2019. O treinamento e os testes do classificador ARTMAP *Fuzzy* foi realizado em um *notebook* com processador Intel Core I7 e 16 GB de RAM. O IDS foi treinado e testado cento e sessenta e oito vezes (168), esse número corresponde ao quantitativo de pacotes observados a cada intervalo de sessenta (60) minutos. Para cada subconjunto avaliado manteve-se o número de amostras trafegadas naquele período, essa metodologia foi adotada para que o IDS processasse o mesmo número de pacotes que processaria em tempo real. Foi desenvolvido um *script* no *software* MATLAB que utiliza a função *randperm* para realizar a troca aleatória das amostras sem repeti-las. A proporção de registros utilizados no treinamento foi de setenta por cento (70,00%) e trinta por cento (30,00%) no teste. A Figura 14 mostra o número de amostras reproduzidas no treinamento e teste do IDS.

Figura 14 - Representação do número amostras reproduzidas no treinamento e teste do IDS.



Fonte: Elaborado pelo Autor.

A primeira métrica avaliada foi a taxa de exatidão global, que corresponde as predições classificadas corretamente pelo IDS. Os resultados obtidos para esta taxa foram superiores a 89%. As células em destaque na Tabela 09 correspondem a maior (verde) e menor (vermelho) resultado obtido pelo IDS. A Tabela 09 mostra os resultados obtidos pelo IDS para cada um dos cento e sessenta e oito (168) subconjuntos avaliados.

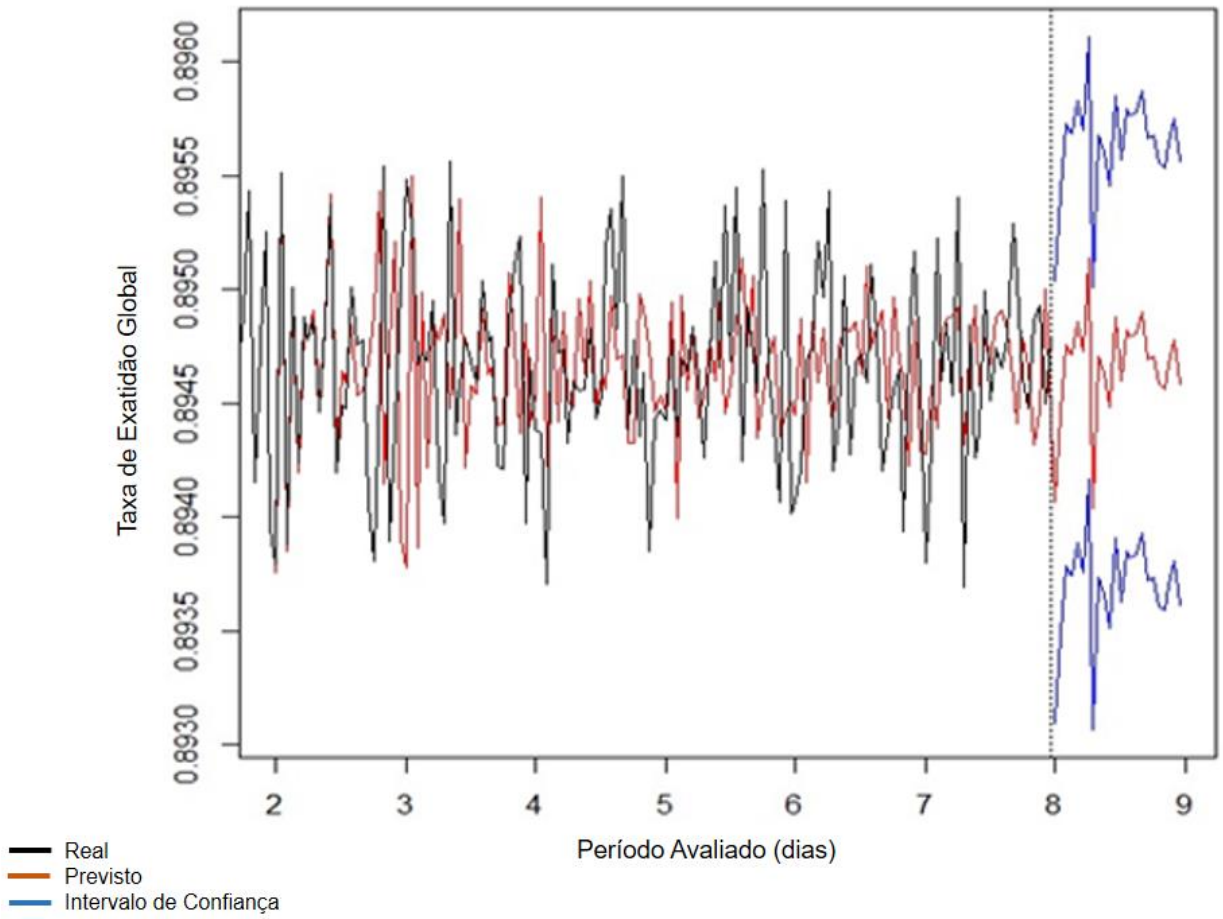
Tabela 09 – Taxa de exatidão global obtida pelo IDS em cada subconjuntos avaliado.

INTERVALO	EXATIDÃO GLOBAL									
[1-10]	0.89422	0.89553	0.89547	0.89478	0.89487	0.89437	0.89440	0.89493	0.89397	0.89480
[11-20]	0.89427	0.89482	0.89470	0.89463	0.89485	0.89451	0.89453	0.89465	0.89488	0.89543
[21-30]	0.89415	0.89476	0.89525	0.89395	0.89379	0.89551	0.89387	0.89500	0.89424	0.89487
[31-40]	0.89477	0.89487	0.89446	0.89483	0.89537	0.89419	0.89449	0.89447	0.89501	0.89475
[41-50]	0.89477	0.89405	0.89381	0.89463	0.89554	0.89389	0.89440	0.89502	0.89548	0.89528
[51-60]	0.89467	0.89472	0.89468	0.89495	0.89418	0.89397	**0.89556**	0.89436	0.89458	0.89478
[61-70]	0.89468	0.89459	0.89504	0.89477	0.89479	0.89422	0.89420	0.89485	0.89511	0.89523
[71-80]	0.89397	0.89470	0.89438	0.89436	0.89370	0.89510	0.89472	0.89473	0.89432	0.89459
[81-90]	0.89455	0.89456	0.89483	0.89443	0.89453	0.89518	0.89535	0.89482	0.89549	0.89438
[91-100]	0.89478	0.89435	0.89463	0.89385	0.89443	0.89447	0.89442	0.89477	0.89435	0.89470
[101-110]	0.89464	0.89483	0.89462	0.89426	0.89470	0.89512	0.89465	0.89536	0.89468	0.89544
[111-120]	0.89425	0.89492	0.89471	0.89454	0.89552	0.89464	0.89441	0.89406	0.89539	0.89401
[121-130]	0.89406	0.89421	0.89468	0.89474	0.89521	0.89496	0.89543	0.89420	0.89442	0.89505
[131-140]	0.89427	0.89468	0.89471	0.89459	0.89510	0.89481	0.89420	0.89438	0.89455	0.89465
[141-150]	0.89393	0.89477	0.89516	0.89460	0.89380	0.89431	0.89522	0.89460	0.89484	0.89453
[151-160]	0.89540	**0.89369**	0.89484	0.89425	0.89436	0.89499	0.89451	0.89474	0.89465	0.89479
[161-168]	0.89529	0.89503	0.89461	0.89447	0.89486	0.89493	0.89450	0.89479		

Fonte: Elaborado pelo Autor.

Também foi realizada uma análise preditiva das taxas de exatidão global obtidas pelo IDS. O *software* estatístico utilizado para gerar esta previsão foi o R, e a série temporal aplicada baseou-se no modelo aditivo de Holt-Winters. Os resultados demostram que as taxas de exatidão global obtidas pelo IDS não apresentam sazonalidade, isso significa que não haverá um padrão de repetição nos resultados da taxa de exatidão global. Os resultados dos valores previsto não foram afetados, isso significa que a série não apresentou tendência. O desvio padrão calculado foi de 0,000425, isso mostra que o IDS possui uma precisão adequada para medição da taxa de exatidão global, pois há um equilíbrio e estabilidade nas séries. A Figura 15 mostra os resultados da análise preditiva gerada pela série temporal estacionária de acordo com o modelo de Holt-Winters.

Figura 15 - Análise preditiva da Taxa de Exatidão Global do IDS.



Fonte: Elaborado pelo Autor.

Outras medidas avaliadas pelo IDS foram as taxas de detecção e falso positivo (WU; BANZHAF, 2010). Nesta etapa foi considerada a latência de processamento do IDS, a Tabela 10 mostra a taxa média dos resultados obtidos pelo IDS e tempo médio de processamento do IDS.

Tabela 10 - Taxa média dos resultados obtidos pelo IDS e tempo médio de processamento do IDS.

Métrica Avaliada	**Resultado**
Exatidão Global Média	89,46
Taxa de Detecção Média	98,90%
Taxa de Falsos Alarmes Média	1,20%
Tempo de processamento	44,33s

Fonte: Elaborado pelo Autor.

No geral, o IDS obteve bons resultados para o problema de detecção de intrusão em redes IEEE 802.11 em todos os 168 subconjuntos avaliados. A taxa média de detecção de anomalias do IDS foi de 98,90% e a taxa média de falso positivo foi inferior a 1,2%. A taxa de exatidão global média foi de 89,46%, no entanto, o IDS possui alta capacidade de detecção de intrusão. O IDS reconheceu a atividade intrusiva, porém não a classificou corretamente. Isso pode ter acontecido devido a presença de algum ruído no conjunto de dados, similaridade entre os ataques ou falta de representatividade de algum campo extraído do quadro MAC do IEEE 802.11. O conjunto de dados usado foi essencial na avaliação do IDS, no entanto, é necessário utilizar um método de seleção de atributos para extrair características que demonstrem o comportamento intrusivo existente para cada tipo de ataque categorizado. O tempo médio de processamento para cada subconjunto treinado e testado foi de 44,33 segundos, isso demonstra que o IDS proposto necessita de poucos recursos computacionais para o seu funcionamento.

6 CONCLUSÃO E TRABALHOS FUTUROS

As redes sem fio IEEE 802.11 possuem diversas vulnerabilidades, e os ataques de negação de serviço são uma das principais ameaças à sua segurança pois exploram justamente a falta de proteção dos quadros de gerenciamento e controle do protocolo MAC. Garantir a segurança absoluta de um ambiente de rede sem fio não é possível, porém ao adicionar mecanismos de proteção extra o risco de incidentes reduz. O uso de IDS é uma maneira de mitigar os riscos contra indisponibilidade de serviços. Para solucionar este problema foi desenvolvido um IDS baseado no modelo de rede neural artificial ARTMAP *Fuzzy*.

A pesquisa foi realizada em quatro etapas: seleção da rede sem fio IEEE 802.11; avaliação da rede IEEE 802.11 construção; padronização e pré-processamento do conjunto de dados; e resultados obtidos pelo IDS.

A escolha do cenário disposto em um ambiente real e com características advindas de sistemas IOT, foi essencial para a construção de um conjunto de dados representativo de redes sem fio IEEE 802.11 que operam em modo infraestruturado. Também serviu para dimensionar a proporção de amostras do tráfego normal e anômalo da rede distribuído em cada subconjunto avaliado pelo IDS.

Os resultados mostraram que o IDS é eficiente. A taxa média de detecção de eventos intrusivos obtida pelo IDS foi de 98,9% e taxa de falsos alarmes muito baixa. A taxa média de exatidão global foi de 89,46%, isso acontece quando a base está desbalanceada. Portanto, faz-se necessário realizar um novo processamento no conjunto de dados para extrair somente os atributos que determinam o comportamento do tráfego normal e anômalo. Evitando distúrbios que possam influenciar na capacidade de detecção correta das amostras. Apesar de ter sido desenvolvido para mitigar ameaças nas redes sem fio IEEE 802.11, o IDS é multi-plataforma, e pode ser treinado por outros conjuntos de dados.

O custo computacional requerido pelo IDS foi considerado baixo, o treinamento e teste dos cento e sessenta e oito (168) subconjuntos foram realizados em um computador de uso pessoal e que processou o total de 78.289.976 amostras. Sua capacidade de processamento médio é de mais de 500 mil amostras a cada 60 minutos.

De acordo com os resultados obtidos, os trabalhos futuros seguidos são sugeridos a seguir:

- Realizar um novo pré-processamento do conjunto de dados para avaliar atributos nulos e não representativos;
- Estratificar cada subconjunto de dados para regular a correspondência entre classificações anômalas;
- Realizar uma captura maior do conjunto de dados;
- Aplicar novos ataques;
- Construir um novo conjunto de dados com o protocolo de segurança WPA3 habilitado;
- Implementar o Classificador com treinamento continuado para funcionamento em tempo real.

REFERENCIAS

AGARWAL, Mayank *et al*. Intrusion detection system for PS-Poll DoS attack in 802.11 networks using real time discrete event system. **IEEE/CAA Journal of Automatica Sinica**, Piscataway, v. 4, n. 4, p. 792-808, 2016.

AHMAD, Md Sohail; TADAKAMADLA, Shashank. Short paper: security evaluation of IEEE 802.11 w specification. *In*: PROCEEDINGS ACM CONFERENCE ON WIRELESS NETWORK SECURITY, 4, 2011, Hamburg. **Proceedings of the** […]. Hamburg: [s.n.], 2011. p. 53-58.

AIRCRACK-NG. Disponível em: http://www.aircrack-ng.org/doku.php. Acesso em: 02 maio 2020.

AAZAM, Mohammad *et al*. Cloud of things: integration of IoT with cloud computing. *In*: KOUBAA, Anis; SHAKSHUKI, Elhadi (ed.). **Robots and sensor clouds**. Cham: Springer, 2016. p. 77-94.

BICAKCI, Kemal; TAVLI, Bulent. Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. **Computer Standards & Interfaces**, Amsterdam, v. 31, n. 5, p. 931-941, 2009.

BUCZAK, RNAa L.; GUVEN, Erhan. A survey of data mining and machine learning methods for cyber security intrusion detection. **IEEE Communications Surveys & Tutorials**, Piscataway, v. 18, n. 2, p. 1153-1176, 2015.

CARPENTER, Gail A. *et al*. *Fuzzy* ARTMAP: a neural network architecture for incremental supervised learning of analog multidimensional maps. **IEEE Transactions on Neural Networks**, Piscataway, v. 3, n. 5, p. 698-713, 1992.

CARPENTER, Gail A.; GROSSBERG, Stephen (ed.). **Pattern recognition by self-organizing neural networks**. Cambridge: MIT Press, 1991.

CARPENTER, Gail A.; GROSSBERG, Stephen. A massively parallel architecture for a self-organizing neural pattern recognition machine. **Computer Vision, Graphics, and Image Processing**, Maryland Heights, v. 37, n. 1, p. 54-115, 1987a.

CARPENTER, Gail A.; GROSSBERG, Stephen. ART 2: self-organization of stable category recognition codes for analog input patterns. **Applied Optics**, Washington, v. 26, n. 23, p. 4919-4930, 1987b.

CARPENTER, Gail A.; GROSSBERG, Stephen; REYNOLDS, John H. ARTMAP: Supervised real-time learning and classification of nonstationary data by a self-organizing neural network. **Neural Networks**, Oxford, v. 4, n. 5, p. 565-588, 1991.

CARPENTER, Gail A.; GROSSBERG, Stephen; ROSEN, David B. *Fuzzy* ART: fast stable learning and categorization of analog patterns by an adaptive resonance system. **Neural Networks**, Oxford, v. 4, n. 6, p. 759-771, 1991.

CHAKRABARTI, S.; CHAKRABORTY, Mohuya; MUKHOPADHYAY, Indraneel. Study of snort-based IDS. *In*: PROCEEDINGS OF THE INTERNATIONAL CONFERENCE AND WORKSHOP ON EMERGING TRENDS IN TECHNOLOGY, 2010, New York. **Proceedings of the** […]. New York: Association for Computing Machinary, 2010. p. 43-47.

CHATZOGLOU, Efstratios; KAMBOURAKIS, Georgios; KOLIAS, Constantinos. Empirical evaluation of attacks against IEEE 802.11 enterprise networks: the AWID3 dataset. **IEEE Access**, Piscataway, v. 9, p. 34188-34205, 2021.

CHOO, K-KR. The cyber threat landscape: challenges and future research directions. **Computers & Security**, Kidlington, v. 30, p. 719–731, 2011.

CHUDASMA, Pratik. **Network intrusion detection system using classification techniques in machine learning**. 2020. Thesis (Master) - Dublin Business School, 2020. Disponível em: https://esource.dbs.ie/handle/10788/4251. Acesso em: 18 set. 2021.

ČOLAKOVIĆ, Alem; HADŽIALIĆ, Mesud. Internet of things (IoT): a review of enabling technologies, challenges, and open research issues. **Computer Networks**, Amsterdam, v. 144, p. 17-39, 2018.

DE SOUZA ARAÚJO, Nelcileno Virgílio *et al*. Kappa-*Fuzzy* ARTMAP: a feature selection based methodology to intrusion detection in computer networks. *In*: IEEE INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS, 12, 2013, Melbourne. **Proceedings of the** […]. Melbourne: IEEE, 2013. p. 271-276.

GROSSBERG, Stephen. Adaptive pattern classification and universal recoding: I. Parallel development and coding of neural feature detectors. **Biological Cybernetics**, Heidelberg, v. 23, n. 3, p. 121-134, 1976a.

GROSSBERG, Stephen. Adaptive pattern classification and universal recoding: II. Feedback, expectation, olfaction, illusions. **Biological Cybernetics**, Heidelberg, v. 23, n. 4, p. 187-202, 1976b.

HEŠÍK, Radek. **Vliv DoS** (Denial of Service) útoků na veřejné Wifi sítě. 2013.
HUANG, Juxin; GEORGIOPOULOS, Michael; HEILEMAN, Gregory L. *Fuzzy* ART properties. **Neural Networks**, Oxford, v. 8, n. 2, p. 203-213, 1995.

IEEE 802.11 WORKING GROUP *et al*. Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher-speed physical layer extension in the 2.4 GHz band. ANSI/IEEE Std 802.11, 1999.

IEEE 802.11w: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: protected management frames. IEEE CS LAN MAN Standards Committee, 2009.

IEEE COMPUTER SOCIETY LAN MAN STANDARDS COMMITTEE *et al*. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. ANSI/IEEE Std. 802.11-1999, 1999.

IEEE LAN/MAN STANDARDS COMMITTEE *et al*. IEEE STD 802.11 i™-2004 (Amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003)). IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific Requirements, Part, v. 11.

IEEE Std 802.1X-2001 IEEE. IEEE Standard for Local and Metropolitan Area Networks‐Port-Based Network Access Control, June 2001.

JING, Qi *et al*. Security of the Internet of Things: perspectives and challenges. **Wireless Networks**, New York, v. 20, n. 8, p. 2481-2501, 2014.

KOLIAS, Constantinos *et al*. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. **IEEE Communications Surveys & Tutorials**, Piscataway, v. 18, n. 1, p. 184-208, 2015.

KUMAR, Deepak *et al*. All things considered: an analysis of IoT devices on home networks. *In*: SECURITY SYMPOSIUM (USENIX) SECURITY 19, 28, 2019, Santa Clara. **Proceedings of the** […]. Santa Clara: Usenix, 2019. p. 1169-1185. Disponível em: https://www.usenix.org/system/files/sec19-kumar-deepak_0.pdf. Acesso em: 18 set. 2021.

KUROSE, James; ROSS, Keith. **Computer networks**: a top down approach featuring the internet. [New York]: Peorsoim Addison Wesley, 2010.

LIAO, H-J. *et al.* Intrusion detection system: a comprehensive review. **Journal Network and Computer Applications**, London, v. 36, p. 16–24, 2013.

LIU, Xiong. A study on smart campus model in the era of big data. *In*: INTERNATIONAL CONFERENCE ON ECONOMICS, MANAGEMENT ENGINEERING AND EDUCATION TECHNOLOGY - ICEMEET 2016, 2, 2016, [New York?]. **Proceedings of the** […]. [New York?]: Atlantis Press, 2017. p. 919-922. Disponível em: https://www.atlantis-press.com/proceedings/icemeet-16/25869251. Acesso em: 18 set. 2021.

LIU, Yonglei; JIN, Zhigang; WANG, Ying. Survey on security scheme and attacking methods of WPA/WPA2. *In*: INTERNATIONAL CONFERENCE ON WIRELESS COMMUNICATIONS NETWORKING AND MOBILE COMPUTING -WICOM, 6, 2010, Niagara Falls. **Proceedings of the** […]. Niagara Falls: IEEE, 2010. p. 1-4.

LOPES, M. L. M. **Desenvolvimento de redes neurais para previsão de cargas elétricas de sistemas de energia elétrica**. 2005. 169 f. 2005. Tese (Doutorado Automação) - Faculdade de Engenharia, Universidade Estadual Paulista, Ilha Solteira, 2005. Disponível em: https://repositorio.unesp.br/handle/11449/100374. Acesso em: 18 set. 2021.

MATHWORKS, MATLAB. MATLAB documentation. 2015.

MDK3. Disponível em: https://en.kali.tools/?p=34. Acesso em: 02 maio 2020.

MOORE, Gordon E. *et al*. Cramming more components onto integrated circuits. **Proceedings IEEE**, Piscataway, v. 86, n. 1, p. 82-85, 1965.

PAHLAVAN, Kaveh; KRISHNAMURTHY, Prashant. Evolution and impact of *WLAN* technology and applications: a historical perspective. **International Journal of Wireless Information Networks**, New York, v. 28, n. 1, p. 3-19, 2021.

REDDY, S. Vinjosh. *et al*. Wireless hacking-a WiFi hack by cracking WEP. *In*: INTERNATIONAL CONFERENCE ON EDUCATION TECHNOLOGY AND COMPUTER, 2, 2010, Shangai. **Proceedings of the** […]. Shangai: IEEE, 2010. p. V1-189-V1-193.

R-STUDIO. Disponível em: https://rstudio.com/. Acesso em: 02 maio 2020.

SANDERS, Chris. **Practical packet analysis**: using wireshark to solve real-world network problems. [New York]:No Starch Press, 2017.

SANTOS JÚNIOR, Carlos Roberto dos. **Uma nova abordagem de treinamento on-line para rede neural ARTMAP *Fuzzy***. 2017. Tese (Doutorado em Automação) – Faculdade de Engenharia, Universidade Estadual Paulista, Ilha Solteira, 2017. Disponível em: https://repositorio.unesp.br/handle/11449/152033. Acesso em: 18 set. 2021.

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

TAMA, Bayu Adhi; RHEE, Kyung-Hyune. Classifier ensemble design with rotation forest to enhance attack detection of IDS in wireless network. *In*: ASIA JOINT CONFERENCE ON INFORMATION SECURITY, ASIAJCIS, 11, 2016, Fukuoka. **Proceedings of the** […]. Fukuoka: IEEE, 2016. p. 87-91.

VANHOEF, Mathy; PIESSENS, Frank. Key reinstallation attacks: Forcing nonce reuse in WPA2. *In*: ACM SIGSAC Conference on Computer and Communications Security, Dallas, 2017. **Proceedings of the** […]. Dallas: CCS', 2017. p. 1313-1328.

VILELA, Douglas 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. **Proceedings of the** […]. Bogota: IEEE, 2014. p. 1-5. Disponível em: https://repositorio.unesp.br/handle/11449/117644?locale-attribute=en. Acesso em: 18 set. 2021.

WU, Shelly Xiaonan; BANZHAF, Wolfgang. The use of computational intelligence in intrusion detection systems: a review. **Applied Soft Computing**, Amsterdam, v. 10, n. 1, p. 1-35, 2010.