WEVERTON DE SOUZA GOUVEIA
JOSÉ VIEIRA NETO

VULNERABILIDADES EM REDES WIRELESS: COM ESTUDO DE CASO DE PROTOCOLO DE SEGURANÇA UTILIZADO PELA MARINHA DO BRASIL

Ji-Paraná

2022

WEVERTON DE SOUZA GOUVEIA
JOSÉ VIEIRA NETO

VULNERABILIDADES EM REDES WIRELESS: COM ESTUDO DE CASO DE PROTOCOLO DE SEGURANÇA UTILIZADO PELA MARINHA DO BRASIL

Monografia apresentada á Banca Examinadora do Centro Universitário São Lucas, como requisito de aprovação obtenção do Título de Bacharel em Sistemas de Informação.

Orientador: Prof. José Rodolfo Milazzotto Olivas

Ji-Paraná

2022

Dados Internacionais de Catalogação na Publicação - CIP

G719v Gouveia, Weverton de Souza.

Vulnerabilidades em Redes Wireless: com estudo de caso de protocolo de segurança utilizado pela Marinha do Brasil. / Weverton de Souza Gouveia ; José Vieira Neto. – Ji-Paraná, 2022.
65 p.; il.

Monografia (Curso de Sistemas de Informação) – Centro Universitário São Lucas Ji-Paraná, 2022.

Orientador: Prof. Esp. José Rodolfo Milazzotto Olivas

1. Rede sem fio. 2. Segurança. 3. Vulnerabilidade. 4. Marinha do Brasil. 5. Internet. I. Vieira Neto, José. II. Olivas, José Rodolfo Milazzotto. III. Título.

CDU 004.7

Ficha Catalográfica Elaborada pelo Bibliotecário Giordani Nunes da Silva CRB 11/1125

WEVERTON DE SOUZA GOUVEIA

JOSÉ VIEIRA NETO

VULNERABILIDADES EM REDES WIRELESS: COM ESTUDO DE CASO DE PROTOCOLO DE SEGURANÇA UTILIZADO PELA MARINHA DO BRASIL

Ji-Paraná, 14 de junho de 2022.

Avaliação/Nota:

Monografia apresentada á Banca Examinadora do Curso Sistemas de Informação do Centro Universitário São Lucas, como requisito de aprovação obtenção do Título de Bacharel em Sistemas de Informação.

Orientador: Prof. José Rodolfo Milazzotto Olivas

BANCA EXAMINADORA

São Lucas Educacional Ji-Paraná

Prof. Esp. José Rodolfo Milazzotto Olivas

São Lucas Educacional Ji-Paraná

Prof. Esp. Romário Vitorino

São Lucas Educacional Ji-Paraná

Prof. Esp. Pablo Henrique Gonçalves Nascimento

Dedicamos este trabalho primeiramente a Deus, segundo aos familiares pelo apoio no decorrer do curso, e terceiro ao corpo docente de professores pela paciência e o comprometimento durante todo o curso.

AGRADECIMENTO

Dedico este trabalho primeiramente a Deus e em segundo a minha família, que me deu suporte em todos os desafios na minha vida pessoal e também na minha vida universitária ao longo desse curso. Tenho e sempre terei minha família como base, norte e fonte de sabedoria.

Aos que de alguma forma contribuíram para minha formação, desde um amigo próximo que começou essa caminhada universitária junto e terminará junto, até aquele que de alguma forma dividiu bons momentos e conhecimentos esporadicamente.

EPÍGRAFE

“A educação não transforma o mundo. A educação transforma as pessoas. Pessoas transformam o mundo”.
(Paulo Freire, 1979)

RESUMO

O presente trabalho busca analisar as vulnerabilidades de segurança ocorridas em redes Wireless, que, devido à expressiva adoção nas últimas décadas, apresentam diversas fragilidades, em grande parte por falta de cuidados dos próprios usuários. As redes de computadores, como a de dispositivos móveis, têm sido recorrentes alvos de ataques. O trabalho busca analisar de forma especifica a segurança de rede da Marinha do Brasil. Por mais que possuam diversos protocolos de segurança, os fraudadores estão cada dia mais audaciosos e utilizando técnicas novas para promover ataques. O estudo foi realizado por meio de revisão bibliográfica de artigos já publicados com diferentes abordagens. Ao final da pesquisa, concluiu-se que a maior causa de problemas relacionados a redes sem fio é a falta de protocolos confiáveis, assim como a negligência dos próprios usuários que, em diversos casos, não buscam utilizar protocolos mais seguros de acesso. No tocante a Marinha do Brasil a saída encontrada foi a adoção de um sistema próprio e mais seguro devido o tipo serviço que mesma presta, associado a defesa nacional.

Palavras-Chave: Rede sem fio. Segurança. Vulnerabilidade. Marinha do Brasil.

ABSTRACT

The present study seeks as vulnerabilities of running in wireless networks, which, due to the adoption of security in the decades, several researches, the last ones largely due to the lack of care of the users themselves. As computer networks, such as mobile devices, have been recurrent targets of attacks. The form analysis work specifies the network security of the Brazilian Navy. As much as they have several security protocols, fraudsters are increasingly audacious and using new techniques to promote attacks. The study was carried out through a literature review of articles already published with approaches. At the end of the research, it was concluded that most of the problem protocols were done wirelessly due to the lack of protocols, as well as a protocol related to the users themselves who, in cases, do not use safe protocols of use. Regarding the Brazilian Navy, the solution found was the adoption of its own system and more due to the type of service it provides, associated with national defense.

Keywords: Wireless network. Safety. Vulnerability. Brazil's navy.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

AES – Advanced Point

AP – Access Point

ARP – Address Resolution Protocol

AMPS – Asvanced Mobile Phone System

CRepSupEspCFN – Centro De Reparos e Suprimentos Especiais do Corpo de Fuzileiros Navais

DOS – Disk Operating System

DCTIM – Diretoria de Comunicações e Tecnologia da Informação da Marinha

FGV – Fundação Getúlio Vargas

GSM – Global System for Mobile Communications

IEEE – Institute of Eletrical and Electronics Engineers

LTE – Long Term Evolution

MB – MARINHA DO BRASIL

MIMO – Multiple input, multiple output

NBR – Norma Técnica brasileira

PA – Ponto de Acesso

PTK – Pairwise Transient Key

PDA – Personal Digital Assistant

RSSF – Rede de Sensores sem fio

TKIP – Temporal Key Integrity Protocol

OSI – Acrônimo do inglês Open System Interconnection

OSPF – Open Shortest Path First

SI – Segurança da Informação

SINGRA – Sistema Integrado de Gerenciamento do Abastecimento

SSID – Service Set Identifier

UMTS – Universal Mobile Telecommunications System, ou Sistema Móvel de Telecomunicações Universal)

WLANs – Wireless Local Area Network

WAP – Wi-fi Protected Access

WPA2 – Wi-Fi Protected Access2

WEP – Wired Equivalent Privacy

WECA – Wireless Ethernet Compatibility Alliance

WI-FI – Wireless Fidelity

Índice

1 INTRODUÇÃO

Diante da globalização e da evolução tecnológica principalmente da internet, a comunicação propiciou maior interação entre vários dispositivos, o computador se tornou uma peça fundamental. A evolução das redes de computadores nas ultimas décadas proporcionou de forma maciça a potencialização da comunicação através de diversos dispositivos, abrangendo não só dispositivos fixos, mas também dispositivos móveis (FIORILLO; CONTE, 2017).

O uso de cabos duplos ou fibras é considerado uma das maneiras mais eficiente de enviar dados, entretanto, vale ressalta que isso tem um custo alto de instalação conseqüentemente requer manutenção, além de outras variáveis como o número de *hosts* e a região a ser atendida. Outro problema identificado é a falta de viabilidade técnica e financeira de algumas regiões para sua instalação, dessa forma, devido a vários problemas ocasionados, surge à necessidade de novas formas que possibilite a conectividade. Nesse contexto as redes móveis conseguem suprir de forma eficaz essa demanda, oportunizando e flexibilizando de forma eficiente o alcance de uma rede (PINHEIRO, 2016).

O mundo atual utiliza a cada dia que se passa mais aparelhos móveis e portáteis que precisam de uma infraestrutura de rede. De acordo com o Centro de Tecnologia de Informação Aplicada (FGVcia), centro esse que faz parte da Fundação Getúlio Vargas (FGV EAESP), no ano de 2020 foram identificados aproximadamente 424 milhões de dispositivos digitais em funcionamento em todo o país, abrangendo: computadores, notebook, tablet e smartphone (FGV, 2020).

Além de que, o que diferencia a rede móvel da cabeada e a maneira de transmissão, propiciando uma instalação de forma simples ou até mesmo a adequação a rede que já existe. Contudo, estes aspectos em alguns casos podem gerar problemas, abrangendo o usuário, assim como os profissionais que exerce a atividade no segmento (BATISTA, 2017).

A segurança é considerada um fator preponderante e deve ser observado principalmente quando se adota a rede sem fio, ou seja, as redes moveis, até porque quando se trata de uma rede cabeada, o invasor precisa ter acesso a um ponto da rede. Entretanto, em relação a redes moveis a segurança do sistema precisa ser bem implementada necessitando vários protocolos que proteja a rede de

forma eficaz e segura, devido à transmissão de informação ser no ar, “livre” (SIMÃO; SUIADEN, 2012).

Dessa forma, facilitando para o invasor, por necessita apenas está na área de alcance do sinal transmitido por uma antena de acesso a comunicação da rede. Neste contexto o objetivo de trabalho é realizar uma revisão bibliográfica buscando identificar as principais falhas cometidas por usuários de redes moveis em relação a segurança, tendo como foco de analise a Marinha do Brasil.

A relevância do estudo está associada ao aumento do uso de redes móveis que tem gerando um grande impacto para o mercado tecnológico, financeiro, como também para a vida das pessoas, contudo, a segurança ainda tem sido questionada por haver uma certa vulnerabilidade no que tange a dados de usuários.

1.1 JUSTIFICATIVA

As redes móveis tem alcançado grande adesão nas ultimas décadas, devido a evolução da tecnologia da informação. Entretanto, sua implementação desorganizada e sem uma legislação especifica tem provocado diversos problemas a segurança de dados (SILVA, 2014).

Entre o grande fluxo de informações que circulam na internet, existem também diversos dados individuais das pessoas, sendo visto como a matéria-prima para inúmeras organizações criminosas. Somente em julho de 2015 foram identificados entorno de 175 mil tentativas de fraudes virtuais no Brasil, sendo uma a cada 15 segundos. O segmento que mais concentra esses números é o da telefonia móvel (G1, 2015, p.1).

Diante desse contexto, as redes são instaladas sem a mínima preocupação em relação a sua segurança, associado a falta de qualificação técnica, há também o próprio descuido das pessoas por não se preocupar com protocolos de seguranças, e tão pouco na atualização de seus dispositivos, com isso, métodos de segurança têm sido ainda considerado um desafio para redes móveis, contudo, com a evolução tecnologia a tendência é que esse cenário seja alterado.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL OU PRIMÁRIO

O objetivo geral deste trabalho é realizar uma revisão bibliográfica buscando identificar as principais falhas cometidas por usuários de redes moveis em relação a segurança. Tendo como foco de analisa a Marinha do Brasil.

1.2.2 OBJETIVOS ESPECÍFICOS OU SECUNDÁRIOS

De modo específico, esse trabalho busca:

- Contextualizar o nascimento das redes móveis
- Desenvolver, uma análise dos principais aspectos funcionais e procedimentos que abrangem a segurança em redes moveis;
- Identificar e citar os problemas que atinge a segurança das redes moveis;
- Identificar meio que traga segurança para redes moveis.

2 METODOLOGIA

Segundo Gil (2008), o método científico pode ser entendido como o caminho para se chegar à verdade em ciência ou como o conjunto de procedimentos que ordenam o pensamento e esclarecem acerca dos meios adequados para se chegar ao conhecimento. Nessa mesma linha Fachin (2010, p. 27), ressalta que o método "é a escolha de procedimentos sistemáticos para descrição e explicação do estudo".

2.1 TIPO DE PESQUISA

Para a realização deste estudo, em primeiro lugar foi definido o tipo de pesquisa, visando identificar as principais falhas cometidas por usuários de redes moveis em relação a segurança. Desse modo, será utilizado à metodologia de pesquisa bibliográfica. Como ressalta Severino (2007, p. 122) "a pesquisa bibliográfica é aquela que se realiza a parti do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses, etc". Neste contexto o procedimento bibliográfico se enquadra na presente pesquisa por utilizar livros, tese, dissertação e monografia de graduação.

Se caracteriza também como um estudo de caso, Marconi e Lakatos (2011), postulam que o estudo de caso tem como foco obter informações e conhecimentos sobre a questão pesquisada, onde se queira comprovar ou desvendar novos fenômenos ou relações, consiste na análise de acontecimentos espontâneos em decorrência da coleta dos dados ou variáveis que apresentam relevância.

O atual estudo teve uma abordagem qualitativa. Richardson (1999 apud BEUREN e RAUPP, 2004, p.92) aponta que: "Os estudos que empregam metodologia qualitativa podem descrever a complexidade de determinado problema, analisar a interação de certas variáveis, compreender e classificar processos dinâmicos vividos por grupos sociais".

2.2 INSTRUMENTO DE COLETA DE DADOS

No decorrer da pesquisa foram feitas buscas em diferentes portais eletrônicos por trabalhos recentes entre (2010 e 2021) em relação ao tema. Scielo, Google Acadêmico, o próprio Google foram usados como ferramentas, por meio deles foi possível ter acesso a inúmeras publicações disponíveis em diferentes sites. Buscando promover maior entendimento da pesquisa uso-se palavras chaves tais como: Rede sem fio, Segurança, Vulnerabilidade. Os artigos originais e de revisão, foram analisados pelo título e resumo, os que não se encaixarem serão excluídos.

2.3 TRATAMENTO E ANÁLISE DOS DADOS

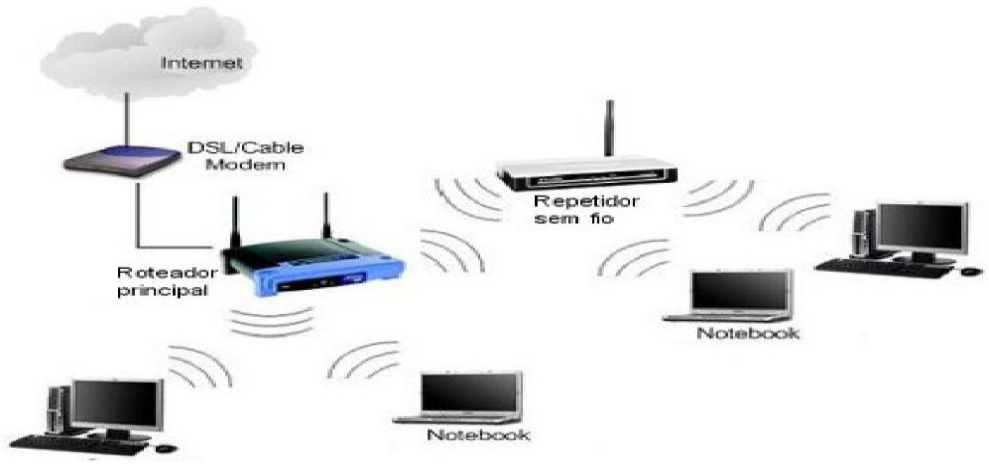
Após a seleção do material para a realização do trabalho, os dados foram tabulados e as informações analisadas à luz das teorias relacionadas ao tema. A análise também levará em consideração outras pesquisas na área. Dessa forma, foi possível promover um maior entendimento, por meio da análise e comparação entre inúmeros trabalhos encontrados, através da leitura. Vale ressalta que no mesmo período de análise outros trabalhos mais antigos foram encontrados, e referenciados, sendo utilizados bem como os trabalhos mais recentes de acordo com sua relevância.

3 REDE SEM FIO

O início da rede sem fio se deu pela a necessidade e desejo de possibilitar uma comunicação mais acessível a todos, que funcione em qualquer lugar 24 horas por dia possuindo um acesso ágil e permitindo a compartilhamento de arquivos. Neste contexto ao contrário do padrão físico, as redes sem fios não precisam de inúmeros equipamentos que as redes tradicionais necessitam, muito menos da grande estrutura em que uma rede convencional precisa (LEMOS; PASTOR; OLIVEIRA, 2012).

Nas ultimas década devido sua funcionalidade a *internet* se tornou uma ferramenta com várias funcionalidades, em primeiro lugar seu alcance é mundial, onde possui como um de seus maiores recursos a conectividade com vários dispositivos, sendo que por eles ocorrem um grande fluxo de informação, em que pesa sejam feitas através da utilização de protocolos, equipamentos esses chamados de hospedeiros ou programas finais. E diante do progresso e evolução que a *internet* alcançou, foram surgindo novos equipamentos e dispositivos tais como: servidores, mecanismos de buscas na *web*, *smartphone, notebooks, tablets* e TVs, todos esses dispositivos conectados à rede. Dessa forma, a internet se constitui como um sistema e uma arquitetura que hospede e dispõe de serviços e operações que são executadas nesses sistemas apresentados (KUROSE, 2013).

Figura 1: Rede sem fio com dispositivos Wireless



Fonte: Efetividade (2009) disponível em: < https://efetividade.net/2009/06/wireless-maior-alcance-para-sua-rede-sem-fio-com-um-repetidor-wi-fi.html>. Acessado em 21 de set de 2021.

Segundo Tanenbaum (2003) desde 1901 o físico Guglielmo Marconi já iniciará projetos que visaram o atual sistema de comunicação das redes sem fio, e o primeiro experimento foi feito por meio do telégrafo sem fio onde dava um suporte a comunicação, que era realizado entre um navio e uma central que localizada no litoral por meio de código Morse, e podemos afirmar que:

> "O Código Morse pode ser visto como uma forma de código digital, já que é binário: ou há o pulso ou não. Por exemplo, podemos usar uma lanterna para nos comunicarmos em Morse apenas ligando ou desligando o facho de luz nos tempos certos. Se tivermos apenas o som de um apito, podemos nos comunicar em Morse fazendo diferentes variações do tempo do apito" (CELI, 2019, p. 2).

De acordo com Engst e Fleishman (2005), já na década de 90 as primeiras redes sem fios ganham maior expressão, porém, naquela época tinha como meio de transmissão em ondas de rádio, período esse marcado pela evolução dos processadores que tiveram maior desempenho propiciando a aplicação do sistema.

Por haver uma falta de compatibilidade em padronizações que havia em torno das redes sem fios, onde existia inúmeras empresas com várias patentes diferentes trabalho no segmento, esse fato trazia muito desconforto e impossibilidade de progresso, diante dessa situação no final da década de 1990, mais precisamente em 1999, algumas empresas que possuía um grande mercado resolveram se unir e buscar um consenso para promover uma compatibilidade nos sistemas, assim surgiu à união de empresas como: *3Com, Nokia e Lucent Technologies*, que posteriormente seria denominada como WECA (*Wireless Ethernet Compatibility Alliance*), e que no ano de 2003 foi intitulada *Wi-fi Alliance*, nomenclatura que possibilitou o surgimento no nome Wi-fi (STEFANUTO, 2016).

Para Jasper (2010) as redes sem fio possuem uma ligação muito próxima com computador móvel, entretanto, a uma distância que a ela e atribuída devido sua utilização. O autor ressalva que a computação móvel consiste na possibilidade dos consumidores poder estarem conectados por mais que esteja em movimento, em contra partida as redes sem fio possuem como maior finalidade ser utilizada de forma que não necessite de cabo.

Com a disseminação da tecnologia wireless, várias tecnologias surgiram, para Tanenbaum (2003, p. 25) relata como um exemplo o Parquímetros como sendo

equipamento que permite que cartão de crédito seja aceito, além de da identificação em tempo real pelo link sem haver nenhum cabo conectado. Essa tecnologia tem capacidade de identificar se um veículo está em um determinado local e até mesmo quando irá sair, sem a necessidade de haver um dispositivo fixo, tendo a praticidade de gerar maior segurança e fiscalização em um pátio de automóveis, e conseguintemente promover um controle em relação a vagas.

Segundo Rufino (2019) há uma grande confusão em relação a chamando wi-fi com o termo wireless, várias pessoas tendem a pensar que são a mesma coisa. Porém a conexão wi-fi tem origem do padrão 802.11 definido pela IEEE (*Institute of Eletrical and Electronics Engineers*) aprovado no fim dos anos noventa. Essa conexão e realizada tendo ponto específico cabeado onde entrega o sinal da rede de internet pelo ar.

3.1 REDE MÓVEL

A rede móvel é considerada um tipo de rede de comunicação, pois engloba todas as redes disponíveis para as operadoras de telefonia celular no Brasil e no mundo, e é projetada principalmente para permitir a prestação de serviços de telefonia móvel, permitindo que os clientes tenham maior mobilidade com seus dispositivos através do uso de comunicação sem fio.

3.1.1 REDE 1G

A primeira rede móvel surgiu em meados da década de 80. Funcionava por meio de um sistema analógico sendo o AMPS (*Asvanced Mobile Phone System*) como o modelo mais conhecido, possuindo uma velocidade que assemelhava a rede discada (BERGHER, 2019. p. 1). É importante ressalta que naquela epoca não havia celulares como os de hoje em dia, dessa forma, a rede 1G era utilizada em particular para aparelhos eletrônicos instalados em veículos automotores, sendo que cada aparelho possui cerca de um quilo, tendo um cumprimento de cerca de 30 cm. Ou seja, sem a mínima possibilidade de levado no bolso. Além do uso da rede para comunicação militar.

3.1.2 REDE 2G

A segunda geração chamada 2G surgiu em meados da década de 1990, tendo como maior destaque a implementação do sinal digital, vale ressaltar que devido sua eficiência essa rede está em funcionamento até hoje até nos dias de hoje. Essa rede usa em especial o GSM (*Global System for Mobile Communications*) sendo considerado um dos recursos mais consolidados da comunicação, por disponibilizar os recursos básicos para as operadoras. Entretanto, em relação a internet móvel, a 2G já não consegue acompanha a demanda, ou seja, é considerada obsoleta (SANTINO, 2013). Portanto:

> "O 2G tomou forma lá pelos anos 90 e permitiu, principalmente, a troca de mensagens de texto e fotos via SMS. Mas o foco era a conexão de voz, falar e ser ouvido no telefone sem a necessidade de existir uma conexão com a internet" (CRUZ, 2018.p. 1).

A tecnologia GSM foi desenvolvida buscando proporcionar soluções para o problema de incompatibilidade que era visto no 1G durante o período da década de 1980, países europeus vendo essa dificuldade buscaram medidas que solucionasse essa falha, porém, foi somente em 1991 que o projeto foi adiante e ocorreu a primeira ligação realizada na rede. "Foram criados padrões para todos os fabricantes se juntarem, para que falassem a mesma língua e tivessem compatibilidade de qualquer tipo de aparelho em redes pelo mundo inteiro. Foi uma grande revolução", ressalta o especialista de computadores e professor, Luís Mateus (ROMER, 2013, p.02).

3.1.3 REDE 3G

A terceira geração (3G) ainda é uma das mais utilizadas atualmente, em todo o mundo, marcada por oferecer uma maneira mais eficaz de se navegar na *internet*, incluindo redes sociais, além de ser usada para *smartphones* em atividades diárias como a conversação *volp*, sendo possível comunicação por vídeo, mensagens de *e-mail*, assim como troca de mensagens instantâneas. Essa tecnologia inicialmente começou a ser usada em localidades do Japão, em regiões Chinesas e no Continente europeu por meio do sistema UMTS (Universal *Mobile*

Telecommunications System, ou Sistema Móvel de Telecomunicações Universal) chegando a disponibilizar pela primeira vez velocidade que alcançava *megabits* a cada segundo (ROMER, 2013).

Segundo Cruz (2018) por meio de uma visão técnica a rede 3G funciona buscando promover a transmissão de dados de voz, como por exemplo, áudio de aplicativos de mensagens e atividades na *internet* com a navegação de *sites*, ou para *downloads* assim como para a utilização de aplicativo *online*. Resumindo é uma conexão que possui maior velocidade do que a do 2G.

3.1.4 REDE 4G

A 4G por sua vez conhecida também com LTE (*Long Term Evolution*) se configura com a quarta geração, surgiu inicialmente em 2009 na Suécia, porém devido sua eficácia hoje já se encontra em cerca de mais de 205 países no mundo, possuindo uma abrangência de mais de 78% da população mundial (BRAGA, 2018).

No Brasil cerca de 4.197 municípios, ou seja, cerca de (75%) já utilizam a rede. Tendo como maior destaque, além da velocidade, ela possibilita que um número maior de pessoas se conecte a ela sem deixar de entregar qualidade em seu sinal (CRUZ, 2018).

Segundo especialista do segmento a rede 4G marca de forma preponderante a era da comunicação:

> “O usuário deixar de aceitar uma banda de transmissão menor para se ganhar a mobilidade, o que acontece até a geração anterior, para passar a exigir ambos em seus dispositivos: portabilidade e banda larga. “Hoje alguém com um tablet não aceitará que a velocidade de acesso á internet seja inferior aquela obtida em casa. A pessoa não vai ligar a mobilidade á nenhum tipo de ônus” ressalta o professor e especialista em rede de computadores Luiz Mateus’ (ROMER, 2013, p. 2).

Dessa forma, fica evidente que a rede 4G possui inúmeros benefícios comparada as redes anteriores, possibilitando uma melhora significativa na interação entre pessoas, por possibilita que mais dispositivos possam ser conectados.

3.1.5 REDE 5G

Segundo Cruz (2018) a 5G é considerada a *internet* do futuro tendo como objetivo torna a conexão bem mais veloz possuindo uma qualidade já mais vista, sendo possível conectar a diversos outros tipos de equipamentos, dispositivos e até veículos.

De maneira resumida a quinta geração conhecida com 5G tem como propósito entregar maior velocidade superior a 4G, além de diminuir as interrupções, disponibilizar maior estabilidade e permiti a interação de mais dispositivos sendo conectado em tempo real ao mesmo tempo (POZZEBOM, 2018).

Segundo a professora de estratégia *mobie* Samantha Carvalho a 5G possibilitará:

> “Pagamento de contas, pedidos de comida, transporte e mensagens. Tudo acontece pelo smartphone. Esse comportamento está forçando marcas e empresas a qualificarem a experiências que oferecem aos seus clientes no meio móvel” (CRUZ, 2018, p. 2).

Portanto devido a essa evolução que possibilitou um aumento bem significativo nas taxas de *download* diversas funcionalidade que até então dependia de redes fixas, passaram ser usadas também em dispositivos que possui acesso a redes moveis, que englobam a navegação na *internet*, a troca de *e-mail*, a própria rede sociais, e em especial operações que precisam de uma grande taxa de transmissão, sendo possível destaca a transmissão de um vídeo que possui alta definição sendo transmitido de forma *online*. Contudo, aliado tudo isso, há um problema bastante recorrente nos últimos anos, a segurança dos dados transmitidos, que requer ainda desenvolvimento de programas que sejam mais eficazes.

3.2 SEGURANÇA DA INFORMAÇÃO

Segundo a NBR ISO/IEC 17799 (2005) a SI (Segurança da Informação) é conceituada como: sendo o sistema de proteção presente sobre dados e informações pertencente a uma específica empresa de diversos ameaças para assegura o prosseguimento das atividades empresárias, diminuindo riscos,

potencializa o retorno em relação a investimentos e as possibilidades de novos negócios. Sendo ela protegida para a utilização restrita ou aberta para o uso público para informações ou obtenção.

Dessa forma segunda as normas relatadas acima, é preciso determinar padrões para estabelecer um nível se segurança que se busca alcançar, por meio de análises constantes permitindo o progresso ou retrocesso no campo da SI (segurança da Informação) na instituição.

Promover melhorias no sistema de segurança da informação não constitui somente em colocar um antivírus em um conjunto de computadores, ou utilizar bloqueios de proteção (firewalls) integradas em rede dos computadores em uma empresa. Contudo para adquirir um sistema de segurança de informação e preciso compreender os aspetos de segurança para que possa elabora medidas adequadas para suprir as carências de cada tipo de instituição.

Nesse contexto a segurança de uma rede só é identificada após sanar todas as falhas, ou seja, verificar as vulnerabilidades que o sistema possui para que terceiros não tenha acesso, não viole nem cometa adulterações após a quebra de senha (RUFINO, 2005).

Segunda Silva (2003), existem cinco pontos essências que são considerados fundamentais para implementação da segurança da informação que são:

Quadro 1: Pontos fundamentais de implementação da SI

1. **A relação custo e benefício:** assegura investimentos para práticas e assistências oportunas, sendo o retorno que possibilita a conservação e proteção do sistema de informação;
2. **O princípio da concentração**: Permite a possibilidade para coordenar ações precisas de segurança da informação, buscando suprir as carências promovendo melhoras de segurança de distintas bases de dados vulnerável a alterações;

3. **O princípio da proteção em profundidade:** possibilita ações protetivas de segurança sendo elas físicas ou lógicas, por meio de câmeras de vigilância, na utilização da biometria e através de reconhecimento de voz ou até mesmo fácil.
4. **O princípio da consistência**: estabelece que ações de proteção a segurança da informação tenha um gral de vulnerabilidade permutável para que possa diminuir o risco de falhas dos programas de segurança de instituições.
5. **O princípio da redundância**: estabelece a necessidade que haja mais de um sistema de proteção da segurança da informação. Assim quando ocorrer um problema do sistema A o B e acionado, mantenha a funcionalidade do sistema.

Fonte: Silva (2003)

Neste contexto apresentado acima devemos observar que se trata de 5 camadas de proteção em que implementadas acarretarar em um nível de proteção maior a empresa e ao usuário, colaborar ou terceiros.

3.2.1 COMPONENTES DE UMA REDE SEM FIO

O funcionamento da rede sem fio é feita pela a comunicação por meio de onda que se difundem no ar tendo um ponto de acesso de referência, deste modo ao haver o processo de envio de dados ocorre a conversão para sinais de rádio onde são transmitidos. Em relação a recebimento de dados e informações o roteador interpreta o sinal e promove a decodificação das informações sendo elas para sinal de rádio e remete para o dispositivo (BRAIN; JOHNSON, 2001).

3.2.2 BENEFÍCIOS DA REDE SEM FIO

A forma de comunicação que a rede sem fio propicia possibilita que seja bem usável devido sua praticidade no cenário atual, sendo principalmente devido a seu baixo custo somado a um aumento significativo de sua eficiência.

A rede sem fio apresenta quatro benefícios essências aos consumidores segundo Silva (2018), que são:

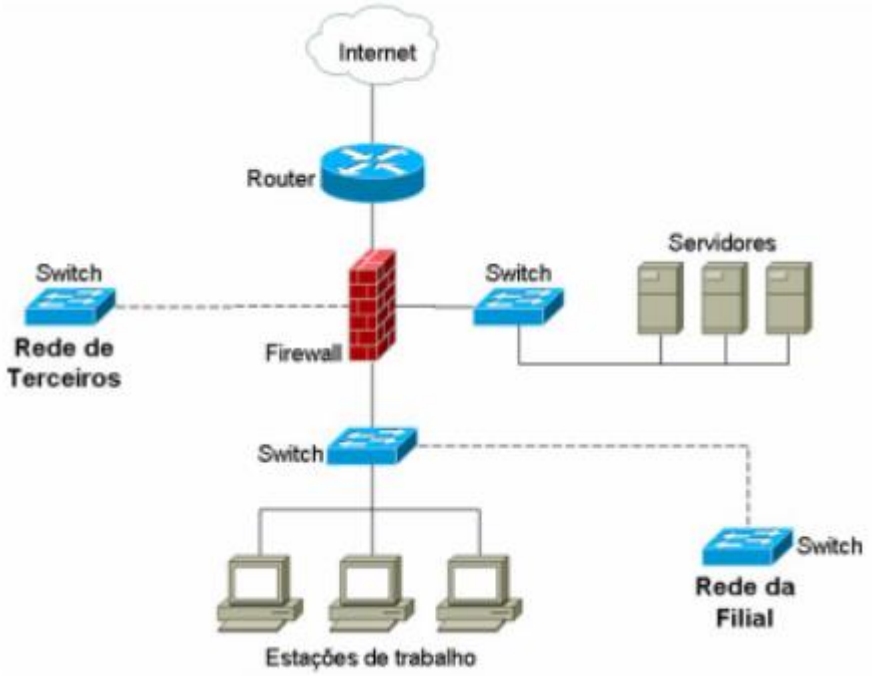
- Flexibilidade a seus usuários – O consumidor possui a flexibilidade de acessa a dados e informações, sem precisar fazer uso de cabos. Ainda é possível estar em movimento e possuir o acesso em tempo real, com alta velocidade de acesso.
- Ágil Instalação – Devido não haver a necessidade de cabeamentos externos a instalação se torna mais accessível por não ter que passar cabeamentos por paredes.
- Versatilidade – por não requere de cabos caso necessite fazer teste e possível sem muitos problemas por poder utilizar outros locais e áreas. De acordo com a necessidade.
- Escalabidade – Quando se fala em rede sem fios, e permite que ocorra configurações onde podem serem utilizadas em pequenas redes por meio de ponto a ponto, ou até mesmo utilizando grandes redes para efetuação de testes, onde sofre com alterações frequentes.

Devido a tanta praticidade a rede sem fio se tornou um mecanismo muito flexível em relação a redes cabeadas, dessa forma, organizações públicas como privadas tem feito o uso desse sistema onde permite o acesso a internet por meio da rede sem fio.

4 SEGURANÇA DE REDE

Quando surgiu a rede de computadores, a segurança era utilizada exclusivamente para partilhar recursos, a impressora era um exemplo onde inúmeros computadores tinha acesso a ela, diante desse contexto a segurança não solicitava cuidados mais relevantes, entretanto com o passar do tempo e com a evolução tecnologia hoje são milhares de indivíduos que acessam dados de inúmeras pessoas por meio da rede, principalmente para operações bancarias, aquisições de produtos, entre outras diversas funcionalidades possibilidades essas que são ofertadas pelas redes que funcione sem necessitar sair de casa (TANENBAUM, 2003). A figura abaixo ilustra a segurança de rede.

Figura 2: Segurança de rede de computadores



Fonte: Escobar (2012) disponivel em: <https://slideplayer.com.br/slide/5617047/>. Acessado em: 21 de set de 2021.

Alguns padrões são considerados fundamentais para as redes sem fio entre eles, Miranda (2013) destaca:

- 802.11a
  E capaz de atingir velocidade de 54 Mbps em relação aos padrões da IEEE 2

chega a 72 a 108 Mbps quando são fábricas sem a padronização exigidas. Rede esse que funciona na frequência de 5 GHz onde consegue atender até 64 usuários a cada Ponto de Acesso (PA). Tendo como maior vantagem a velocidade, além de suafrequência ser gratuita e não haver interferência. Sua desvantagem se encontra na incompatibilidade em relação a padrões associado ao Access Points 802.11b e g, já no que diz respeito a consumidores, o padrão 802.11a oferece compatibilidade para 802.11b e 802.11g em grande parte dos casos, onde vem se constituindo como um padrão de fabrica dos equipamentos (MIRANDA, 2013).

- 802.11b

Esse padrão consegue atingi velocidade de 11 Mbps seguindo os padrões da IEEE chega a uma velocidade de 22 Mbps, ofertas por fabricantes que não possui uma padronização. Funciona na frequência de 2.4 GHz. Atende até 32 usuários em cada ponto de acesso (PA). Sua desvantagem constitui na alta interferência que abrangem a transmissão assim como a recepção do sinal, devido opera a 2,4 GHz proporcional a telefones móveis, aparelhos de micro-ondas e dispositivos *Bluetooth*. Já os fatores positivos se encontram no custo baixo de seus dispositivos, a dimensão de banda grátis, assim como sua oferta que corresponde a gratuidade em todo o mundo. Esse padrão tem grande mercado por ser provedores de internet sem fio (MIRANDA, 2013).

- 802.11g

E baseado em sua compatibilidade em relação a 802.11b ofertando uma velocidade de 54 Mbps. Opera com uma frequência de 2,4 GHz. Possui as mesmas desvantagens em relação ao padrão 802.11b, ou seja, a falta de compatibilidade com dispositivos de fabricantes distintos. Em relação a vantagens podem ser apresentadas como as velocidades. Utiliza a autenticação por meio da WEP (*Wired Equivalent Privacy*) estática. Entretanto a uma grande dificuldade para realizar sua configuração, como *Home Gateway* por sua frequência ser de rádio além de outros sinais (MIRANDA, 2013).

- 802.11n

Padrão esse que por sua vez possui uma banda que chega até 300 Mbps e atinge 70 metros. Funciona com uma frequência de 2,4 GHz e 5 GHz. Sendo considerado um padrão novo e que possui tecnologia diferenciada, MIMO (multiple input, multiple output) sendo identificada pela utilização de diversas Atenas para a

transferência de dados de um lugar para outro. Tendo como ponto fonte a tecnologia aplicada e o aumento considerável que possibilitou maior expansão da banda e o alcance que possibilita (MIRANDA, 2013).

Figura: 3 Visão geral em relação aos padrões da tecnologia sem fio

Padrão	Taxa máxima de transmissão	Frequência	Compatibilidades
802.11a	54 Mbps	5 GHz	Não
802.11b	11 Mbps	2.4 GHz	Não
802.11g	54 Mbps	2.4 GHz	802.11b
802.11n	600 Mbps	2.4 GHz ou 5 GHz	802.11b/g
802.11ac	1.3 Gbps	2.4 GHz e 5.5 GHz	802.11b/g/n
802.11ad	7 Gbps	2.4 GHz, 5 GHz e 60 GHz	802.11b/g/n/ac

Fonte: Infortic (2018) disponível em: <https://inforticsite.wordpress.com/tipos-de-padroes-de-redes-wireless/>. Acessado em: 21 de set de 2021.

Na tabela podemos observar um comparativo entre os padrões 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad em que se apresenta suas taxa de transmissão, frequência e compatibilidade.

4.1 ATAQUES DE REDE SEM FIO

Devido a grande funcionalidade as redes de computadores possuem como base as tecnologias wireless onde se tornaram uma realidade para inúmeras organizações, sendo reconhecida como um recurso muito eficiente. Contudo, as redes sem fio possuem diversas fragilidades onde tem seu início no conceito de métodos adotados.

Diferente das redes cabeadas, a chamada rede sem fio tem sua transmissão baseada em um ponto cabeado que retransmitem o sinal onde quem está no raio de sinal pode ser favorecido pelo sinal independente quem seja, caso não tenha uma chave de segurança segura, neste sentido sendo vista como vulnerável devido não ter controle a quem tem o acesso.

Grande parte dos ataques realizados em rede sem fio consiste na aquisição

de dados e informações sem permissão, acessos sem autorização e ataques a negação referente a serviços. Vale ressalta que tais ataques podem diferenciar dependendo de como foi configurada a rede, Tanenbaum e Wetherall (2011, p. 530) salientam que:

> "Quase toda semana, lemos nos jornais notícias sobre problemas de segurança de sites. A situação é bastante séria [...] Primeiro, a home Page de inúmeras organizações é atacada e substituída por nova *home Page* escolhida pelos crackers. [...] Na maioria dos casos, os crackers simplesmente colocavam algum texto engraçado, e os sites eram arrumados dentro de algumas horas. [...] Diversos sites foram derrubados por ataques de negação de serviço, nos quais, o cracker inunda o site com tráfego, tornando-o incapaz de responder a consultas legítimas. Com frequência, o ataque é montado a partir de um grande número de máquinas que o cracker já invadiu. [...] Esses ataques são tão comuns que já não geram mais notícias, mas podem custar ao site atacado milhares de dólares em negócios perdidos."

Segundo Gomes e Neto (2001), existe uma trajetória bem elaborada antes que aconteça um ataque, devido existe alguns protocolos básicos de acesso, a um caminho que o invasor planeja antes de invadir o sistema que pese na identificação dos pontos mais vulneráveis, ou seja, explorar as fraquezas que fazem parte do ambiente de rede sendo possível serem vista na:

- Suspensão: A mensagem e interrompida ante de chegar ao destinatário final;
- Alteração: As informações ou dados são modificados;
- Produção: São geradas informações sem veracidade, ou seja, falsas.

Portanto pode ser entendido que para que uma rede sem fio seja capaz de ter o mesmo nível de segurança da rede cabeada, e preciso que contenha procedimentos e protocolos para a autenticação de dispositivos e sigilo de dados.

4.1.1 TIPOS DE INVASORES

Existem diversos tipos e formas que oportunizam rede serem atacadas por invasores segundo Melo; Rhoden e Westphall (2012), a maioria dos sistemas computacionais podem obter algum tipo de invasão originado por fragilidades e erros de protocolos referente a configuração, sendo possível a longo prazo ser explorado para inúmeros fins, chegando até a gerar riscos aos sistemas.

> Os ataques às redes sem fio são novos. Ao invés disso, eles são baseados em ataques anteriormente descobertos em redes guiadas. Alguns destes ataques não sofrem nem uma modificação, já outros sofrem algumas modificações para que possam ser disparados e obter melhores resultados. Na realidade, o objetivo dos ataques não é comprometer a rede sem fio, mas sim ganhar acesso ou comprometer a rede guiada (DUARTE, 2003, p. 38).

Na tabela 1 abaixa demonstra os tipos de invasores que mais são frequentes em redes de computadores segundo Tanenbaum; Wetherall, (2011, p. 479.).

Tabela 1: problemas de segurança

Adversário	**Objetivo**
Aluno	Tem como maior objetivo apenas observar as mensagens recebidas em relação a outras pessoas;
Cracker	São motivados por realizar testes de segurança ou até mesmo a aquisição de dados indevidos;
Representante de vendas	Motivados por representar várias regiões dentro de seu mercado e não apenas uma região;
Executivo	Motivados por tentar desvendar as estratégias que os concorrentes utilizam em seu mercado;
Ex-funcionário	Motivados por promover algum tipo de injustiça e tenta afetar a empresa que o despedido;
Contador	Motivado por ações ilícitas entre elas desviar recursos financeiros;
Corretor de valores	Contrapor uma proposta de um cliente através de uma mensagem recebida via e-mail;
Vigarista	Furtar números de cartões de créditos e vendê-los para fins inapropriados;
Espião	Descobrir informações militares e empresarias sigilosas de um adversário.
Terrorista	Surrupiar informações de equipamentos militares e biológicos.

Fonte: Tanenbaum; Wetherall (2011, p. 479.)

4.1.2 ASSOCIAÇÃO ACIDENTAL

O acesso não autorizado a redes sem fio e com fio da empresa pode vir de

diversos números e com diferentes métodos e intenções. Buscando promover mover flexibilidade aos usuários, diversos dispositivos possuem configurações autônomas, dessa forma, a grande possibilidade que ocorra uma associação acidental em outros dispositivos, mesmo sem a permissão e liberação do usurário.

A vários locais que ocorrem essa associação entre elas pode ser citados estabelecimentos que possui redes sem fios como restaurantes, e bares. Caso ocorra uma rede corporativa que possua um sinal aberto sem protocolos de acesso, de maneira geral o cliente terá acesso a essa rede, associando a mesma. Há países que consideram tais acessos como uma violação de espaço cibernético (*cyber tresspassing*) o usurário que usa tais redes privadas, mesmo que não saiba, é considerado um “invasor” (NAPOLITANO, 2019).

4.2 ASSOCIAÇÃO MALICIOSA

“Associações maliciosas” são quando dispositivos sem fio podem ser ativamente feitos por *crackers* para se conectar a uma rede da empresa através de seu *laptop* (computador portátil), nesta forma de ataque o invasor ajusta sua placa de rede sem fio para operar se maneira que seja um ponto de acesso (PA).

Em geral buscam lugares que possui grande aglomeração de pessoas, entre eles shoppings e aeroportos, e após aguardo o usuário entrar na rede para realizar o acesso, assim de forma invisível tem seus dados e passos monitorados pelo infrator, após sua navegação na internet (VACCA, 2016).

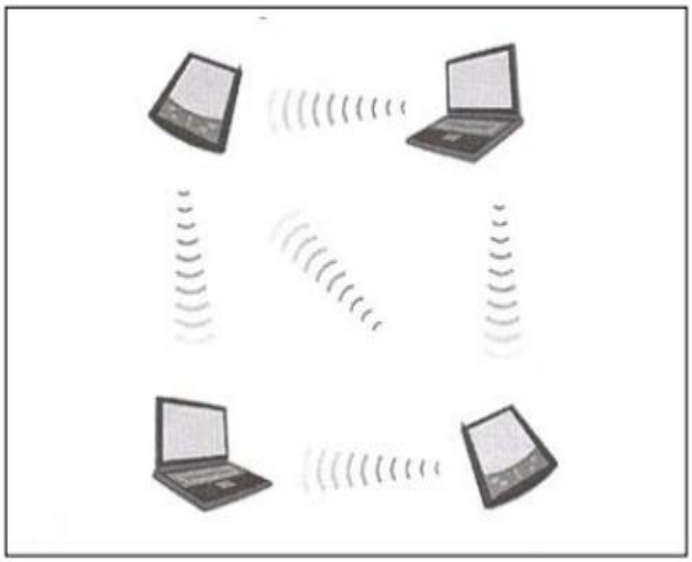
4.3 REDES AD-HOC

Os ataques realizados a redes *ad hoc* sem fio em sua grande maioria e separado em dois aspectos que abrangem os passivos e os ativos: Os ataques realizados de forma passiva não abalam o funcionamento da rede, onde apresenta como maior característica a espionagem de dados, porém sem afetá-los. Em relação a ataques ativos o risco aumento devido haver a criação e alteração de dados, além de rejeita ou impossibilita a utilização de dados em circulação.

Nesse contexto a quantidade de ataques ativos e bem maior, tendo a capacidade de agir em diversas camadas do modelo OSI. Vale ressalta que tais

ataques podem variar dependendo do acesso que o criminoso possuir a rede (MURTHY; MANO, 2004).

Figura 4: Topologia de rede modelo Ad-Hoc

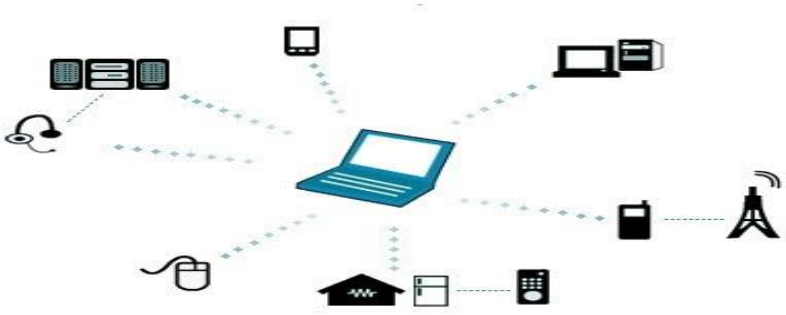


Fonte: Rufino (2005) disponível em: <https://s3.novatec.com.br/capitulos/capitulo-9788575222430.pdf>. acessado em: 21 de set de 2021.

4.5 REDES NÃO TRADICIONAIS

Redes não tradicionais, como: dispositivo *Bluetooth* de rede pessoal, não são seguras de rachaduras e deve ser considerado como um risco de segurança. Mesmo leitores de código de barras, PDAs portáteis, computadores conectados para soltar suas conexões e se reconectar com o AP *soft* do *cracker*.

Figura 5: Redes convencionais



Fonte: Jorge10infrc (2020) disponível em: <https://sites.google.com/site/jorge10infrc/home/tipos-de-rede>. Acessado em 21 de set de 2021.

Uma ação chamada *Man-in-the-middle* e o nome desse ataque virtual que é executado da maneira que o criminoso fica entre o usuário e a pessoa que está se conectando a ele, consequentemente entre a atividade que estão sendo efetuadas (TORRES, 2018). Nesse tipo não existe uma maneira infalível que impeça a invasão do criminoso geralmente o invasor aproveita de um descuido do usuário onde consegue entrar e cometer ilegalidade. A figura abaixo demonstra como ocorre o ataque.

Figura: 6 Ataque Man-in-the-middle

Fonte: Imepac (2019) disponível em: <https://imepac.edu.br/navegar-e-preciso-se-expor-nao-conheca-o-ataque-man-in-the-middle/>. Acessado em: 21 de set de 2021.

4.6 NEGAÇÃO DE SERVIÇO

Um ataque de negação de serviço (DoS) ocorre quando um invasor bombardeia continuamente AP alvo (*Access Point*) ou rede com pedidos falsos, sucesso prematuro mensagens de conexão, mensagens de falha e / ou outros comandos.

Isso causa problemas aos usuários não podem entrar na rede e podem até mesmo causar falha na rede. Sendo que na maioria das vezes o foco dos ataques se concentra na navegação de serviços por meio de servidores *web* (CANALTECH, sd).

Figura 7: SOBRECARGA NO SISTEMA

Fonte: Arte G1 (2009) disponível em: <https://g1.globo.com/noticias/tecnologia/0,,mul951883-6174,00saiba+como+funcionam+os+ataques+que+bloqueiam+servicos+na+internet.html>. acesso em: 15 de set de 2021.

Como vista na ilustração acima, o ataque de negação de serviço, e realizado por um invasor que assume o controle do computador buscando sobrecarregar o sistema. Contudo, a caso que o acesso feito pelo próprio dono da rede já e o bastante para promover a queda do serviço.

4.7 INJEÇÃO DE REDE

Em um ataque de injeção de rede, um *cracker* pode fazer uso de pontos de acesso que são expostos a tráfego de rede não filtrado, transmitindo especificamente tráfego de rede como "*Spanning Tree*" (802.1D), OSPF, RIP e HSRP.

O *cracker* injeta falsos comandos de reconfiguração de rede que afetam roteadores, *switches e hubs*. Uma rede inteira pode ser derrubada dessa maneira e exigir reinicialização ou até reprogramação de todos os dispositivos de rede inteligentes (REDES SEGURA, 2012).

4.8 ATAQUE *CAFFE LATTE*

O ataque *Caffe Latte* é outra maneira de derrotar o WEP. Não é necessário para o atacante estar na área da rede usando este *exploit*. Usando um processo que tem como alvo a pilha sem fio do *Windows*, é possível obter a chave WEP de um

controle remoto cliente.

Ao enviar uma enxurrada de solicitações ARP criptografadas, o agressor aproveita a autenticação de chave compartilhada e as falhas de modificação de mensagem no 802.11 WEP. O invasor usa as respostas ARP para obter a chave WEP em menos de 6 minutos (MORENO, 2016).

4.9 FALHAS QUE OCORREM EM PROTOCOLOS QUE SÃO UTILIZADOS NO PADRÃO ATUAL DE REDES SEM FIO

Quando se fala em falhas em relação à segurança da informação e usada como uma ameaça, uma vulnerabilidade (*bug*), isto é, um defeito que pode ser utilizado para um específico *software\hardware,* ou um protocolo, um recurso, algarismo, dispositivo ou sistema. Dessa forma, quando o ataque e feito com sucesso isso pode gerar diversos problemas, a âmbito individual, ou até mesmo organizacional.

4.10 PROTOCOLOS DE REDE MAIS CONHECIDOS

A rede sem fio é considerada um avanço muito significativo para a comunicação, tendo como maior recurso a facilidade de acesso. Contudo, essa praticidade, advinda da tecnologia, tem falhas que deixa o sistema vulnerável, não tendo um nível se segurança adequada.

Buscando assegura a proteção dos usuários de rede sem fio (Wi-fi), e dificultar a entrada de usuários sem autorização, já há um tempo protocolos de seguranças foram criados (ATS, 2012).

Abaixo estão uma lista de alguns protocolos mais utilizados segundo ATS (2012, p. 2), que são:

Tabela: 2 tipos de protocolos

WEP	*Wired Equivalent Privacy* (Privacidade equivalente aos fios) e conhecido como o primeiro protocolo sendo ele de criptografia apresentado para redes sem fio. O WEP faz parte de um processo de criptografia utilizado pelo modelo IEEE 802.11. Sua utilização e feita por meio de uma senha partilhada para criptografar as informações e trabalhar de maneira fixa. Sendo aquele que possui somente um comando de acesso garantindo assim sua privacidade em relação a rede sem fio e suas transmissões de dados.
WEP 2 ou WPA	Sendo vista como *Wi-fi Protected Access* (Wi-fi de acesso protegido) possui um aprimoramento em relação ao WEP. Ela também é chamada de TKIP (*Temporal Key Integrity Protocol*). Foi criada no ano de 2003 com o objetivo de melhorar a segurança sobre o protocolo WEP. Tendo como foco central alterações no algarismo de criptografia.
WPA 2 ou 802. 11i	Sendo tida como a versão final da WPA, a WPA2 surgiu com diferencial de ter um sistema mais apurado de criptografar dados e informações. Nesse contexto a WPA usa TKIP por meio de algarismo de criptografia, já o WPA2 usa o algarismo AES (*Advanced Encryption Standard*). Porém o algarismo AES possui um peso bem mais significativo que o TKIP. Devido a isso placas antigas não conseguem suporta o WPA2, por mais que atualizem o firmware.

Fonte: ATS (2012, p. 2)

4.11 FALHA NO PROTOCOLO WEP

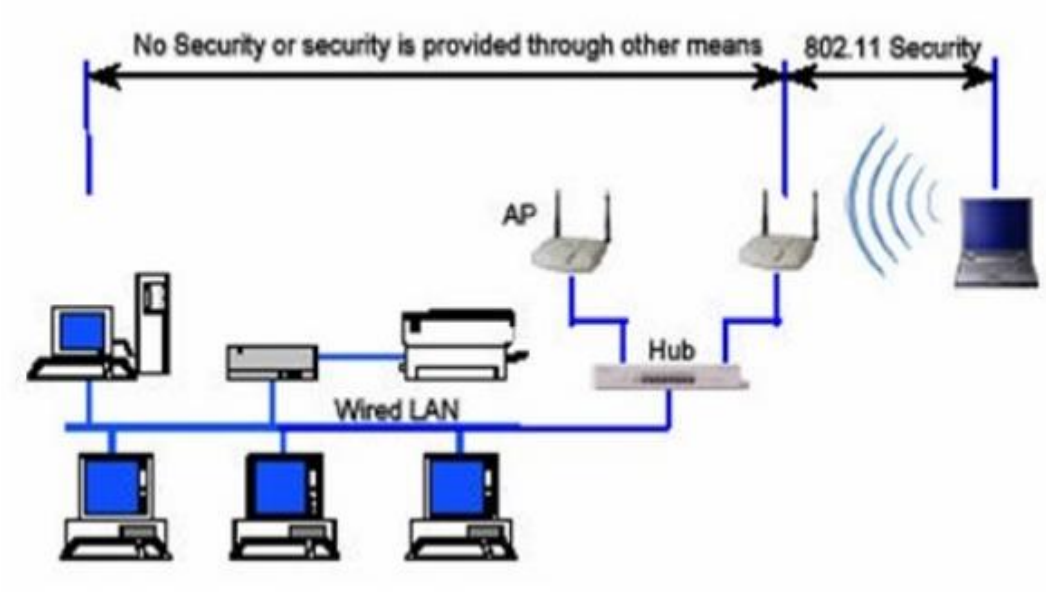
A WEP utiliza como forma de serviço chaves simétricas, isto é, a chave será sempre a mesma, sendo usada para encriptar, ou seja, só pode ser lida por aquele indivíduo que possui a chave, em relação a informações que serão apresentadas na rede. Sendo essa a maior vulnerabilidade, devido isso um invasor que pretende ter acesso a senha basta apenas utilizar uma escuta, e assim sendo possível decifrar os dados e informações que estão na rede. O outro ponto que atribui uma ameaça e o fato de todos terem que possui a mesma chave, possibilitando a difusão ilegal da chave de segurança (SISTEMA PERSONALIZADO, sd).

> “O WEP – Wired Equivalent Privacy – é uma configuração de segurança disponível em roteadores de conexões sem fio Wi-fi. Desde 2004, o WEP é considerado “obsoleto” pela definição do padrão do Wi-fi, em grande parte por conta de sua fraqueza: o WEP foi criado em uma época que as regras de exportação dos Estados Unidos limitavam a utilização de tecnologias de segurança com base em criptografia. Por isso, não demorou para o WEP ser quebrado e substituído por tecnologias melhores” (DMOICANO, 2012, p. 2).

Para Corrêa Júnior (2008) ressalta que a WEP tende a sofrer ações de

invasores, que utilizam de instrumentos distribuídos pela própria *internet* de forma grátis, entre elas estão: *Airsnort, WEPCrack, Aircrack* entre outras, que são construídas para fazer a decodificação de quadros codificados. Tais instrumentos são usados por *hackesrs* buscando cometer diversos ataques a rede.

Figura 8: Protocolo WEP Não garante segurança fim a fim, segurança somente na parte sem fio.



Fonte: Hernandes (2014) disponível em: <https://slideplayer.com.br/slide/1762604/>
Acessado em 21 de set de 2021.

4.12 FALHA NO PROTOCOLO WPA

Em relação à WPA há um protocolo denominado TKIP, que tem como função gerir todas as chaves provisórias, onde tem a capacidade de mudar de chave a cada pedido de um nov4o pacote, isso promove maior dificuldade em acesso ao fluxo de dados na rede (BRITO, 2013).

No WPA também há outro protocolo chamando de EAP, esse possui responsabilidade de autorizar e a autenticação de usuários. Sendo assim, o que pode ser compreendido e que a segurança fica mais eficiente com a adoção da autenticação, entretanto, por utilizar novas ferramentas, entre elas o banco de dados e servidores, potencializa a capacidade de haver ataques específico a cada recurso

individual (BRITO, 2013).

Segundo Corrêa Júnior (2008) salienta que a WPA nasceu de pesquisas criteriosas feitas de um padrão que se encontrava em estudo pelo IEEE. Protocolo esse que não possui várias funcionalidades que são consideradas fundamentais para que o sistema seja confiável quando se fala em organizações de auto padrão, dessa forma, se apresenta como um substituto do WEP devido e falhas que o sistema demonstrava, e chegou com a missão de cobrir as vulnerabilidades do WEP, ou seja, criado sem que tivesse que descartar todo o *hardware* já vendido.

4.13 FALHA NO PROTOCOLO WPA 2

Já a WPA2 tem como maior vulnerabilidade o fato de o AES exigir maior potência do sistema para sua execução. Devido a isso sua utilização é aconselhada para quem precisa de um alto padrão de segurança. Contudo, máquinas de ultimas gerações tem capacidade de suportá-lo sem grandes dificuldades (CANALTECH, sd).

> “O Wi-fi com falhas de segurança é um grande perigo. Mesmo quando a conexão está corretamente é protegida ela já é vulnerável a possíveis ataques, [...] isso provoca uma falsa sensação de segurança, se tornando um grave erro. Pois basta algum pequeno descuido e ela poderá ser afetada. [...] Essa vulnerabilidade acontece sim e uma prova disso é que o próprio protocolo WPA2 tem suas vulnerabilidades. Sendo assim problema está na tecnologia de rede e não nos aparelhos e dispositivos usados” (MINHA CONEXÃO, 2020, p. 2).

De acordo com Corrêa Júnior (2008) a grande desvantagem do WPA2 se encontra na falta de interoperabilidade com os mecanismos legados IEEE 802.11b, o que gera atualização de todo o *hardware* da rede sem fio que trabalha somente com WEP onde seu hardware foi construído para opera com o RC4 e não com AE.

5 ATUAIS PROTOCOLOS DE SEGURANÇAS PARA REDES SEM FIO

De acordo com Bof (2020) no decorrer das últimas décadas, percebe-se um aumento considerável em relação ao número de redes sem fios, que em grande parte vem sendo utilizadas por usuários domésticos, entidades, universidades e ate

empresas corporativas. Tendo grande adesão e sendo bastante popular, neste contexto o usurários vem ganhado com a praticidade que o sistema oferta, aos seus usuários, contudo devido a praticidade e fácil adesão a uma grande preocupação com a segurança de rede. Com isso, atualmente vem sendo criados protocolos bem mais seguros nos últimos anos, sendo desenvolvidos e atualizados de forma mais constante, além de agregar maior velocidade cada dia mais.

No ano de 2017 ocorreram muitas reclamações em relação ao protocolo WPA2, por ser encontrar diversas vulnerabilidades em especial em redes Wi-fi, isso ganho uma repercussão negativa, devido ser o protocolo mais utilizado até então. Essa ameaça gerou debates em relação a um novo protocolo que pudesse trazer mais segurança e confiabilidade. Sendo assim, em 2018 a *Wi-fi Alliance*, empresa responsável pelos certificados de *Wi-fi* cria o WPA3, versão essa que não busca apagar os problemas de vulnerabilidade do WPA2, mas tem como objetivo acrescentar novas ferramentas e promover melhor segurança (PASTORINO, 2018).

6 REDES WIMAX

Essa nova tecnologia denominada WiMAX constitui em um mecanismo de transmissão sem fio, sendo chamada de padrão IEEE 802.16, e referida como uma nova tecnologia que surgiu tendo como desenvolver o grupo WiMAX Fórum. Tendo na época o apoio de organizações como Intel e Nokia, o projeto visa a construção de um padrão aberto, sendo marcado por ser capaz de proporcionar maior conectividade entre vários fabricantes. Segundo a empresa Intel em seu ponto de vista o IEEE 802.16 “é uma variação muito importante desde o advento da própria internet”. Zucchi (2005).

Para Zucchi (2005), o WiMAX terá a capacidade aumentar o desempenho do Wi-fi, não apenas em distancias, mais em maiores potências de transmissão, isto é maior qualidade.

Figura: 9 Rede WiMax que possui capacidade de atingi 50 km

Fonte: Target Solutions (2017) disponível em: <<http://blog.targetso.com/2017/03/14/redes-wireless-wimax-e-wifi-quais-as-diferencas/>. Acesso em: 15 de set de 2021.

Neste contexto a Figura 9 acima demonstra como funciona a rede WiMax e o alcance que possui.

7 CAMADA DE PROTEÇÃO

Quando se fala em proteção de informação, não pode ser mesurado exclusivamente como um processo tecnológico, até porque envolve pessoas e necessita haver um entendimento por parte de todos, principalmente em relação a dados de usuário confidências, informações de clientes, informações privilegiadas, capacidade e competência de quem a executa. Dentro do regimento institucional da organização. Sendo assim para dar maior proteção a informações confidencias de clientes, que trabalha na área de tecnologia precisa pensar de forma multidisciplinar, que abrangem segurança lógica, o fluxo de dados, chegando à criptografia dos bancos de dados, e por fim a segurança do acesso a dados que são armazenados em memórias durante o processamento de dados e informação (CASUSCELLI, 2016).

Segundo Fortes e Delabrida (2014) a segurança de rede necessariamente não está associada a componentes específicos do conjunto de protocolos, dessa forma, cada tipo de camada emprega um modelo de segurança, sendo apresentada

da seguinte forma:

- Camada Física: nesse tipo de camada “Grampos” tende a ser evitados protegendo linhas de transmissões em canais fechados onde contem gás estático dentro de uma alta pressão;
- Camada de Enlace: esse tipo de camada permite que uma máquina seja codificada e decodificada aparti da hora que outra máquina seja introduzida;
- Camada de Rede: Tem como característica a utilização de *firewalls* em que busca preserva ou rejeitar pacotes;
- Camada de Transporte: nessa camada a possibilidade de criptografar conexões completas de um ponto a outro, isto é, de um sistema a outro sistema.
- Camada de Aplicação: Sendo compreendida como a camada que cuida de procedimentos de autenticação e não rejeição.

7.1 CAMADA FÍSICA

Segundo Torres, Mazzoni e Alves (2002), o papel da camada física está associado a ação de colher informações em relação aos conjuntos de dados e posteriormente a colheita transmitir em ondas eletromagnéticas através do rádio. Entretanto isso ocorre de acordo com o protocolo utilizado, sendo ele: IEEE 802.11b, IEEE 802.11g, IEEE 802.11a e por fim o IEEE 802a. 11n, sendo que cada um tem suas particularidades.

A camada física tem como finalidade também cuidar de problemas que em grande parte são considerados comuns, em inúmeras transmissões da rede sem fio, como por exemplo, a reflexão do sinal.

7.2 CAMADA DE ENLACE

Segundo Politécnica (2015) a principal finalidade da camada e possibilita que um canal de transmissão que possua alta capacidade se transforme em uma linha que se apresente com maior liberdade principalmente em relação a erros de transmissão não encontrados pela camada de rede.

Nesse contexto segundo a Politécnica (2015, p.14) são ofertados três serviços através dessa camada que são:

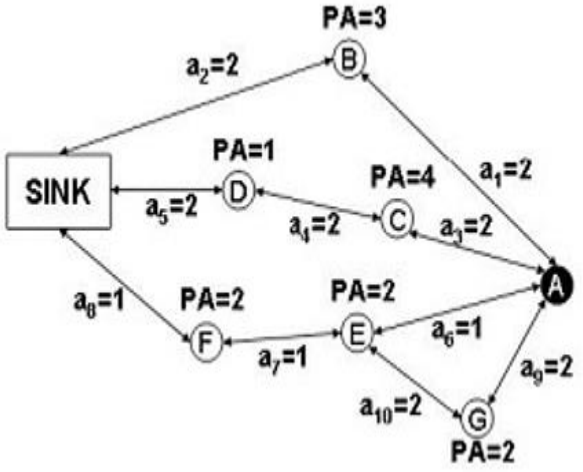
1. Serviço sem conexão e sem confirmação;
2. Serviço sem conexão com confirmação;
3. Serviço orientado a conexões com confirmação.

7.3 CAMADA DE REDE

A camada de rede tem como obrigação o roteamento de dados através dos sensores. Dessa forma os protocolos referentes ao roteamento usado precisam manter a comunicação *multihop*, e necessita buscar o uso máximo da eficiência da energia potencializado pelos sensores. Ou seja, a escolha da rota mais adequada entre um sensor que pretenda transmitir uma informação se encontra nó *sink,* sendo possível alencar vários fatores (TELECO, 2020).

Tendo como exemplo a Figura 10 abaixo, caso o sensor identifique uma ação e queira enviar essa informação para o nó *sink*, esse sensor tem diversas rotas a sua escolha.

Figura 10: Seleção de rotas numa RSSF



Fonte: Teleco (2020) disponivel em: <https://www.teleco.com.br/tutoriais/tutorialrssf/pagina_5.asp> acessado em: 21 de set de 2021.

7.4 CAMADA DE TRANSPORTE

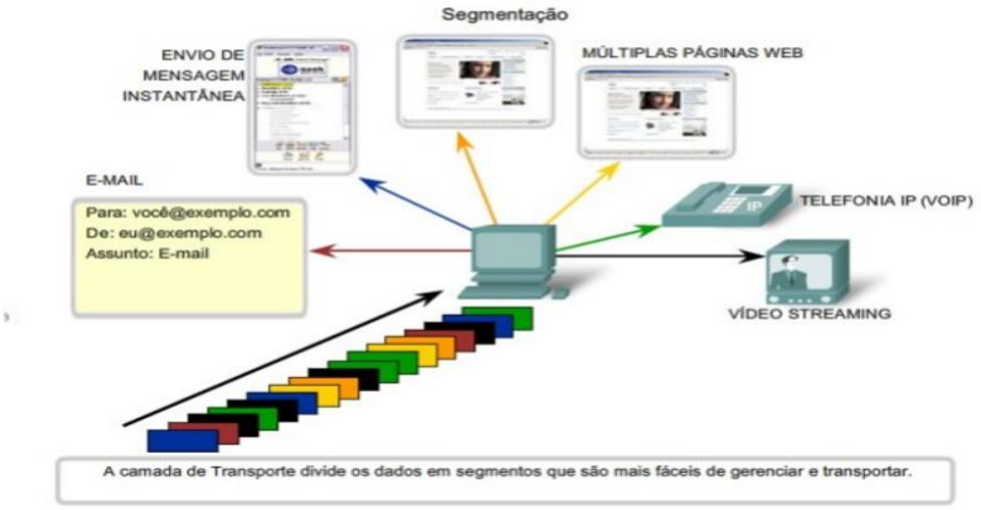
Essa camada e responsável pelo fluxo de dados, de maneira eficiente e segura, entre os processos que estejam em funcionamento em máquinas conectadas a uma rede de computadores, seja lá, qual rede seja, sendo uma ou mais. Essa camada tem o fluxo de dados e assegura a confiabilidade, garantindo que os dados atingiam seus destinos sem erros e em ordem (PEREIRA, 2020).

De acordo com Pereira (2020, p. 2) as principais atribuições da camada de transporte que são:

- Transporte de unidades de dados;
- Segmentação e blocagem;
- Detecção e correção de erros fim a fim;
- Sequenciarão;
- Controle de fluxo de dados nas conexões de transporte;
- Multiplexação (combinar várias conexões de transporte em uma mesma de rede para reduzir custos) ou *splitting*;
- Transporte de dados expresso (para sinalização).

Dessa forma a camada de transporte tem capacidade de oferta um serviço seguro no que pese a entrega de dados das aplicações. Na Figura 11 é representadaessa segmentação das funções da camada de transporte.

Figura: 11 Segmentação da camada de transporte para facilitar seu gerenciamento



Fonte: Docente (2020) disponivel em: <https://docente.ifrn.edu.br/tadeuferreira/disciplinas/2016.1/arq-tcp-ip/Aula16.pdf> acessado em: 21 de set de 2021.

7.5 CAMADA DE APLICAÇÃO

Segundo Lopes (2011) a camada de aplicação pode ser representada por meio de uma analogia do “*win+e*”, por exemplo, no momento que ocorre a abertura do “*explore do Windows*”, é visto uma resposta em relação a uma ação, ou seja, e observado que um aplicativo foi executado, assim provoca que uma comunicação quando é feito outra ação pelo usuário.

Nesse contexto os aspectos referentes a camada de aplicação direcionada para esse padrão, ocorre quando é realizado uma atividade em rede, e quando necessita ser enviada ou possui uma fácil compreensão para o destinatário final ou agente sendo de forma lógica ou não, sendo assim é realizado o uso da camada de aplicação.

8 PROTEGENDO A CONFIDENCIALIDADE DAS TRANSMISSÕES WIRELESS

Existem dois tipos de contramedidas para reduzir o risco de espionagem transmissões sem fio. O primeiro envolve métodos para dificultar a localização e interceptar os sinais sem fio. O segundo envolve o uso de criptografia para preservar confidencialidade, mesmo que o sinal sem fios seja interceptado (RODRIGUES, 2018). E são identificados de seguinte maneira:

8.1 TÉCNICAS DE OCULTAÇÃO DE SINAL PARA INTERCEPTAR TRANSMISSÕES SEM FIO

Os atacantes precisam identificar e localizar redes sem fio. Existem, no entanto, alguns passos que organizações podem fazer para dificultar a localização de seus pontos de acesso sem fio. O mais fácil e menos caro inclui o seguinte: Desligar o identificador do conjunto de serviços (SSID) radiodifusão por pontos de acesso sem fio, atribuir nomes enigmáticos para SSIDs, Sinal de redução força para o nível mais baixo que ainda fornece cobertura necessária ou Localização de acesso sem fio, pontos no interior do edifício, longe de janelas e paredes exteriores. Mais efetivo, mas também métodos mais caros para reduzir ou ocultar sinais incluem: antenas para restringir as emanações de sinal dentro das áreas de cobertura

desejadas ou técnicas de blindagem de emanações, por vezes referidas como TEMPEST, 1 para bloquear a emanação de sinais sem fio (RODRIGUES, 2018).

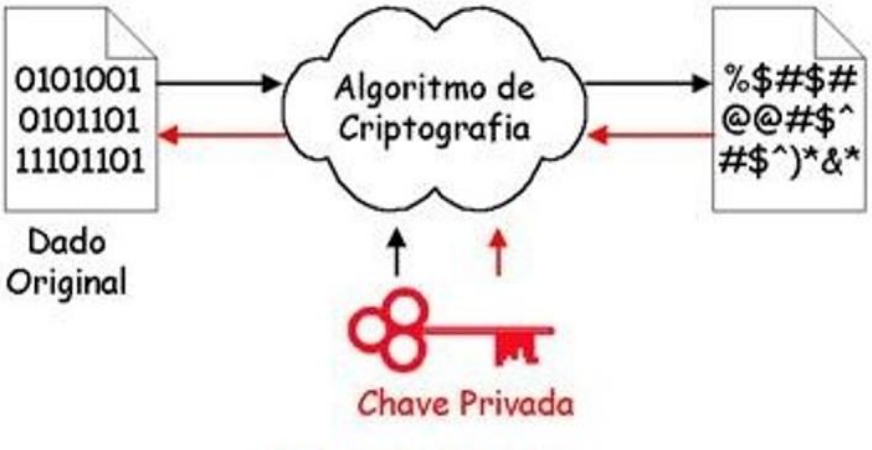
8.2 CRIPTOGRAFIA

O melhor método para proteger a confidencialidade das informações transmitidas por redes sem fio é criptografar todo o tráfego sem fio. Isso é especialmente importante para organizações sujeitas a regulamentos (STALLINGS, 2003).

> “De forma simples, a criptografia é um conjunto de técnicas pensadas para proteger uma informação de modo que apenas emissor e receptor consigam compreendê-la. O protocolo de criptografia pode ser mais ou menos elaborado e técnicas como essas existem desde a antiguidade, com o primeiro sistema de criptografia conhecido tendo surgindo no Egito, cerca de 1.900 anos antes de Cristo” (CIRIANO, 2015, p.2).

Segundo Melo (2012) a criptografia tem como uma de suas funções dificultar a aquisição de informações restritas, ou o rompimento de comunicações sigilosas. Por mais que um invasor consiga interceptar sua comunicação o sistema inviabiliza sua visualização, sendo comunicação em fluxo ou armazenadas em servidores e provedores que realizam o serviço.

Figura: 12 Modelo de criptografia



Fonte: Assinatura Digital (2017) disponivel em: <https://www.gta.ufrj.br/grad/ 07_1/ass-dig /TiposdeCriptografia.html> acessado em: 21 de set de 2021.

Na Figura 12 e apresentado um simples modelo de criptografia onde tanto o emissor da mensagem quanto o recepto tem a mesma chave, isto é, a chave e utilizada quanto para a codificação como para a decodificação.

8.3 IMPEDINDO A ALTERAÇÃO DE COMUNICAÇÕES INTERCEPTADAS

Interceptação e alteração de transmissões sem fio representam uma forma de ataque "*Man-in-the-middle*". Dois tipos de contramedidas podem reduzir significativamente o risco de tais ataques: criptografia forte e autenticação forte de dispositivos e usuários (BECK e TEWS, 2012).

8.4 CONTRAMEDIDAS PARA REDUZIR O RISCO DE ATAQUES DE NEGAÇÃO DE SERVIÇO

De acordo com Junior et al., (2004) a utilização da rede sem fio possibilitou maiores facilidade e mobilidades a seus consumidores, entretanto um aspecto essencial não possui a atenção que deveria ter, em relação a segurança da informação. A utilização de mecanismos de segurança e fundamental para promover maior eficiência nos serviços realizados, devido haver a necessidade de reduzir os riscos e acessos inapropriados á rede.

Sendo assim para que tenha o mínimo de segurança e necessário promover controles externos aos dispositivos. Criado configurações confiáveis, pela criptografia, autenticação eficiente e supervisionando os acessos da rede sem fio, medidas essas essências para sua efetivação (JUNIOR et al, 2004).

As comunicações sem fio também são vulneráveis a ataques de negação de serviço (DoS). As organizações podem tomar várias medidas para reduzir o risco de tais como o DoS não intencionais ataques.

Pesquisas de site cuidadosas podem identificar locais onde os sinais de outros dispositivos existem; os resultados de tais pesquisas devem ser usados ao decidir onde localizar pontos de acesso. Auditorias periódicas regulares de atividade e desempenho de redes sem fio pode identificar áreas problemáticas; ações corretivas apropriadas podem incluir a remoção dos dispositivos ofensivos ou

medidas para aumentar a força do sinal e a cobertura dentro da área de problema (BR DEFENDER, 2016).

9 ESTUDO DE CASO

9.1 MARINHA DO BRASIL: ORIGEM E ESTRUTURA

Componente das Forças Armadas do Brasil, a Marinha faz parte da integração enquanto um dos três ramos das forças armadas brasileiras, sendo que as Forças Armadas do Brasil e Forças Aéreas do Brasil compõem os restantes. É mais antiga instituição de defesa marítima do continente sul-americano, com registro iniciados ainda no século XVIII, pelo rei português Dom João V. Por serem definidas como forças nacionais, sua principal função é a defesa dos interesses e integridade dos territórios brasileiros (REIS; ZUCCO, 2020).

Atualmente, a relevância da instituição é representada pela atuação em outros países como o Líbano, em ação conjunta com as forças marítimas alemãs, gregas e turcas, como resultado da participação da Marinha brasileira na Força Interina das Nações Unidas (VILELA, 2020). Ainda segundo o autor, é a Marinha do Brasil que, por meio das atividades do Comando de Operações Navais, realiza os treinamentos e formações de seus subordinados para questões de esquadra, tráfego marítimo, busca e salvamento.

A realização das atividades da instituição exige uma capacidade estrutural composta por departamento marítimo, com fragatas inglesas submarinos, embarcações de apoio logístico e barcos veleiros para acompanharem missões de funções diplomáticas em eventos nacionais e internacionais (WALDMANN JÚNIOR, 2013).

O trabalho de Conceição (2012) ainda acrescenta que a estrutura da Marinha do Brasil conta com Força Aeronaval, formada por aviões e helicópteros navais operacionalizadas por organização militar para operações aéreas a partir das embarcações. Sendo esquadrões espalhados por todo o país e que fornecem apoio aéreo para as demais organizações militares das forças armadas.

9.2 CENTRO DE REPAROS E SUPRIMENTOS ESPECIAIS DO CORPO DE FUZILEIROS NAVAIS

De maneira paralela à estrutura, faz parte da prática e organização institucional da Marinha do Brasil (MB) a existência de departamentos que possam atender de maneira simultânea ao suporte interno, clientes fora do escopo hierárquico das forças armadas. Esse é o caso do Centro De Reparos e Suprimentos Especiais do Corpo de Fuzileiros Navais (CRepSupEspFN), fruto da expansão de atribuições do Depósito de Material do Comando-Geral do Centro de Fuzileiros Navais ainda na década de 1960 (CTECCFN, 2013).

Dessa forma, um dos principais meios de comprovação da eficiência dos serviços prestados pelo CRepSupEspCFN são seus diversos clientes sejam militares, governamentais ou empresas privadas, as quais oferecem diversas autorizações de representação e manutenção ao Centro (SILVA, 2010).

Se incluí até marcas internacionais como *Toyota*, *Land Rover* e *Harley-Davidson* que, acabam também prestando serviço à Marinha por fornecerem veículos. Contudo, essa parceria também alcança dimensões tecnológicas entre as instituições (SILVA, 2010).

Fato esse, observado como demanda pelo próprio processo evolutivo do Centro que, ao se expandir, passou a

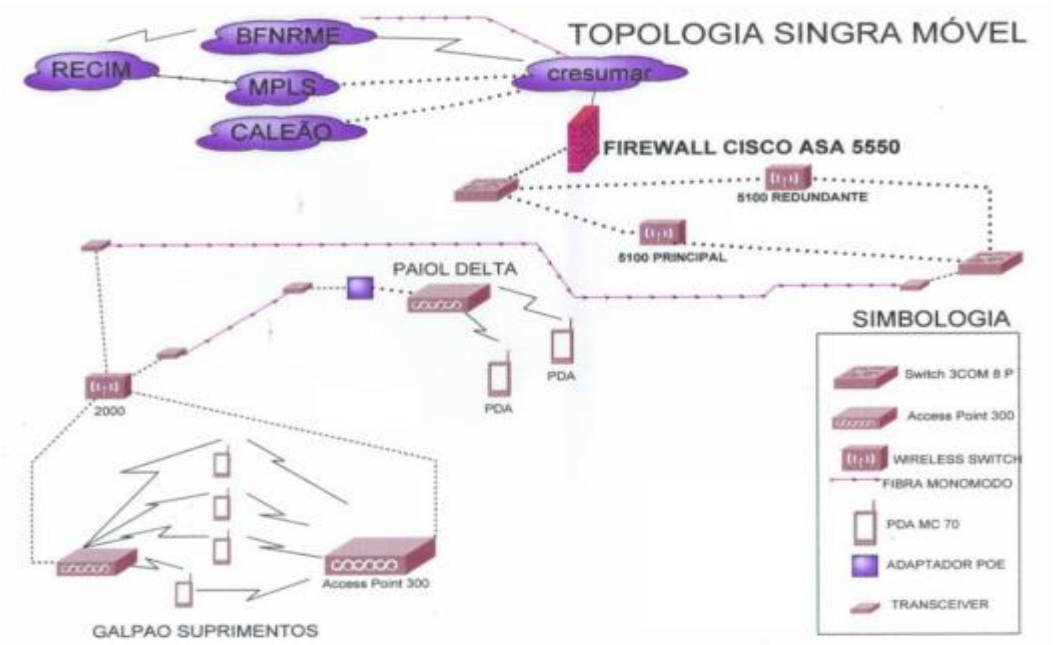
> contribuir para o desenvolvimento tecnológico da Marinha do Brasil [MB] por meio de atividades de ciência, tecnologia e inovação; e para o pronto-emprego e o abastecimento do material específico do CFN, das armas leves de toda a MB e, quando determinado, de equipamentos de outros símbolos de jurisdição (CTECCFN, 2013, p. 1).

Contudo, passar a atender essas contribuições exigiu do Centro um desenvolvimento significativo, rápido e seguro em termos administrativos. De modo que, a principal demanda tecnológica foi relativa a um sistema de controle de seus bancos de dados digitais e estoques físicos. Especialmente ao considerar que peças sobressalentes ou demais complicações no armazenamento da instituição podem comprometer o retorno econômico, dado que são representações de aumento de custos operacionais (SILVA, 2010).

De acordo com o trabalho de Silva (2010), a resposta a essa demanda foi pensada a partir do desenvolvimento de uma rede WiFi (Figura 1) que permitisse o acesso ao SINGRA (Sistema Integrado de Gerenciamento do Abastecimento) da

instituição. Entretanto, ao permitir esse acesso se abriu a oportunidade do risco de perda, manipulação ou qualquer outro dano à segurança das informações do Centro.

Figura 13: Rede SINGRA do Centro De Reparos e Suprimentos Especiais do Corpo de Fuzileiros Navais



Fonte: Silva (2010) disponivel em: < https://pantheon.ufrj.br/bitstream/11422/3352/1/ CSilva.pdf> acessado em: 21 de set de 2021.

A Figura 13 apresentada acima demonstra o funcionamento da rede SINGRA, o passo a passo em relação a seu desenvolvimento enquanto uma rede WIFI, assim como seus possíveis riscos.

9.3 PRINCIPAL COMPLICAÇÃO DA CONEXÃO AO SINGRA

O controle de acesso das redes *wireless* da Marinha é realizado pelo padrão WPA2 além de ter constante monitoramento realizado pelo sistema preventivo *Wireless Intrusion Prevention System* (WIPS) que atua de maneira remota com 200 sensores nos locais de instalação das redes (SILVA, 2010).

Mas, a execução é centralizada na Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM). Além disso, a DCTIM definiu que os *acess points* da rede sejam redundantes nos dispositivos de controle e que contém um *firewall* próprio para dar acesso apenas aos funcionários autorizados (SILVA, 2010).

É notável que a utilização do padrão WPA2 confere segurança e eficiência às redes, mas exige um nível alto de capacidade de processamento. Característica oriunda do fato de que ao utilizar o AES em associação com o TKIP, as chaves são 256 *bits*, de maior poder criptográfico e que exige *hardware* equivalente para processamento dos cálculos de criptografia (ARASAKI; DELLA FLORA, 2012).

Assim, dispositivos domésticos, antigos ou obsoletos que fazem parte da estrutura da Marinha têm compatibilidade reduzida com o padrão e exigem obrigatórias realizações de testes antes de implementados às redes. Essa exigência faz com que exista custo pessoal, operacional e econômico à instituição sem a certeza de correta equivalência entre a rede, o controle de acesso, o monitoramento e o dispositivo de interesse (SILVA, 2010).

9.4 ANÁLISE

Considerando que após a expansão, o principal objeto de trabalho do CRepSupEspCFN são as informações digitais dos recursos materiais e de inteligênciada Marinha, a segurança destes é entendida como prioridade absoluta na possibilidade de acesso e monitoramento por redes *wireless*.

Além disso, se deve levar em conta a existência do enforcamento orçamentário da instituição. Representados, conforme Brasil (2021) pelo valor de R$ 491,2 milhões. Situação essa que força ações institucionais de destacar cada vez mais as prioridades já postas, como a segurança em detrimento de áreas como a tecnologia e os recursos pessoais, como ressaltado na reportagem.

Nesse sentido, em concordância, Silva (2010) aponta que, de fato, a Marinha mais se atenta à segurança de sua rede do que a performance de seus dispositivos, já no período inicial de desenvolvimento das redes. E que a decisão pelo uso do padrão WPA2 é um claro sinal dessa realidade, mesmo ao considerar os dispositivos já instalados pela instituição.

Outro ponto importante a se discutir é associação do padrão WPA2 com o sistema WIPS, como complementação. Mais um claro sinal de coerência com a preocupação da integridade e acesso restrito aos dados. Sobre isso, Silva (2010) acrescenta que

> “A forma pró-ativa como atua este sistema vem ao encontro dos anseios de segurança da instituição, visto que a simples detecção poderia dar tempo ao dispositivo atacante de realizar o seu intento. Como o WIPS atua de forma preventiva, interferindo ativamente e automaticamente na conexão do dispositivo atacante, este não tem meios de completar o seu ataque” (SILVA,2010, p. 45).

Ao analisar o estudo em questão associado a marinha do Brasil nota-se que, por ser um órgão militar carece de um sistema eficiente e seguro por se tratar da defesa nacional, os dados desse setor precisa de protocolos é uma equipe confiável, tendo em vista que não pode ser vazado muito menos hackeados.

Por último, o que se ressalta é ação da Marinha não só em proteger e controlar o acesso às suas redes, mas também em monitorá-las para garantir o aspecto confidencial das atividades militares que desenvolve. Fato esse que representa o desenvolvimento adequado da adesão da instituição à tecnologia *wireless* ou seja, realizado de maneira prudente e segura, mesmo em condições financeiras adversas.

CONSIDERAÇÕES FINAIS

Com o avanço tecnológica, muitos processos mudaram, as redes sem fio promoveram diversas funcionalidades, no entanto, a falta de compatibilidade entre os elementos durante o processo de evolução, limitou a sua expansão/difusão. Esse fato gerou muitos testes que oportunizaram o desenvolvimento de melhorias significativas para que os sistemas suportassem a grande demanda. E com o passar do tempo muitos processos foram atualizados, gerando maior conectividade.

Diante desse contexto, o consumo aumentou, porém contribuiu para que os invasores encontrassem nas redes novas formas de cometer irregularidades. Com isso, surgiram variados problemas que acarretaram exigências de melhores protocolos de segurança. Os protocolos trouxeram mais confiabilidade para o sistema, no entanto, devido aos usuários nem sempre tomarem os devidos cuidados, ainda gera diversos problemas, principalmente em relação a roubo de dados e informações sigilosas, como é o caso de contas bancárias e dados de organizações de grande porte que requerem bastante sigilo.

Portanto, conclui-se que a vulnerabilidade relacionada à segurança de rede sem fio está associada a inúmeros fatores, assim como a vigilância dos usuários e a atenção das empresas que realizam diversas transações e troca de dados através dessas redes.

REFERÊNCIAS

ATS, G. **Entenda WEP e WPA, protocolos de segurança de rede Wi-Fi**. Techtudo. 2012. Disponível em: https://www.techtudo.com.br/artigos/noticia/2012/02/entenda-wep-e-wpa-protocolos-de-seguranca-de-rede-wi-fi.html. Acesso em: 15 de set de 2021.

ARASAKI, A. M.; DELLA FLORA, J. C. L. **Teste de intrusão em redes sem fio padrão 802.11**. 2012. 63 f. Monografia (Especialista em Rede de Computadores e Segurança da Informação) Centro Universitário Filadélfia de Londrina – Unifil, Londrina, 2012.

BATISTA, E. O. **Sistemas de informação**. Saraiva Educação SA, 2017.

BERGHER, R. **Do 1G ao 5G: conheça a evolução da internet no celular**. Zoom. 2019. Disponível em: https://www.zoom.com.br/celular/deumzoom/do-1g-ao-5g-evolucao-internet-no-celular. Acesso em: 12 de set de 2021.

BECK, M.; TEWS, E. **Segurança em Redes IEEE 802.11** - Revista Infra Magazine 7. 2012. Disponível em: https://www.devmedia.com.br/seguranca-em-redes-ieee-802-11-revista-infra-magazine-7/25680. Acesso em: 15 de set de 2021.

BEUREN, I. M.; RAUPP, F. M. Metodologia da pesquisa aplicável ás ciências sociais. In: BEUREN, IIse Maria (org). **Como elaborar trabalhos monográficos em contabilidade: teoria e prática**. 2. Ed. São Paulo: Atlas, 2004.

BOF, E. **Segurança em Redes Wireless**. 2010. Monografia. (Especialista em Gestão da Segurança da Informação) – Faculdade do Centro Leste. Serra. Disponível em: http://br.monografias.com/trabalhos-pdf/seguranca-redes-wireless/seguranca-redes-wireless.pdf. Acesso em: 15 de set de 2021.

BRAIN, M.; WILSON, T. V.; JOHNSON, B. How Stuff Works. **howstuffworks**. 2001. Disponível em: http://computer.howstuffworks.com/wireless-network1.htm. Acesso em: 15 de set de 2021.

BRAGA, L. **4G/LTE: saiba como o 4G funciona.** Tecnoblog.2018. Disponível em: https://tecnoblog.net/88088/lte-4g-como-funciona/. Acesso em: 12 de set de 2021.

BRASIL SERVIDORES, 2012. **Segurança da Informação.** Disponível em http://www.wbrasilservidores.com.br/seguranca-da-informacao. Acesso em: 15 de set de 2021.

BRITO, E. **Qual é a diferença entre WEP e WPA? Qual é o mais seguro?** Techtudo. 2013. Disponível em: https://www.techtudo.com.br/dicas-e-tutoriais/noticia/2013/05/qual-e-diferenca-entre-

wep-e-wpa-qual-e-o-mais-seguro.html. Acesso em: 15 de set de 2021.

BRASIL, Câmara dos deputados. **Forças Armadas dizem que cortes comprometem programas estratégicos**. Caderno de Relações Exteriores: F. Brandão; A. Chalub, 2021. Disponível em: https://www.camara.leg.br/noticias/755229-forcas-armadas-dizem-que-cortes-comprometem-programas-estrategicos/. Acesso em: 31 mar. 2022.

BR DEFENDER. **Saiba como reduzir risco de Ataque Distribuído de Negação de Serviço (DDoS).** Brdefender. 2016. Disponível em: https://www.brdefender.com.br/noticias/2016/05/11/saiba-como-reduzir-risco-de-ataque-distribuido-de-negacao-de-servico.html. Acesso em: 15 de set de 2021.

CASUSCELLI, L. **Cybersecurity: as camadas eficientes da proteção**. Tiinside. 2016. Disponível em: https://tiinside.com.br/13/06/2016/cybersecurity-as-camadas-eficientes-da-protecao/. Acesso em: 15 de set de 2021.

CANALTECH. **O que é DoS e DDoS?** Canaltech. Disponível em: https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/. Acesso em: 15 de set de 2021.

CELI, R. **Código Morse:** o que é, tabela e história. Stoodi. 2019. Disponível em: https://www.stoodi.com.br/blog/2019/03/08/codigo-morse-o-que-e/. Acesso em: 15 de set de 2021.

CIRIANO, D. **O que é criptografia e por que você deveria usá-la**. Canaltech. 2015. Disponível em: https ://canaltech.com.br/seguranca/o-que-e-criptografia-e-por-que-voce-deveria-usa-la/. Acesso em: 15 de set de 2021.

CORRÊA, J. M. A. C. **Evolução da Segurança em Redes Sem Fio.** 2008. Monografia (Bacharel em Ciência da Computação) – Centro de Informática (CIN). Universidade Federal de Pernambuco (UFPE), Recife. Disponível em: http://www.cin.ufpe.br/~tg/2008-1/maccj.pdf. Acesso em: 15 de set de 2021.

CONCEIÇÃO, M. D. **Marinha do Brasil e Programa Netuno**: excelência gerencial como meio e uma Força Armada de qualidade como fim. 2012. 89 f. Dissertação (Mestre em Administração) Fundação Getúlio Vargas, Rio de Janeiro, 2012.

CRUZ, B. C. **3G, 4G e 5G: entenda a tecnologia por trás da conexão do seu celular**. Uol. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/10/18/entenda-a-tecnologia-por-tras-do-3g-4g-e-5g.htm. Acesso em: 12 de set de 2021.

CTECCFN, Marinha do Brasil. **Centro Tecnológico do Corpo de Fuzileiros Navais**. Acervo Arquivístico da Marinha do Brasil: A. P. Garcêz, 2013. Disponível em:

http://www.arquivodamarinha.dphdm.mar.mil.br/index.php/centro-tecnologico-do-corpo-de-fuzileiros-navais-2. Acesso em: 31 mar. 2022.

DA SILVA, B. F. **Resiliência na transmissão de dados multicaminhos em redes heterogêneas sem fio**. 2018. 121 f. Tese (Doutor em Informática) Universidade Federal do Paraná, Curitiba, 2018.

DMOICANO**. Protocolo WEP**: uma falsa sensação de segurança nas redes Wi-Fi. Linhadefensiva. 2012. Disponível em: https://linhadefensiva.org/2012/10/29/protocolo-wep-uma-falsa-sensacao-de-seguranca-nas-redes-wi-fi/. Acesso em: 15 de set de 2021.

DUARTE, L. O. **Análise de Vulnerabilidades e ataques inerentes a Redes sem fio 802.11x**. 2003. Projeto Final de Curso. (Bacharel em Ciência da Computação) – Departamento de Ciências de Computação e Estatística do Instituto de Biociências, Letras e Ciências Exatas (IBILCE). Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP). Campus São José do Rio Preto, São José do Rio Preto. Disponível em:http://www.micropic.com.br/paginadecliente/noronha/Informatica/SEGURANCA/ataques%20e%20vulnerabilidades%20em%20redes%20sem%20fio.pdf. Acesso em: 15 de set de 2021.

EFETIVIDADE. **Aumento da cobertura da rede sem fio**. Efetividade. 2009. Disponível em: https://efetividade.net/2009/11/rapidinha-efetiva-004-avaliacao-cobertura-do-wi-fi-aprendendo-a-tocar-guitarra-na-web-retrovisores-e-brindes.html. Acesso em: 15 de set de 2021.

ENGST, A.; FLEISHMAN, G. **Kit do Iniciante em Redes Sem Fio**: O guia prático sobre redes Wi-Fi para Windows e Macintosh. 2ª ed.: São Paulo. Ed.: Pearson Makron Books. 2005.

FACHIN, O. **Fundamentos de Metodologia**. 3. ed. São Paulo: Saraiva, 2001.

FIORILLO, C. A. P.; CONTE, C. P. **Crimes no meio ambiente digital**. Saraiva Educação SA, 2017.

FORTES, R.; DEABRIDA, S. **Segurança**. Decom. 2014. Disponível em: http://www.decom.ufop.br/reinaldo/site_media/uploads/2014-02bcc361/aulas/bcc361-2014-02_-_p7_seguranca.pdf. Acesso em: 15 de set de 2021.

Fundação Getúlio Vargas - FGV EAESP. **Brasil tem 424 milhões de dispositivos digitais em uso, revela a 31ª Pesquisa Anual do FGVcia.** Fgv. 2020. Disponível em:https://portal.fgv.br/noticias/brasil-tem-424-milhoes-dispositivos-digitais-uso-revela-31a-pesquisa-anual-fgvcia. Acesso em: 12 de set de 2021.

Gil, A. C. **Métodos e técnicas de pesquisa social**: - 6. ed. - São Paulo: Atlas, 2008.

GOMES I. E., NETO, B. M. **Sistema para Validação e Visualização de**

Certificados Digitais. 2003. Trabalho de Conclusão de Cursos. (Bacharelado em Ciência da Computação) – Universidade Federal de Santa Catarina (UFSC), Departamento de Informática e Estatística. Santa Catarina. Acesso em: 15 de set de 2021.

G1. **Pesquisa revela que internet tem uma tentativa de golpe a cada 15 segundos.** G1. 2015. Disponível em: http://g1.globo.com/bom-dia-brasil/noticia/2015/09/pesquisa-revela-que-internet-tem-uma-tentativa-de-golpe-cada-15-segundos.html. Acesso em: 15 de set de 2021.

JASPER, A. P. **Entendendo redes wireless**. Vivaolinux. 2010. Disponível em: https://www.vivaolinux.com.br/artigo/Entendendo-rede-wireless. Acesso em: 15 de set de 2021.

JUNIOR, C. A. C; BRABO, G. S; AMORAS, R. A. S. **Segurança em redes wireless padrão IEEE 802.11b**: Protocolos WEP, WPA e análise de desempenho. Belém, PA., 2004, 78p. Monografia (Bacharel em Ciência da Computação) Universidade da Amazônia, Belém. 2004.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet: uma abordagem top-down.** [S.l.]: Editora Pearson, São Paulo-SP, 2013.

LEMOS, A.; PASTOR, L.; OLIVEIRA, N. Wi-Fi Salvador: mapeamento colaborativo e redes sem fio no Brasil. **Intercom: Revista Brasileira de Ciências da Comunicação**, v. 35, p. 183-204, 2012.

LOPES, P. A. **A camada de aplicação no modelo tcp/ip**. Disponível em: https://periciacomputacional.com/camada-de-aplicacao-modelo-tcpip/. Acesso em: 15 de set de 2021.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica.** 6. ed. São Paulo: Atlas, 2011.

MELO, E. T. L., RHODEN, G. E., WESTPHALL, C. B., **Detecção de intrusões em Backbones de Redes de computadores Através da Analise de Comportamento com SNMP.** Laboratório de Redes e Gerência. Curso de Pós-Graduação em Ciência da Computação – Universidade Federal de Santa Catarina (UFSC), 2012. Artigo da Web. Disponível em: http://labcom.inf.ufrgs.br/ceseg/anais/2002/02.pdf. Acesso em: 15 de set de 2021.

MIRANDA, A. **Redes Wi-Fi 802.11 o que é?** 2013, Disponível em: http://antoniomjf.wordpress.com/2013/08/24/redes-wi-fi-802-11-o-que-e-eseuspadroes/. Acesso em: 15 de set de 2021.

MINHA CONEXÃO. **Veja como se proteger da falha que pode deixar seu Wi-Fi vulnerável a ataques**. Minhaconexao. 2020. Disponível em: https://www.minhaconexao.com.br/blog/veja-como-se-proteger-da-falha-que-pode-deixar-seu-wi-fi-vulneravel-a-ataques/. Acesso em: 15 de set de 2021.

MORENO, D. **Pentest em Redes sem fio** Novatec Editora Ltda. 2016.

MURTHY, C.; MANO, B. **Ad Hoc wireless networks: architetures and protocols**. Prentice Halll Professional Technical Reference. 2004.

NBR ISO/IEC 17799 (2005), Disponívelem:http://pt.scribd.com/doc/2449992/Abnt-**NBR-Isoiec-17799**-Tecnologia-da-Informacao-Tecnicas-de-Seguranca-Codigo-de-Pratica-para-a-Gestao-da-Seguranca-da-Informacao. Acesso em: 15 de set de 2021.

NAPOLITANO, O. C. **Estudo de Viabilidade para a Utilização da Tecnologia Wireless no Monitoramento de Condições Operacionais de Motores em Usinas Nucleares**. 2019. 94 f. Dissertação (Mestre em Energia Nuclear) Universidade Federal do Rio de Janeiro. Rio de Janeiro. 2019.

OLIVEIRA, C. B. **Proposta de um modelo de segurança da informação: o caso de uma aplicação no colégio Pedro II**. 2016. 123 f. Dissertação. (Mestrado em sistema de Gestão). Universidade Federal Fluminense, Niterói, 2016.

PINHEIRO, J. **Guia completo de cabeamento de redes**. Elsevier Brasil, 2016.

POZZEBOM, R. **O que é 5G?** oficinadanet. 2018. Disponível em:https://www.oficinadanet.com.br/internet/22293-o-que-e-5g. Acesso em: 12 de set de 2021.

PASTORINO, C. **Quais as melhorias do novo protocolo WPA3 para as redes WiFi?** Welivesecurity. 2018. Disponível em: https://www.welivesecurity.com/br/2018/01/22/melhorias-do-protocolo-wpa3-para-as-redes-wi-fi/. Acesso em: 15 de set de 2021.

PEREIRA, C. A. **Camada de Transporte**. Ece. 2020. Disponível em: http://www.ece.ufrgs.br/~fetter/ele00012/transporte.pdf. Acesso em: 15 de set de 2021.

POLITÉCNICA. **Protocolos de Enlace**. Politécnica. 2015. Disponível em: https://www.politecnica.pucrs.br/professores/tergolina/Redes_e_Protocolos_Industriais/APRESENTACAO_-_Aula_06_Protocolos_Enlace.pdf. Acesso em: 15 de set de 2021.

SANTINO, R. **Conheça as diferenças entre 1G, 2G, 3G e 4G**. olhardigital. 2013. Disponível em:https://olhardigital.com.br/noticia/conheca-as-diferencas-entre-1g,-2g,-3g-e-4g/34225. Acesso em: 12 de set de 2021.

SEVERINO, A. J. **Metodologia do trabalho científico**. 23. ed. rev. e atual. São Paulo: Cortez, 2007.

SISTEMA PERSONALIZADO**. Falhas na Wep - Protocolo do Wireless (Rede sem Fio).** Sistemapersonalizado. Disponível em: https://www.sistemapersonalizado.com/cob/wep.htm. Acesso em: 15 de set de 2021.

SIMÃO, J. B.; SUIADEN, E. J. Cidades digitais em municípios brasileiros de pequeno porte: proposta de um modelo de implantação. **Inclusão Social**, v. 5, n. 2, 2012.

SILVA, L. A. F. da, DUARTE, O. C. M. B. **RADIUS em Redes sem Fio**. Universidade Federal do Rio de Janeiro. RJ – 2003. Disponível em:http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/lafs/RADIUS_em_Redes_sem_Fio.pdf. Acesso em: 15 de set de 2021.

SILVA, C. E. M. **Segurança em redes Wi-Fi corporativas:** estudo de caso na Marinha do Brasil. 2010. 50 p. Monografia (Especialista em Gerência de Redes de Computadores) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2010.

SILVA, M. L. G. **A inclusão digital nas políticas públicas de inserção das Tecnologias de Informação e Comunicação na Educação**: o discurso e a prática dos cursos de formação de professores. 186 f. 2014. Dissertação (Mestrado em Educação) – Faculdade de Educação, Universidade Federal da Bahia, Salvador, 2014.

STEFANUTO, I.; SANTOS, J. A. M. dos; TORRES, C. T. Evolução das redes sem fio: Comparativo entre wi-fi e bluetooth. **Caderno de Estudos Tecnológicos,** v. 4, n. 1,2016.

STALLINGS, W. **Cryptography and Network Security** - Principles and Practices, 3nd ed., Prentice Hall, 2003.

TANENBAUM, A. *S.* **Redes de Computadores***. São Paulo: Ed*. [S.l.]: Campus, 2003 CELI, R. **Código Morse: o que é, tabela e história**. Stoodi. 2019. Disponível em: https://www.stoodi.com.br/blog/2019/03/08/codigo-morse-o-que-e/. Acesso em: 15 de set de 2021.

TANENBAUM, A; WETHERALL, D. **Redes de computadores**. Tradução Daniel Vieira. 5ª ed. São Paulo: Pearson Prentice Hall, 2011.

TORRES, E. F.; MAZZONI, A. A; ALVES, J. B. M. A acessibilidade à informação no espaço digital. **Ciência da Informação**, v. 31, p. 83-91, 2002.

TORRES, G. **O que é um ataque Man-in-the-Middle?** Avg. 2018. Disponível em: https://www.avg.com/pt/signal/man-in-the-middle-attack. Acesso em: 15 de set de 2021.

REDE SEGURA. **O que são ataques de injeção de sql**? Redesegura. 2012. Disponível em:http://www.redesegura.com.br/2012/02/serie-ataques-saiba-mais-sobre-os-ataques-d e-injecao-de-sql/. Acesso em: 15 de set de 2021.

REIS, V. C.; ZUCCO, L. P. As experiências das Oficiais da Marinha do Brasil no exercício do comando. **Revista Estudos Feministas**, v. 28, n. 1, 2020.

ROMER, R. **GSM, 3G, EDGE, HPSA, 4G e LTE: entenda as siglas de conexão mobile**. Canaltech. 2013. Disponívelem:https://canaltech8.rssing.com/chan-14368716/all_p2.html. Acesso em: 12 de set de 2021.

RODRIGUES, R. B. **Novas Tecnologias da Informação e da Comunicação**. IFPE Recife, 2016.

RODRIGUES, J. **Dez coisas que você não deve fazer com o seu roteador Wi-Fi.** Techtudo. 2018. Disponível em:https://www.techtudo.com.br/listas/2018/08/dez-coisas-que-voce-nao-deve-fazer-co m-o-seu-roteador-wi-fi.ghtml. Acesso em: 15 de set de 2021.

RUFINO, N. M. O. **Segurança em redes sem fio**. 2. Ed. São Paulo: Novatec, 2005.

RUFINO, N. M. O. **Segurança em redes sem fio: aprenda a proteger suas informações em ambientes wi-fi e bluetooth**. Novatec Editora, 2019.

VACCA, J. R.; **Guide to Wireless Netowrk Security**; New York;SpringerScience+Business Media; 2006.

VILELA, É. S. **Amazônia azul:** a estratégia da Marinha do Brasil para a segurança marítima. 2020. 33 f. Trabalho de Conclusão de Curso (Graduação em Inteligência Estratégica) ESCOLA SUPERIOR DE GUERRA – ESG, Rio de Janeiro, 2020.

WALDMANN JÚNIOR, L. **Tecnologia naval e política**: o caso da Marinha brasileira na era dos contratorpedeiros, 1942-1970. 2013. 155 f. Dissertação (Mestre em Ciência Política) Universidade Federal de São Carlos – UFSC, São Carlos, 2013.

ZUCCHI, W. L,"**O que é a tecnologia WiMAX e qual sua relação comas redes locais compatíveis com o padrão IEEE 802.11** ?", revista RTI, p. 108-111, maio de 2005.