

SEGURANÇA EM REDES WIRELESS: VULNERABILIDADES, AMEAÇAS E ESTRATÉGIAS DE MITIGAÇÃO NA ERA DA IOT

SECURITY IN WIRELESS NETWORKS: VULNERABILITIES, THREATS, AND MITIGATION STRATEGIES IN THE IOT ERA

Magno Isidorio de Souza Quaresma¹

RESUMO

O artigo aborda os desafios trazidos pela Internet das Coisas (IoT) e tem como objetivo analisar as fragilidades das redes wireless, identificando estratégias de mitigação dos riscos, que se intensificam com o crescimento da IoT. A justificativa do estudo está na crescente popularidade das redes sem fio, que oferecem vantagens como mobilidade e flexibilidade, mas ampliam as ameaças à segurança, já que suas comunicações via frequências de rádio são mais suscetíveis à interceptação de dados. A pesquisa destaca que, embora tecnologias como criptografia e autenticação sejam comuns para mitigar essas ameaças, a gestão adequada é essencial, pois muitas falhas de segurança estão na configuração e administração das redes. A metodologia é baseada em uma revisão bibliográfica de publicações entre 2014 e 2023, coletadas no Google Acadêmico, com análise de vulnerabilidades como ataques de interceptação e falhas nos protocolos WEP e WPA, além de riscos associados à adoção de IoT. Os resultados mostram que as redes sem fio, especialmente em ambientes IoT, enfrentam desafios significativos, com vulnerabilidades em protocolos de autenticação e criptografia. Embora o WPA3 tenha melhorado em relação ao WPA2, ataques como downgrade e canal lateral ainda podem comprometer os sistemas. A popularização da IoT traz novas demandas, como baixo consumo de energia e escalabilidade, agravando a segurança, pois muitos dispositivos IoT utilizam criptografia fraca ou inexistente. Para mitigar essas vulnerabilidades, o estudo recomenda uma abordagem multifacetada, com criptografia ponta a ponta, protocolos robustos como o TLS e estratégias de gerenciamento de risco que integrem tecnologia e capacitação de administradores. Práticas como segmentação de redes, autenticação multifatorial e uso de VPNs são essenciais. O artigo conclui que, apesar de não ser possível eliminar totalmente os riscos, boas práticas de gestão e criptografia avançada podem reduzir significativamente as ameaças, especialmente em ambientes IoT, onde a segurança deve ser prioridade.

Palavras-chave: IoT; Segurança. Wireless Network.

¹ Graduando em Redes de computadores pelo Centro Universitário UNA. Contato:

ABSTRACT

The article addresses the challenges posed by the Internet of Things (IoT) and aims to analyze the vulnerabilities of wireless networks, identifying risk mitigation strategies that intensify with the growth of IoT. The study's justification lies in the increasing popularity of wireless networks, which offer advantages such as mobility and flexibility, but also expand security threats, as their communications via radio frequencies are more susceptible to data interception. The research highlights that, although technologies like encryption and authentication are common in mitigating these threats, proper management is essential, as many security flaws lie in the configuration and administration of networks. The methodology is based on a bibliographic review of publications between 2014 and 2023, collected from Google Scholar, analyzing vulnerabilities such as interception attacks and flaws in WEP and WPA protocols, as well as risks associated with the adoption of IoT. The results show that wireless networks, especially in IoT environments, face significant security challenges, with vulnerabilities in authentication and encryption protocols. Although WPA3 has improved over WPA2, attacks like downgrade and side-channel attacks can still compromise systems. The popularization of IoT brings new demands, such as low power consumption and scalability, which worsen security as many IoT devices use weak or non-existent encryption. To mitigate these vulnerabilities, the study recommends a multifaceted approach, including end-to-end encryption, robust protocols like TLS, and risk management strategies that integrate technology and administrator training. Practices like network segmentation, multifactor authentication, and VPN use are essential. The article concludes that, while it is impossible to completely eliminate risks, good management practices and advanced encryption can significantly reduce threats, especially in IoT environments, where security should be a top priority.

Keywords: IoT; Security; Wireless Network.

1. INTRODUÇÃO

As redes sem fio oferecem inúmeras vantagens, como mobilidade, flexibilidade e facilidade de configuração, tornando-se uma escolha cada vez mais comum em diversos ambientes. No entanto, essas mesmas redes também ampliam o leque de ameaças à segurança, já que suas comunicações via frequências de rádio são mais suscetíveis à interceptação e a outras formas de ataque.

Com o crescimento exponencial da Internet das Coisas (IoT), a quantidade de dispositivos conectados a essas redes se multiplica, ampliando a superfície de ataque e expondo vulnerabilidades antes menos exploradas. A segurança nas redes sem fio, portanto, tornou-se

um tema central, especialmente em contextos que envolvem a IoT, onde dispositivos frequentemente operam com capacidades de criptografia limitadas ou inexistentes.

A fragilidade de protocolos de segurança como WEP, WPA e WPA2, bem como os desafios impostos pela adoção de WPA3, evidenciam a necessidade urgente de estratégias robustas de mitigação de riscos. Nesse contexto, a gestão inadequada das redes e a configuração deficiente tornam-se os principais pontos de falha, o que justifica a necessidade de estudos aprofundados sobre o tema. Assim, o presente estudo tem como objetivo analisar as principais vulnerabilidades das redes sem fio no contexto da IoT, abordando as deficiências dos protocolos de segurança atuais e propondo estratégias de mitigação que possam efetivamente reduzir os riscos de segurança associados a esses ambientes.

Diante desse cenário, a segurança em redes wireless, especialmente em ambientes IoT, apresenta-se como um desafio significativo para especialistas e administradores de redes. A crescente conectividade de dispositivos e a utilização de redes sem fio em setores críticos, como saúde e indústria, trazem à tona uma questão central: quais são as principais vulnerabilidades presentes nas redes wireless em ambientes de IoT e como é possível mitigá-las de forma eficaz? A resposta a essa questão exige uma análise abrangente dos protocolos de segurança adotados, dos métodos de configuração e gerenciamento de redes, bem como das práticas de uso inadequadas que acabam por ampliar as ameaças existentes. A busca por uma solução para essa problemática envolve não apenas a implementação de novas tecnologias de segurança, mas também uma mudança na forma como as redes wireless são administradas e protegidas.

Dessa forma, este estudo formula duas hipóteses centrais para guiar sua investigação. A primeira hipótese (H1) considera que as estratégias de segurança tradicionais, amplamente utilizadas em redes wireless, são insuficientes para proteger adequadamente essas redes em ambientes IoT, em razão das características específicas dos dispositivos conectados, que muitas vezes operam com criptografia limitada ou inexistente. Já a segunda hipótese (H2) propõe que a adoção de tecnologias mais avançadas, como o WPA3, combinada com a implementação de boas práticas de gerenciamento de redes e o uso de criptografia ponta a ponta, seria uma solução eficaz para mitigar os riscos de segurança em redes wireless no contexto da IoT. Testar essas hipóteses permitirá identificar não apenas as fragilidades existentes, mas também as soluções

mais viáveis para garantir a segurança em um cenário de conectividade cada vez mais ampla e desafiadora.

2. FUNDAMENTAÇÃO TEÓRICA

A IoT abrange uma ampla gama de aplicativos e dispositivos. Exemplos de aplicativos Wi-Fi na IoT são apresentados em Li *et al.* (2021). Hoje, quase todas as casas, locais de trabalho, cafés e universidades têm uma rede Wi-Fi. Wi-Fi tornou-se o termo de fato quando se refere à conexão com a Internet por meio de um ponto de acesso sem fio. A ampla adoção do Wi-Fi o torna a primeira escolha de tecnologia para muitos aplicativos de IoT. No entanto, em algumas aplicações de IoT, a escolha da tecnologia é limitada aos recursos de hardware dos dispositivos, requisitos de baixo consumo de energia e custo geral.

Muitos dispositivos IoT exigem o uso de um sistema de tecnologia sem fio de baixo custo e baixo consumo de energia ao se conectar à Internet (Want, Schilit, Jenson, 2015). Tradicionalmente, o consumo de energia sempre foi um fator limitante em muitas aplicações de rede de sensores sem fio. Este fator limitante continuará como um grande desafio enfrentado pelo desenvolvimento de muitas aplicações na IoT. Para o crescimento da IoT, o baixo consumo de energia é um requisito essencial que precisa ser atendido.

Para além do baixo consumo de energia, outros requisitos associados devem ser considerados como, por exemplo, o custo da tecnologia, segurança, simplicidade (fácil de usar e gerenciar), taxas e intervalos de dados, entre outros, como os relatados em Christin *et al.* (2019), são requisitos essenciais que requerem atenção.

O rápido crescimento da tecnologia sem fio traz preocupações legítimas sobre a segurança e a privacidade dos dados transmitidos continuamente. Com vários aplicativos, vêm várias considerações de segurança. A tecnologia sem fio geralmente desempenha um papel crítico na autenticação de serviços de Internet, um processo necessário para confirmar a identidade dos usuários que buscam acesso a esses serviços. A autenticação é normalmente realizada por meio de fatores como senhas, números de identificação pessoal ou biometria, entre outros. Paralelamente à autenticação, existe o conceito de autorização, onde diferentes sistemas

são configurados com vários níveis de autorização, concedendo aos usuários diferentes graus de acesso (Rathod *et al.*, 2022).

Em sistemas que combinam autenticação e autorização, um volume considerável de dados é frequentemente retransmitido, englobando vários tipos que requerem criptografia para proteção. A criptografia adiciona uma camada de complexidade que torna mais desafiador para indivíduos não autorizados acessar os dados sem a devida autorização e autenticação. Apesar dessas medidas de segurança, vários métodos foram desenvolvidos para explorar vulnerabilidades e obter acesso aos dados, potencialmente causando danos significativos aos proprietários dos dados. Portanto, proteger a tecnologia sem fio é de suma importância para estabelecer sistemas robustos e seguros que possam impedir danos potenciais.

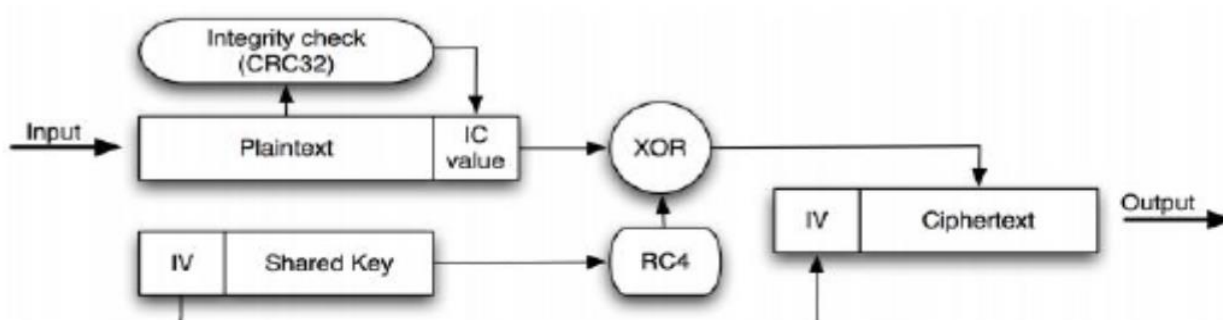
2.1 VULNERABILIDADES EM REDES WIRELESS

2.1.1 Wired Equivalent Privacy (WEP)

WEP é um algoritmo de criptografia desenvolvido por um grupo de voluntários do IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos), cujo objetivo é fornecer uma comunicação segura por sinais de rádio entre usuários das duas extremidades de uma WLAN. O WEP emprega o algoritmo RC4 para criptografia e usa dois tamanhos de chave: 40 bits e 104 bits; Para cada um é adicionado um vetor de inicialização de 24 bits (IV) que é transmitido diretamente. No lado do transmissor, o texto simples é XOR com o fluxo de chaves, gerado após KSA e o processo PRGA de RC4 e texto cifrado é obtido.

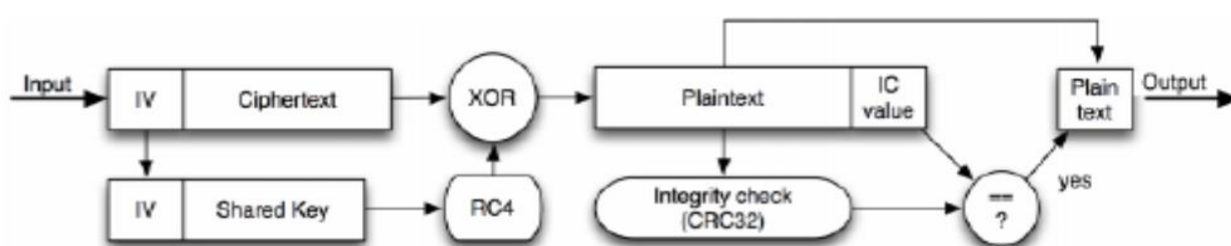
Estas etapas ocorrem na ordem inversa no lado do receptor usando a mesma chave. WEP usa algoritmo CRC-32 para integridade de dados (Santhadevi, Kareer, Tokas, 2016). As figuras a seguir apresentam os processos de criptografia e descriptografia WEP.

Figura 1 – Criptografia WEP



Fonte: Santhadevi, Kareer, Tokas (2016)

Figura 2 – Descriptografia WEP



Fonte: Santhadevi, Kareer, Tokas (2016)

Segundo Gutjahr (2012) as principais vulnerabilidades do protocolo WEP são:

- Não impedir a falsificação de pacotes;
- Não impedir ataques de repetição: um atacante pode simplesmente gravar e reproduzir pacotes conforme desejado e eles serão aceitos como legítimos;
- Usar RC4 incorretamente: as chaves usadas são muito fracas e podem ser forçadas, usando livremente software disponível;
- Reutilizar vetores de inicialização. Uma variedade de métodos criptoanalíticos disponíveis podem descriptografar dados sem saber a chave de criptografia.
 - Permitir que um invasor modifique (sem ser detectado) uma mensagem sem saber a chave de criptografia.
 - Não possuir gerenciamento adequado de chaves

2.1.2 Wi-Fi Protected Access (WAP)

O mecanismo de segurança de segunda geração para fornecer comunicação mais confiável é 802.11i (também chamado WAP2), mas uma solução intermediária chamada WPA foi desenvolvida. Nesta solução, o Protocolo de Integridade de Chave Temporal (TKIP) foi projetado como um patch para WEP nesta solução. TKIP também emprega o algoritmo RC4, mas inclui algumas modificações. Durante a comunicação, as chaves são alteradas dinamicamente e um vetor de inicialização muito maior (48 bits) é usado (Menezes, 2012).

Uma função de mixagem de teclas é usada para diferentes teclas em cada sessão. A fim de fornecer a integridade dos dados durante a transmissão, um novo algoritmo chamado Michael é usado como código de integridade de mensagem (MIC). Em breve, o TKIP fornece combinação de chaves de pacotes, uma verificação da integridade da mensagem e um mecanismo de chaveamento

O WPA fez um excelente trabalho ao corrigir os problemas do WEP. Com apenas uma atualização de software, corrigiu todos os problemas de segurança criados ou ignorados pelo WEP. No entanto, o WPA também criou novos problemas:

- Uma falha permite que um invasor cause um ataque de negação de serviço, se o invasor puder ignorar várias outras camadas de proteção.
- Existe uma segunda falha no método com o qual o WPA inicializa seu esquema de criptografia. Consequentemente, é realmente mais fácil quebrar o WPA do que quebrar WEP.

2.1.3 WAP2 (802.11i)

A solução de longo prazo projetada para redes sem fio pelo Task Group i (TGi) é o 802.11i (também chamado de WPA2). Esse protocolo, que foi ratificado como padrão em 2004, não emprega RC4 como WEP ou WPA; utiliza o modo de contador com CBC-Protocolo MAC

(CCMP) para criptografar o tráfego de rede. CCMP emprega o Advanced Encryption Standard (AES) como algoritmo de criptografia. O WPA2 é compatível com versões anteriores de WPA, mas não com WEP (Moreno, 2016).

De acordo com Lima e Silva (2021), ao contrário do WEP, onde métodos estatísticos podem ser usados para acelerar o processo de quebra, geralmente apenas técnicas brutas puras podem ser usadas contra WPA/WPA2 em uma tentativa de descobrir a senha. Ou seja, porque a chave não é estática, então a coleta de vetores de inicialização não acelerar o ataque. Isso significa que a senha deve estar contida no dicionário que está sendo usado para quebrar WPA/WPA2.

A única coisa que dá a informação para iniciar um ataque é o *handshake* entre o cliente e o AP. O *handshake* é feito quando o cliente se conecta à rede e, durante o *handshake*, o AP e cada estação precisam de uma chave transitória de pares (PTK) individual para proteger a comunicação unicast entre eles. O PTK é derivado do PMK (Pairwise Master Key), uma string, o endereço MAC do AP, o endereço MAC do cliente e dois números aleatórios.

A fraqueza do WPA-PSK é baseada na chave mestra de pares (PMK) que é derivada da concatenação da frase secreta, SSID, comprimento do SSID e nonce's (um número ou string de bits usado apenas uma vez em cada sessão). Este é o algoritmo: $PMK = PBKDF2(\text{senha}, \text{SSID}, \text{comprimento do SSID}, 4096, 256)$. A string de resultado é hash 4.096 vezes para gerar um valor e, em seguida, combinado com valores nonce. Como já mencionado, o PTK é derivado do PMK usando o 4-Way Handshake e todas as informações usadas são transmitidas em texto simples. Ao capturar o 4-Way Handshake, obtém-se os dados necessários para sujeitar a senha em um ataque de dicionário.

2.1.4 WAP3

Em junho de 2018, a Wi-Fi Alliance anunciou o Wi-Fi Protected Access 3 (WPA3) e, em julho de 2020, o WPA3 tornou-se obrigatório para implementações certificadas por Wi-Fi. Esperava-se que a taxa de adoção do WPA3 crescesse rapidamente, mas as estatísticas mostraram o oposto disso (Lamers *et al.*, 2021).

O aprimoramento da segurança do *handshake* WPA2-PSK foi a principal motivação para o desenvolvimento do WPA3. Pesquisadores independentes não conseguiram revisar os recursos recém-implementados desde o desenvolvimento do WPA3, o processo foi mantido em segredo do público. O WPA3, semelhante ao seu antecessor, tem dois modos de operação: WPA3-Pessoal e WPA3-Empresarial.

WPA3 permite um modo de transição em que WPA2 e WPA3 são suportados simultaneamente para fornecer compatibilidade. WPA3-personal está usando autenticação simultânea de Iguais (SAE), que representa um protocolo de troca segura de chaves entre pares projetado para atender a propósitos de autenticação (Al-Mejibli, Alharbe, 2020).

E assim, a autenticação é realizada com base em uma senha compartilhada entre todos os handshakes. Uma Chave Mestra em Pares (PMK) de alta entropia é a saída da autenticação WPA3-SAE, que será utilizada como entrada para o handshake de 4 vias para criar um Pairwise (Vanhoef, Ronen, 2019)

Existem muitas vulnerabilidades que foram encontradas em protocolos de segurança sem fio anteriores que causam danos às redes ou adquirem controle indesejado. WPA2 foi modificado e atualizado para WPA3 em um esforço para melhorar a segurança abordando essas vulnerabilidades.

2.2 TIPOS COMUNS DE ATAQUES

2.2.1 Downgrade contra o modo de transição WPA3

Esse ataque acontece quando uma rede suporta WPA2 e WPA3. Neste ataque, o invasor cria um AP não autorizado e força o usuário que suporta WPA3 a ser conectado ao seu AP invasor que suporta apenas WPA2 e, em seguida, executar ataques no *Handshake* WPA2 para recuperar a senha. Esse ataque força os usuários a fazerem *downgrade* de WPA3 para WPA2, então a rede é vulnerável aos pontos fracos do WPA2.

2.2.2 Downgrade contra o handshake WPA3-Dragonfly

Neste ataque, o downgrade está no aperto de mão Dragonfly, onde ele usa um fraco grupo de segurança. Ao iniciar um *handshake*, um quadro de confirmação é enviado ao AP junto com o grupo de segurança. O usuário seria forçado a fazer downgrade de seu grupo de segurança depois de tentar localizar um grupo de segurança que funcionaria configurando um ponto de acesso invasor que aceita apenas um grupo de segurança fraco.

2.2.3 Ataque de canal lateral

1. Canal lateral baseado em tempo: quando um AP usa um grupo de segurança, o tempo de resposta do AP depende da senha que está sendo usada. A duração necessária para um AP responder a uma confirmação pode vazar informações sobre a senha. Um invasor pode explorar isso para executar um ataque de dicionário simulando o tempo necessário para processar cada senha e comparar o resultado com os tempos observados.
2. Canal lateral baseado em cache: quando um invasor obtém controle sobre um aplicativo no dispositivo de um usuário, ele é capaz de observar padrões de acesso à memória no dispositivo do usuário quando o dispositivo envia os quadros de confirmação durante o handshake do Dragonfly. O acesso à memória tem dados sobre a senha, que podem ser simulados pelo invasor para descobrir a senha real.

2.2.4 Rogue Access Point

Um ponto de acesso não autorizado é um ponto de acesso instalado em uma rede sem a rede permissão do proprietário. Esse ataque funciona enganando os usuários para que se conectem a um AP falso que imita uma rede legítima. Pontos de acesso não autorizados, também conhecidos como roteadores não autorizados, são dispositivos configurados intencionalmente

por indivíduos para enganar os usuários da rede sem fio. Esses criminosos configuram um roteador para replicar o Service Set Identifier (SSID) de uma rede Wi-Fi legítima (Jang *et al.*, 2020).

Para um usuário desavisado, o Wi-Fi SSID visto em seus dispositivos parece idêntico. Os usuários geralmente assumem que esse SSID pode pertencer a uma banda Wi-Fi diferente, como a banda de 5 Gigahertz ou 2,4 Gigahertz, e pode se conectar a qualquer SSID sem pensar muito. No entanto, o perigo reside no fato de que esses pontos de acesso não autorizados podem não fornecer transmissão de dados criptografados entre o host e os clientes, aumentando assim o risco de ser vítima de ataques de phishing e outras formas de lacunas de segurança (Beyah, Venkataraman, 2016).

Caso o usuário se conecte inadvertidamente ao ponto de acesso não autorizado, que é controlado pelo invasor mal-intencionado, se torna vulnerável a várias formas de ataques. Todo o tráfego da Internet passa pelos dispositivos do invasor antes de chegar ao servidor pretendido e as respostas do servidor também passam pelo equipamento do invasor. Isto implica que cada dado, cada pacote, transmitido entre o usuário e o servidor de forma eficaz passa pelo atacante. Como resultado, o invasor ganha a capacidade de monitorar e interceptar todas as informações pessoais e confidenciais pertencentes à vítima. Isso, por sua vez, pode levar a perdas substanciais e violações significativas de privacidade para a vítima.

2.2.5 Negação de Serviço

Existem dois tipos principais de ataques de negação de serviço. A principal diferença entre esses dois tipos de ataques está no número de computadores ou dispositivos usados para executar o ataque, que pode envolver um único dispositivo ou vários. Um ataque que emprega apenas um computador para interromper o sistema de destino é conhecido como ataque de negação de serviço. Por outro lado, um ataque que utiliza mais de um computador ou dispositivo para interromper o sistema de destino é chamado de ataque de negação de serviço distribuído.

Em um ataque de negação de serviço, o dispositivo de origem envia um volume esmagador de dados desnecessários para o dispositivo alvo, como gateways de rede, switches

de rede, roteadores, pontos de acesso de rede e muito mais, com a intenção de causar interrupção na rede de destino (Muzafar *et al.*, 2022).

Essas interrupções podem resultar em tempo de inatividade prolongado da rede, falhas de rede e respostas de rede lentas. A facilidade de lançamento desses ataques, juntamente com sua exigência mínima de conhecimento especializado, contribui para sua prevalência. Vale a pena notar que estes ataques podem ser iniciados por meio de redes sem fio, bem como a World Wide Web, o que significa que mesmo as redes públicas correm o risco de serem alvo e comprometidas por ataques de negação de serviço (Muzafar, Jhanjhi, 2022).

2.3 ESTRATÉGIAS DE MITIGAÇÃO

2.3.1 Metodologias aplicadas na estratégia de mitigação

É importante ressaltar que, embora WEP, WPA-PSK e WPA2-PSK estejam usando técnicas de criptografia para fornecer controle de acesso e proteção contra-ataques, isso ocorre somente no tráfego sem fio entre o cliente e o ponto de acesso, não na parte com fio do caminho de comunicação. Para a proteção se completa, é necessária criptografia de ponta a ponta.

A maioria dos usuários não sabe que seus e-mails privados, conversas de bate-papo e até senhas são frequentemente enviados "sem criptografia" por dezenas de redes não confiáveis antes de chegar ao seu destino final na Internet. Por mais equivocados que possam estar, os usuários ainda costumam ter alguma expectativa de privacidade ao usar redes de computadores. A privacidade pode ser alcançada, mesmo em redes não confiáveis, como pontos de acesso públicos e a Internet. O único método comprovadamente eficaz para proteger a privacidade é o uso de criptografia forte de ponta a ponta.

Essas técnicas funcionam bem mesmo em redes públicas não confiáveis, onde os bisbilhoteiros estão ouvindo e possivelmente até manipulando dados provenientes de um ponto de acesso. Para garantir a privacidade dos dados, uma boa criptografia de ponta a ponta deve fornecer os seguintes recursos:

- Autenticação verificada da extremidade remota. O usuário deve ser capaz de

saber, sem dúvida, que a extremidade remota é quem afirma ser. Sem autenticação, um usuário pode fornecer dados confidenciais a qualquer pessoa que afirme ser o serviço legítimo;

- Métodos de criptografia fortes: o algoritmo de criptografia deve resistir ao escrutínio público e não deve ser facilmente descriptografado por terceiros. Não há segurança na obscuridade, e a criptografia forte é ainda mais forte quando o algoritmo é amplamente conhecido e sujeito à revisão por pares. Um bom algoritmo com uma chave adequadamente grande e protegida pode fornecer criptografia que provavelmente não será quebrada por qualquer esforço usando a tecnologia atual;
- Criptografia de chave pública: embora não seja um requisito absoluto para criptografia de ponta a ponta, o uso de criptografia de chave pública em vez de uma chave compartilhada pode garantir que os dados de um indivíduo permaneçam privados, mesmo que a chave de outro usuário do serviço seja comprometida. Ele também resolve certos problemas com a distribuição de chaves para usuários em redes não confiáveis;
- Encapsulamento de dados: um bom mecanismo de criptografia de ponta a ponta protege o máximo de dados possível. Isso pode variar desde a criptografia de uma única transação de e-mail até o encapsulamento de todo o tráfego IP, incluindo pesquisas de DNS e outros protocolos de suporte. Algumas ferramentas de criptografia simplesmente fornecem um canal seguro que outros aplicativos podem usar. Isso permite que os usuários executem qualquer programa que desejarem e ainda tenham a proteção de criptografia forte, mesmo que os próprios programas não a suportem.

2.3.2 Tecnologias aplicadas na estratégia de mitigação

A tecnologia de criptografia de ponta a ponta mais amplamente disponível é o Transport Layer Security, conhecido simplesmente como TLS (ou seu antecessor SSL: Secure Sockets

Layer). Integrado em praticamente todos os navegadores da Web e em muitos outros aplicativos, o TLS usa criptografia de chave pública e uma infraestrutura de chave pública (PKI) confiável para proteger as comunicações de dados na Web.

A implementação do TLS incorporada aos navegadores da Web inclui uma coleção de certificados de organizações chamadas Autoridades de Certificação (CA). Uma CA valida a identidade dos usuários e/ou provedores da rede e garante que eles são quem dizem ser e emite um certificado dizendo isso.

Em vez de fazer isso por meio de um documento sofisticado assinado adequado para enquadramento, isso é feito por meio da troca de chaves criptográficas. Por exemplo, alguém que deseja um certificado para seu site envia uma CR (Solicitação de Certificado), codificada ("assinada") com uma chave criptográfica criada especificamente para assinar a solicitação de certificado. Eles enviam essa solicitação à CA, que então "assina" a solicitação com sua própria chave. Eles são codificados no certificado junto com o nome exato do site para o qual o solicitante deseja que o certificado seja válido.

Ao navegar para um site que usa TLS, o navegador e o servidor trocam certificados. Em seguida, o navegador verifica se o nome do host no certificado fornecido pelo servidor corresponde ao nome do host DNS pelo qual o navegador conhece o servidor, se o certificado não expirou ou foi revogado e se foi assinado por uma autoridade de certificação confiável. O servidor verifica opcionalmente a validade do certificado do navegador. Se os certificados forem aprovados, ambos os lados negociarão uma chave de sessão mestra usando os certificados trocados anteriormente para proteger a sessão que está sendo estabelecida. Essa chave é então usada para criptografar todas as comunicações até que o navegador se desconecte. Esse tipo de encapsulamento de dados é conhecido como túnel.

Outra tecnologia utilizada é o protocolo SSH (Secure Shell), que estabelece uma conexão entre o dispositivo de um usuário e uma máquina distante, geralmente um servidor. Ele usa criptografia para embaralhar os dados que atravessam a conexão. Ao estabelecer uma conexão SSH com um local confiável próximo (ou mesmo em) um servidor remoto, os protocolos inseguros podem ser protegidos. Como o TLS, ele usa criptografia de chave pública forte para verificar o servidor remoto e criptografar dados. Em vez de uma PKI, ele usa um

cache de fingerprint de chave que é verificado antes que uma conexão seja permitida. Pode usar senhas e chaves públicas para autenticação do usuário e, por meio de seu suporte ao sistema Pluggable Authentication Modules (PAM), também pode oferecer suporte a outros métodos de autenticação.

Embora essa técnica possa ser um pouco avançada para muitos usuários, os arquitetos de rede podem usar o SSH para criptografar o tráfego em links não confiáveis, como links ponto a ponto sem fio. Como as ferramentas estão disponíveis gratuitamente e são executadas em TCP padrão, qualquer usuário instruído pode implementar conexões SSH por conta própria, fornecendo sua própria criptografia de ponta a ponta sem intervenção do administrador.

Também é bastante utilizada a tecnologia OpenVPN, que é uma implementação de VPN construída em criptografia SSL com uma edição "comunitária" licenciada comercialmente e de código aberto. Tem algumas desvantagens, como latência bastante alta de tráfego no túnel VPN. Alguma quantidade de latência é inevitável, pois toda a criptografia/descriptografia é feita no espaço do usuário, mas o uso de computadores relativamente novos em cada extremidade do túnel pode minimizar isso.

Porém, tem muitas vantagens que o tornam uma boa opção para fornecer segurança de ponta a ponta, tais como:

- é baseado em protocolos de criptografia comprovados e robustos (SSL e RSA);
- funciona em muitas plataformas diferentes;
- está bem documentado.

Uma versão "Comunidade" de código aberto é mantida, além de uma versão comercial paga. O OpenVPN precisa se conectar a uma única porta TCP ou UDP no lado remoto. Uma vez estabelecido, ele pode encapsular todos os dados até a camada de rede ou até mesmo até a camada de link de dados, se sua solução exigir. Pode ser utilizado para criar conexões VPN robustas entre máquinas individuais ou simplesmente para conectar roteadores de rede em redes sem fio não confiáveis.

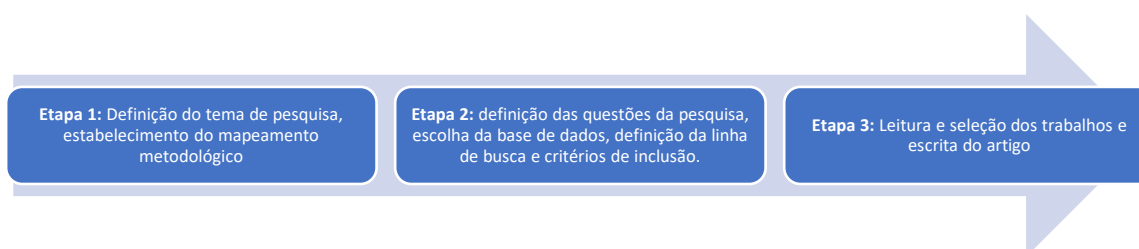
3. MÉTODOS

Este trabalho se desenvolveu a partir de uma pesquisa bibliográfica, realizada por meio de dados levantados através do Google Acadêmico. Realizou-se a busca com o objetivo de selecionar trabalhos, revistas, livros entre outros meios de informações que abordassem o tema de soluções para os resíduos plásticos pós-consumo. O levantamento bibliográfico, segundo Zamberlan *et al.* (2014) abrange todo o referencial teórico publicado e é uma etapa de pesquisa caracterizada em obter uma resposta por meio de referências teóricas publicadas em documentos (MICHEL, 2015).

Quanto à pesquisa bibliográfica, Marconi e Lakatos (2017) ensinam que a fonte da coleta de dados da pesquisa está limitada a documentos escritos ou não, o que constituem como fontes primárias, podendo ser recolhidas no momento em que o fenômeno ocorreu ou após. Matias-Pereira (2016) contribui acerca da pesquisa bibliográfica, dizendo que ela tem como objetivo reunir, classificar e distribuir os documentos de todos os gêneros, é composta de documentos que não utilizaram documentos analíticos.

Para a busca dos trabalhos que correspondessem ao objetivo proposto pelo presente artigo, foi conduzida buscas na base de dados Google Acadêmico com a combinação dos descritores (“REDES” + “WIRELESS”) OR (“WIRELESS” + “SEGURANÇA”) OR (“WIRELESS” + “SEGURANÇA” + “IOT”) OR (“REDES” + “WIRELESS” + “SEGURANÇA”), nos títulos das publicações de 2014 a 2023 e com acesso disponíveis. As etapas do processo de busca são apresentadas a seguir.

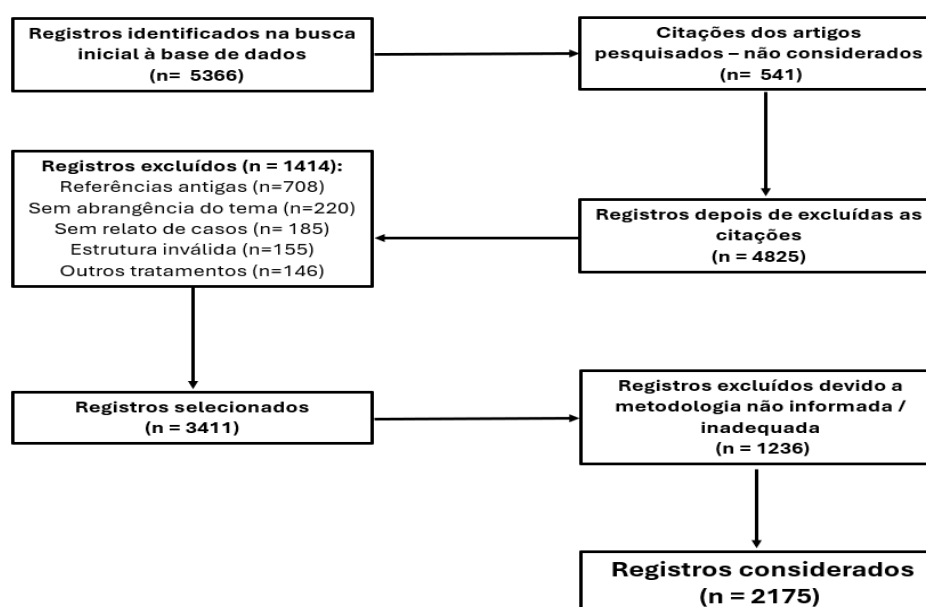
Figura 3 – Etapas do Processo de busca



Fonte: Elaboração própria

O detalhamento do processo de busca seguiu o método Para a busca dos trabalhos que correspondessem ao objetivo proposto pelo presente artigo, foi conduzida buscas na base de dados Google Acadêmico com a combinação dos descritores (“REDES” + “WIRELESS”) OR (“WIRELESS” + “SEGURANÇA”) OR (“WIRELESS” + “SEGURANÇA” + “IOT”) OR (“REDES” + “WIRELESS” + “SEGURANÇA”), nos títulos das publicações de 2014 a 2023 e com acesso disponíveis. O fluxograma detalhado das etapas do processo de seleção de estudos é apresentado a seguir.

Figura 4 – Fluxograma detalhado das etapas do processo de seleção de estudos



Fonte: Elaboração própria

4. RESULTADOS E DISCUSSÃO

Ao acessar a base com os descritores especificados, foram encontrados os resultados mostrados na tabela a seguir.

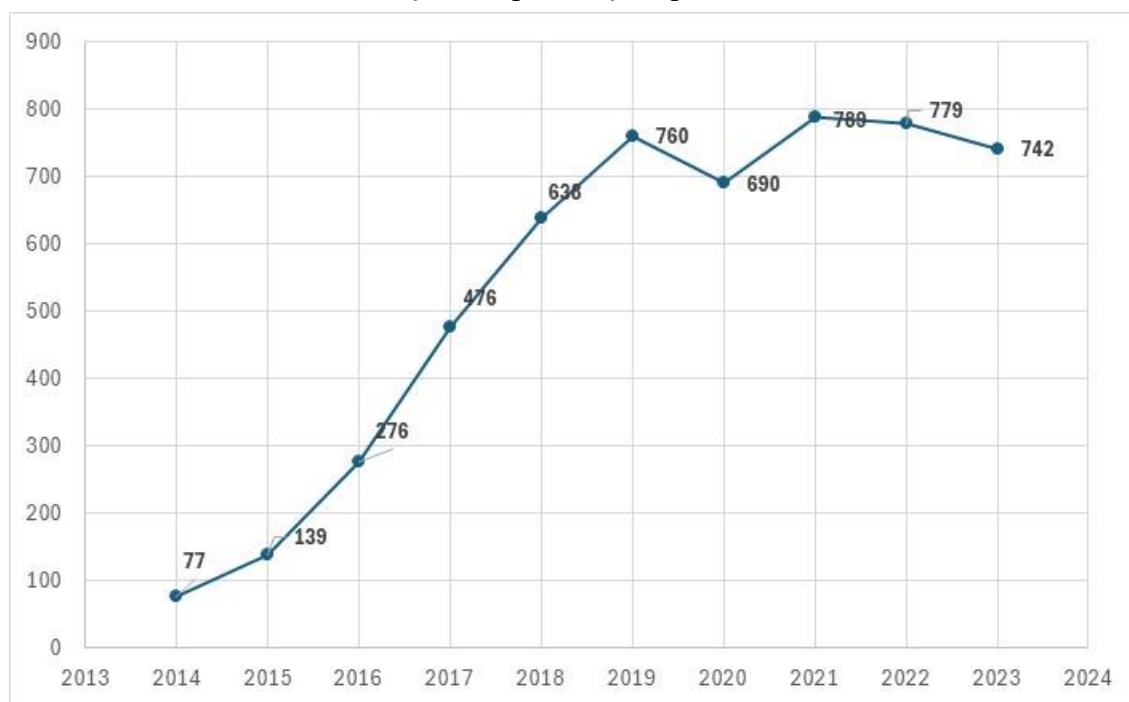
Tabela 1 – Resultados da pesquisa na base de dados Google acadêmico – 2014 a 2023

Ano	Quantidade
2023	742
2022	779
2021	789
2020	690
2019	760
2018	638
2017	476
2016	276
2015	139
2014	77
Total	5366

Fonte: Elaborado pelo autor com base nos resultados da pesquisa

Como se pode observar na Tabela 1, há uma quantidade elevada de publicações, com crescimento consistente nos anos do período pesquisado, o que induz ao entendimento de se tratar de um tema tem alta relevância para os acadêmicos.

O Gráfico 1 fornece uma melhor visualização da distribuição das publicações no período pesquisado, mostrando que houve um crescimento mais ressaltado no período da pandemia de Covid-19, o que é coerente uma vez que nesse período, devido ao isolamento social, aumentou a demanda pela utilização dos serviços de acesso remoto para trabalhar em casa.

Gráfico 1 – Distribuição das publicações por ano de 2014 a 2023

Fonte: Elaborado pelo autor com base nos resultados da pesquisa

Ao executar uma nova série de pesquisas na base, desta vez excluindo as citações do critério de seleção, foram obtidas as quantidades mostradas na Tabela 2.

Tabela 2 – Resultados da pesquisa na base de dados Google acadêmico – 2014 a 2023 – expurgadas as citações do critério de seleção

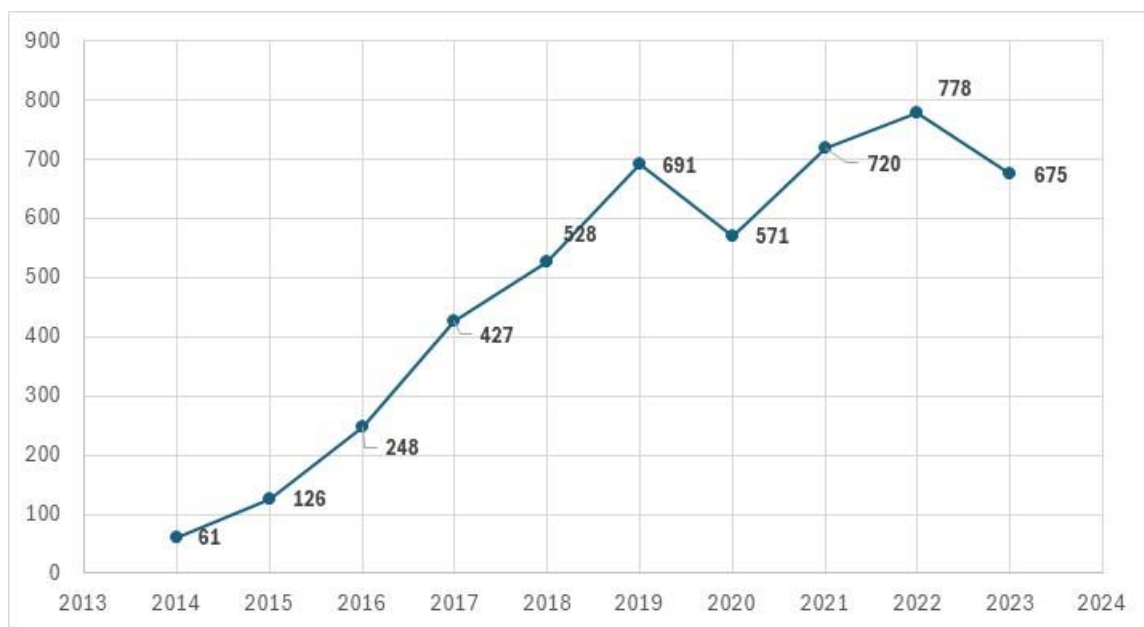
Ano	Quantidade
2023	675
2022	778
2021	720
2020	571
2019	691

2018	528
2017	427
2016	248
2015	126
2014	61
Total	4825

Fonte: Elaborado pelo autor com base nos resultados da pesquisa

Como se pode observar na Tabela 2, ao expurgar as citações dos resultados da primeira pesquisa, não ocorre uma redução significativa nos números obtidos. O Gráfico 2 apresenta a visualização da distribuição das publicações no período pesquisado, quando expurgadas as citações.

Gráfico 2 – Distribuição das publicações por ano de 2014 a 2023 - expurgadas as citações do critério de seleção



Fonte: Elaborado pelo autor com base nos resultados da pesquisa

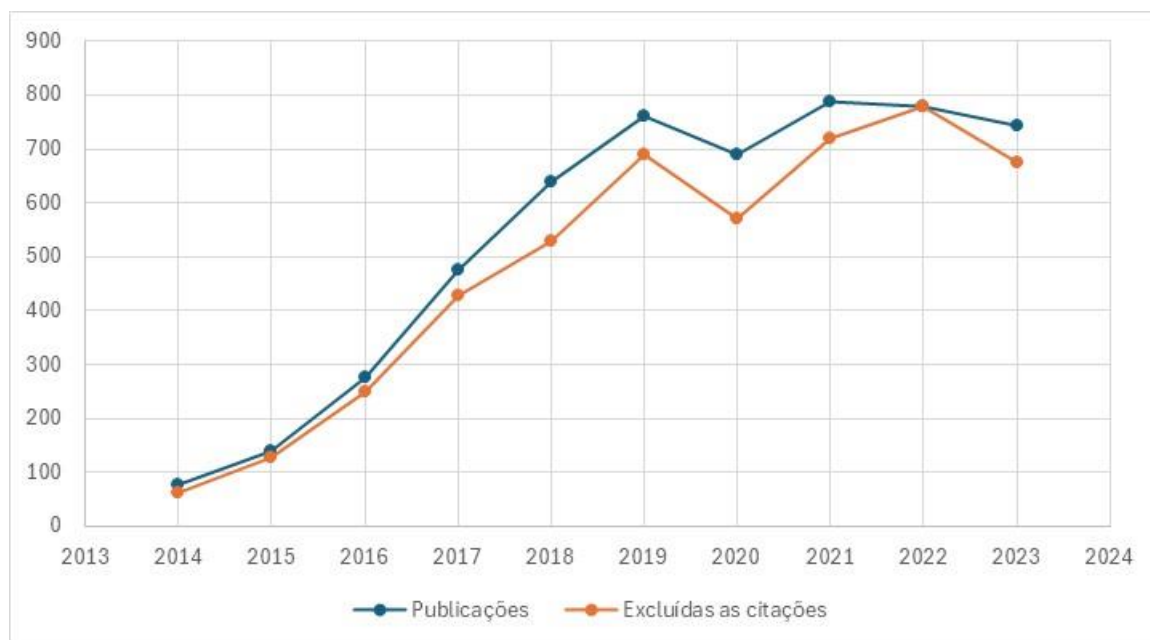
A seguir é apresentada uma análise da comparação entre a quantidade de publicações considerando as citações e a quantidade de publicações sem considerar as citações. Pode-se observar que as duas linhas praticamente estão sobrepostas, o que indica que os estudos publicados sobre o tema não foram muito citados até essa data.

Tabela 3 – Comparação entre as publicações considerando e não considerando as citações, resultantes da pesquisa na base de dados Google acadêmico – 2014 a 2023

Ano	Publicações	Excluídas as citações
2023	742	675
2022	779	778
2021	789	720
2020	690	571
2019	760	691
2018	638	528
2017	476	427
2016	276	248
2015	139	126
2014	77	61
Total	5366	4825

Fonte: Elaborado pelo autor com base nos resultados da pesquisa

Gráfico 3 – Distribuição da comparação entre as publicações considerando e não considerando as citações, resultantes da pesquisa na base de dados Google acadêmico – 2014 a 2023



Fonte: Elaborado pelo autor com base nos resultados da pesquisa

5. CONCLUSÃO

A pesquisa mostrou que, mesmo com o avanço de protocolos de segurança como o WPA3, ainda existem falhas exploráveis, como ataques de downgrade e de canal lateral, que podem comprometer a segurança dessas redes. As fragilidades dos dispositivos IoT, que muitas vezes operam com criptografia insuficiente ou inexistente, agravam esse cenário, demonstrando que as estratégias de segurança tradicionalmente aplicadas a redes wireless não são mais suficientes. As soluções sugeridas, como a adoção de criptografia ponta a ponta, autenticação multifatorial, segmentação de redes e uso de VPNs, apresentam-se como passos importantes, mas dependem de uma gestão rigorosa e bem capacitada para serem plenamente eficazes.

A partir da pergunta problemática que orientou este estudo — Quais são as principais vulnerabilidades presentes nas redes wireless em ambientes de IoT e como é possível mitigá-

las de forma eficaz? — conclui-se que a adoção de tecnologias de segurança mais avançadas, como o WPA3, combinada com práticas de gestão e administração de redes bem estruturadas, representa uma solução eficaz para mitigar as vulnerabilidades exploradas em ambientes IoT. No entanto, essas soluções não podem ser implementadas de maneira isolada. A gestão adequada dos dispositivos e das redes, aliada ao uso de criptografia forte e à atualização constante de protocolos, é fundamental para garantir a integridade e segurança das informações trafegadas. Assim, a hipótese H2, que propõe que a adoção de WPA3 em conjunto com boas práticas de gerenciamento de redes e criptografia ponta a ponta seria eficaz na mitigação dos riscos de segurança, foi confirmada.

Para futuros pesquisadores, é recomendável explorar novas estratégias de segurança que possam acompanhar o ritmo acelerado de crescimento da IoT, considerando não apenas os dispositivos em si, mas também o ecossistema em que eles operam. Além disso, a investigação sobre a aplicabilidade de sistemas de inteligência artificial e aprendizado de máquina na detecção precoce de ameaças e na automação de respostas a ataques pode trazer avanços importantes para a segurança das redes wireless. Também seria útil desenvolver estudos que foquem em ambientes específicos, como redes sem fio em hospitais ou em setores industriais, onde os desafios de segurança podem ser ainda mais críticos devido à natureza dos dados manipulados.

6. REFERÊNCIAS

- AL-MEJIBLI, I. S.; ALHARBE, N. R. **Analisando e avaliando os padrões de segurança em redes sem fio: um estudo de revisão**, Iraqi Journal for Computers and Informatics, vol. 46, no. 1, pp. 32-39, 2020.
- BEYAH, R.; VENKATARAMAN, A. **Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions**, IEEE Security & Privacy Magazine, vol. 9, no. 5, pp. 56-61, 2016.
- CHRISTIN, D.; REINHARDT, A.; MOGRE, P. S.; STEINMETZ, R. **Redes de sensores sem fio e Internet das Coisas: desafios selecionados**. 21º GI/ITG. Munique, Alemanha, 2019.
- GUTJAHR, Alexander. **Wired Equivalent Privacy (WEP) Functionality, Weak Points, Attacks**. 2012.

JANG, R.; KANG, J.; MOHAISEN, A.; NYANG, D. **Prenda-me se puder: detecção de ponto de acesso não autorizado usando interferência intencional de canal**, IEEE Transactions on Mobile Computing, vol. 19, no. 5, pp. 1056-1071, 2020.

LAMERS, E.; DIJKSMAN, R.; VAN DER VEGT, A.; SARODE, M.; LAAT, C. de. **Securing home Wi-Fi with WPA3 personal**. In 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021: IEEE, pp. 1-8.

LI, L.; XIAO GUANG, H.; KE, C.; KETAI, H. **As aplicações da rede de sensores sem fio baseada em WiFi na Internet das Coisas e na rede inteligente**. In 2021 16th IEEE Conference on Industrial Electronics and Applications (ICIEA – Virtual Conference), 2021.

LIMA, I. V.; SILVA, J. A. **Análise de vulnerabilidades e contramedidas em relação a ataques em redes sem fio**. UFAL - Campus de Arapiraca. 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 8. ed. São Paulo: Atlas, 2017.

MATIAS-PEREIRA, José. **Manual de metodologia da pesquisa científica**. 4. Ed. São Paulo: Atlas, 2016.

MENEZES, Bernard L. **Network Security and Cryptography**. Course Technology Ptr. 2012.

MICHEL, Maria Helena. **Metodologia e pesquisa científica em ciências sociais: um guia prático para acompanhamento da disciplina e elaboração de trabalhos monográficos**. 3. ed. São Paulo: Atlas, 2015.

MORENO, D. **Pentest em redes sem fio**. Novatec Editora Ltda, Sao Paulo, SP, 1ª ed. 2016.

MUZAFAR, S.; JHANJHI, N. Z.; KHAN, N. A.; ASHFAQ, F. **DDOS attack detection approaches in on software defined network**, 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Nov. 2022,

MUZAFAR, S.; JHANJHI, N. Z. **DDoS attacks on software defined Network: Challenges and issues**. 2022 International Conference on Business Analytics for Technology and Security (ICBATS), Feb. 2022,

RATHOD, T.; JADAV, N. K.; ALSHEHRI, M. D.; TANWAR, S.; SHARMA, R.; FELSEGHI, R. A.; RABOACA, M. S. **Blockchain for Future Wireless Networks: A Decade Survey**. *Sensors*, 22(11), 4182. 2022. <https://doi.org/10.3390/s22114182>.

SANTHADEVI, D.; KAREER, V.; TOKAS, S. A. **Revisão - Problemas e desafios na segurança de redes sem fio**. Vol 2, No 2. 2016.

VANHOEF, M.; RONEN, E. **Dragonblood: Uma Análise de Segurança do Handshake SAE do WPA3**, IACR Cryptol. ePrint Arch., vol. 2019, p. 383, 2019.

WANT, R.; SCHILIT, B. N.; JENSON, S. **Habilitando a Internet das Coisas**, Computer, 2015.

ZAMBERLAN, Luciano, et al. **Pesquisa em ciências sociais aplicadas**. Ijuí: Editora Unijuí, 2014.