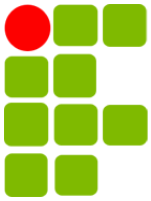


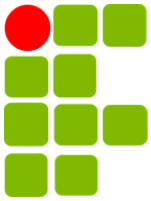
Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

Privacidade e Anonimato em IoT: Integrando a Rede Onion em *Smartphones*

WOSNEY PENAFORTE CAVALCANTE

Orientador: Professor Me. Victor Emanuel Farias da Costa Borges

Campina Grande, dezembro de 2025



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Cursos Superior de Tecnologia em Telemática

Privacidade e Anonimato em IoT: Integrando a Rede Onion em *Smartphones*

WOSNEY PENAFORTE CAVALCANTE

Monografia apresentada à Coordenação do Curso Superior de Tecnologia em Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso de Tecnologia em Telemática.

Orientador: Professor Me. Victor Emanuel Farias

Campina Grande, dezembro de 2025

C376p Cavalcante, Wosney Penaforte

Privacidade e anonimato em IoT: uma revisão bibliográfica sobre redes Onion em smartphones / Wosney Penaforte Cavalcante. - Campina Grande, 2025.

28 f.: il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) - Instituto Federal da Paraíba, 2025.

Orientador: Prof. Me. Victor Emanuel Farias da Costa Borges

1. Telemática. 2. Internet das coisas - IoT. 3. Segurança da informação - privacidade da informação. 4. Redes Onion. I. Borges, Victor Emanuel Farias da Costa. II Título.

CDU 004.738

Privacidade e Anonimato em IoT: Integrando a Rede Onion em *Smartphones*

WOSNEY PENAFORTE CAVALCANTE

Professor Me. Victor Emanuel Farias da Costa Borges
Orientador

Professor Dr. Anderson Fabiano Batista Ferreira da Costa
Membro da Banca

Professora Ma. Iana Daya Cavalcante Facundo Passos
Membro da Banca

Campina Grande, Paraíba, Brasil
Dezembro/2025

Agradecimentos

Dedico um agradecimento especial ao meu orientador, professor **Victor Emanuel Farias da Costa Borges**, pela inestimável paciência e sabedoria. Agradeço por ter mantido a orientação e o suporte, guiando-me com clareza mesmo nos momentos em que meu andamento não condizia com o esperado. Sua insistência e ajuda foram fundamentais para a conclusão desta etapa.

Estendo minha profunda gratidão aos professores **Anderson Fabiano Batista Ferreira da Costa** e **Iana Daya Cavalcante Facundo Passos**. Agradeço imensamente pela compreensão demonstrada em relação aos prazos e contratempos na entrega deste trabalho. A disponibilidade e a generosidade de vocês em avaliar este projeto, apesar das circunstâncias, são atitudes que levarei como exemplo.

Resumo

A onipresença da Internet das Coisas (IoT) transformou o cotidiano, trazendo conveniência, mas expondo usuários a riscos de vigilância massiva. Neste cenário, a Rede Onion (Tor) surge como uma arquitetura potencial para restaurar o anonimato. Este Trabalho de Conclusão de Curso (TCC) tem como objetivo investigar a viabilidade técnica e a eficácia da segurança na integração da rede Tor em ecossistemas IoT, utilizando *smartphones* como *gateways* de computação de borda. Através de uma Revisão Bibliográfica de natureza qualitativa, foram analisados estudos na base de dados da CAPES e Google Scholar, focando na intersecção entre protocolos de anonimato, limitações de hardware móvel e análise forense. A pesquisa evidenciou que, embora a rede Onion mitigue a análise de tráfego por adversários globais, sua implementação em dispositivos móveis enfrenta o desafio de equilibrar segurança e usabilidade. Identificou-se que a dependência de *timestamps* precisos e a sensibilidade à latência tornam a manutenção de circuitos estáveis difícil em redes móveis instáveis. Os resultados indicam barreiras significativas de desempenho, especificamente a sobrecarga criptográfica que compromete aplicações de tempo real. Além disso, revelou-se um paradoxo de segurança: enquanto o túnel Tor protege os dados em trânsito, o sistema operacional Android tende a armazenar rastro digital locais que podem desanonimizar o usuário. Conclui-se que a solução é promissora para cenários de alta criticidade, mas requer otimizações de protocolo e hardware para ser adotada massivamente sem degradação severa da usabilidade

Palavras-chave: internet das doisas (IoT); rede onion (Tor); smartphones; privacidade; segurança de redes; computação de borda.

Abstract

The ubiquity of the Internet of Things (IoT) has transformed daily life, bringing convenience but exposing users to massive surveillance risks. In this scenario, the Onion Network (Tor) emerges as a potential architecture to restore anonymity. This Course Conclusion Paper (TCC) aims to investigate the technical viability and security effectiveness of integrating the Tor network into IoT ecosystems, using smartphones as edge computing gateways. Through a qualitative Bibliographic Review, studies in the CAPES database were analyzed, focusing on the intersection between anonymity protocols, mobile hardware limitations, and forensic analysis. The research evidenced that while the Onion network mitigates traffic analysis by global adversaries, its implementation on mobile devices faces the challenge of balancing security and usability. It was identified that the dependence on precise timestamps and sensitivity to latency make maintaining stable circuits difficult in unstable mobile networks. The results indicate significant performance barriers, specifically the cryptographic overhead that compromises real-time applications. Furthermore, a security paradox was revealed: while the Tor tunnel protects data in transit, the Android operating system tends to store local forensic artifacts that can deanonymize the user. It is concluded that the solution is promising for high-criticality scenarios but requires protocol and hardware optimizations to be massively adopted without severe usability degradation.

Keywords: Internet of Things (IoT). Onion Network (Tor). Smartphones. Privacy. Network Security. Edge Computing.

Sumário

Lista de Siglas

CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
DNS	*Domain Name System* (Sistema de Nomes de Domínio)
EDGE	*Edge Computing* (Computação de Borda)
FOG	*Fog Computing* (Computação em Névoa)
IOT	*Internet of Things* (Internet das Coisas)
IP	*Internet Protocol* (Protocolo de Internet)
ISP	*Internet Service Provider* (Provedor de Serviços de Internet)
MQTT	*Message Queuing Telemetry Transport* (Protocolo de Transporte de Telemetria de Fila de Me
P2P	*Peer-to-Peer* (Ponto a Ponto)
PETs	*Privacy-Enhancing Technologies* (Tecnologias de Aprimoramento de Privacidade)
RTT	*Round-Trip Time* (Tempo de Ida e Volta)
TOR	The Onion Router (O Roteador Cebola)
VoIP	*Voice over Internet Protocol* (Voz sobre Protocolo de Internet)
VPN	*Peer-to-Peer* (Ponto a Ponto)
PETs	*Privacy Enhancing Technology* (Rede Privada Virtual)
Wi-Fi	*Wireless Fidelity* (Fidelidade Sem Fio)

Lista de Figuras

Capítulo 1

Introdução

A sociedade contemporânea vivencia uma transformação digital sem precedentes, impulsionada pela onipresença da Internet das Coisas (IoT). Casas, indústrias e infraestruturas críticas tornaram-se ecossistemas inteligentes, onde sensores e atuadores comunicam-se incessantemente. No entanto, essa conveniência cobra um preço oculto: a privacidade. A imensa massa de dados gerada por esses dispositivos compõe um retrato detalhado dos hábitos, rotinas e vulnerabilidades dos usuários, muitas vezes expostos a vigilância corporativa ou governamental através da análise de tráfego e metadados.

Nesse cenário de um sistema contemporâneo de vigilância e controle social, a criptografia convencional ponta-a-ponta mostra-se insuficiente, pois protege o conteúdo, mas não oculta os padrões de comunicação, o quem, onde e quando. Surge, então, a Rede Onion (Tor) como uma arquitetura promissora para restaurar o anonimato, ofuscando o rastro digital através de camadas criptográficas distribuídas globalmente. O desafio, contudo, reside na infraestrutura: como implementar protocolos robustos de anonimato, desenhados originalmente para desktops, em dispositivos de borda (Edge) com recursos limitados?

O presente trabalho propõe-se a desvendar esse dilema técnico, colocando o *smartphone*, o principal hub de controle pessoal da atualidade no centro da investigação. Ao longo desta pesquisa, explora-se não apenas a viabilidade teórica de integrar a rede Tor ao ecossistema IoT móvel, mas também as barreiras práticas impostas pela física dos processadores e pelas baterias de lítio. Através de uma Revisão Bibliográfica, este estudo confronta as promessas de privacidade com a realidade da latência de rede e dos vestígios forenses deixados em sistemas Android, oferecendo uma análise crítica sobre se a proteção da privacidade total é uma meta alcançável ou uma utopia técnica.

1.1 Justificativa e Relevância do Trabalho

A relevância deste trabalho reside na necessidade urgente de mitigar a exposição de dados sensíveis trafegados por dispositivos IoT. A literatura aponta que a superfície de ataque em redes domésticas e industriais expandiu-se drasticamente. Dispositivos IoT, frequentemente

limitados em recursos de hardware e rodando firmwares inseguros, tornaram-se vetores primários para ataques cibernéticos. Conforme destacado por [Ali Mohamed Abdelrazek 2024], essa vulnerabilidade é exacerbada pela falta de padronização de segurança, permitindo que criminosos explorem falhas simples para comprometer redes inteiras.

O *smartphone*, ao atuar como *gateway* para esses dispositivos (por exemplo, controlando câmeras de segurança ou assistentes pessoais), torna-se o ponto crítico de falha ou de defesa.

Justifica-se, portanto, uma investigação aprofundada sobre a aplicação da rede Onion neste contexto específico. Diferentemente de computadores de mesa robustos, *smartphones* enfrentam restrições severas de bateria, processamento e tolerância à latência. Entender se o protocolo Tor pode operar eficientemente nessas condições, sem degradar a usabilidade a um ponto inviável, é crucial para o desenvolvimento de futuras tecnologias de privacidade voltadas para o mercado de massa. Além disso, conforme [Arshad Mehdi Hussain 2021] alertam que a análise forense da integração Tor-Android revela nuances críticas sobre a persistência de dados, que são vitais tanto para auditores de segurança quanto para usuários finais preocupados com o rastreamento digital, pois o próprio sistema operacional pode comprometer o anonimato prometido pela rede.

1.2 Problema de Pesquisa

A aplicação da rede Onion em dispositivos móveis enfrenta um trilema técnico complexo: a infraestrutura pesada de criptografia colide com a capacidade limitada de processamento e bateria dos smartphones, enquanto a complexidade técnica cria barreiras de usabilidade intransponíveis para o usuário comum.

A arquitetura da rede Onion prioriza, por design, o anonimato em detrimento da eficiência. O tráfego de dados não percorre o caminho mais curto (ponto A ao ponto B), mas é criptografado em múltiplas camadas e saltado através de diversos nós (relays) ao redor do mundo. Em smartphones, onde a expectativa é de resposta instantânea, esse mecanismo gera uma barreira significativa. Em redes móveis (4G/5G), que já possuem instabilidades inerentes, a latência adicional introduzida pelo sistema de retransmissão torna o uso de aplicativos de tempo real, como chamadas de voz, vídeo ou automação crítica, praticamente inviável devido à baixa velocidade de navegação resultante [Islam Guangjie Liu 2021].

1.3 Objetivos

Esta seção delineia as metas centrais que orientam a presente pesquisa. Diante da complexidade de unir protocolos de anonimato robustos com dispositivos de *hardware* restrito, estabelece-se um roteiro investigativo focado na análise crítica da literatura existente. O propósito é transpor a lacuna entre a teoria da criptografia Onion e a prática da segurança móvel em IoT, definindo claramente o escopo da Revisão Bibliográfica da Literatura (RBL)

realizada.

1.3.1 Objetivo Geral

O objetivo geral deste trabalho consiste em investigar e analisar, por meio de uma Revisão Bibliográfica da Literatura (RBL) , a viabilidade técnica e a eficácia da segurança na integração da rede Onion (Tor) em ecossistemas IoT, utilizando *smartphones* como *gateways* de borda. Busca-se identificar quais arquiteturas de tunelamento são capazes de preservar o anonimato dos dados gerados por dispositivos inteligentes, confrontando essas soluções com as limitações de latência (*overhead*) e consumo de recursos inerentes à computação móvel.

1.3.2 Objetivos Específicos

• Fundamentar os conceitos de arquitetura IoT, vulnerabilidades de borda (*Edge Computing*) e o funcionamento do protocolo Onion Routing.

• Identificar na literatura acadêmica as abordagens existentes para a execução do Tor em sistemas operacionais móveis (Android) e sua interação com dispositivos IoT.

• Analisar os desafios técnicos relacionados à latência (*overhead*), consumo de recursos e detecção de tráfego malicioso em redes tuneladas.

• Discutir as limitações práticas e a discrepância entre os cenários de simulação acadêmica e a realidade da implementação física.

1.4 Metodologia

Este trabalho adota como método científico a Revisão Bibliográfica da Literatura (RBL). A abordagem é qualitativa e descritiva, visando identificar, avaliar e interpretar as pesquisas disponíveis relevantes para a questão de segurança em IoT e Tor. A busca bibliográfica concentrou-se na base de dados do Portal de Periódicos da CAPES, abrangendo estudos que conectam técnicas de anonimato, análise forense em smartphones e segurança de redes. O detalhamento dos critérios de inclusão, exclusão e o processo de seleção dos estudos será apresentado no Capítulo 3.

1.5 Organização do Trabalho

Capítulo 1: Apresenta a introdução ao tema, a justificativa da pesquisa, a definição do problema, os objetivos, geral e específicos e a metodologia empregada.

Capítulo 2:Estabelece a fundamentação teórica, abordando os conceitos de IoT, arquitetura de borda, vulnerabilidades de segurança e o funcionamento técnico da Rede Onion (Tor).

Capítulo 3:Detalha a metodologia de revisão bibliográfica, incluindo a formulação da questão de pesquisa, os termos de busca utilizados e os critérios de seleção dos artigos analisados.

Capítulo 4:Analisa e discute os resultados obtidos na literatura, confrontando as abordagens de integração Tor-IoT com os desafios técnicos de desempenho e as limitações forenses identificadas.

Capítulo 5:Apresenta as considerações finais, sintetizando as conclusões sobre a viabilidade da integração e sugerindo direcionamentos para trabalhos futuros na área.

Capítulo 2

Fundamentação Teórica

Na etapa exploratória, foi realizada Revisão Bibliográfica da Literatura (RBL) existente. O objetivo foi mapear o cenário atual e entender o principal motivo para usar a rede O rede Onion (do inglês, *The Onion Router* - Tor) em dispositivos da Internet das Coisas (do inglês, *Internet of Things* - IoT).

A pesquisa revelou que a crescente integração de dispositivos IoT na vida cotidiana, é uma preocupação central que estimula a busca por privacidade. Esse universo da IoT é frequentemente visto como uma porta de entrada para ataques cibernéticos muito mais perigosos, levantando sérias preocupações sobre vigilância e coleta extensiva de dados. Essa situação justifica o uso de redes de anonimato, como o Tor, como uma forma de proteger a segurança e a privacidade desses dispositivos [Kauser Tauqeer Safdar Malik 2022].

A segurança na borda da IoT (Edge) é um desafio multidimensional que exige não apenas criptografia forte, mas também protocolos de roteamento anônimo eficientes. Gușiță et al. (2025) [Gușiță *et al.* 2025] destacam em seu survey a necessidade de criptografia leve adaptada para dispositivos com recursos limitados, enfatizando que melhorias nos protocolos de comunicação são essenciais para viabilizar o anonimato sem sacrificar a performance operacional da rede IoT.

2.1 Internet das Coisas (IoT)

A Internet das Coisas (IoT) representa uma mudança de paradigma fundamental na computação, evoluindo da interação humano-computador para uma comunicação onipresente entre máquinas. Não se trata apenas de conectar objetos à internet, mas de criar um ecossistema pervasivo onde dispositivos físicos coletam, processam e trocam dados autonomamente para melhorar a eficiência de sistemas e a qualidade de vida humana. Conforme destacado por [Ali Mohamed Abdelrazek 2024], essa expansão massiva que abrange desde marca-passos cardíacos e sensores industriais até assistentes virtuais domésticos — gera um volume de dados sem precedentes, transformando o ambiente físico em um sistema de informação contínuo e interconectado.

Entretanto, essa capilaridade traz consigo um desafio intrínseco de heterogeneidade. A rede IoT é composta por dispositivos com capacidades extremamente díspares: de um lado, sensores minúsculos com baterias que devem durar anos e capacidade de processamento mínima; de outro, *gateways* robustos e smartphones avançados que orquestram essa rede. Essa diversidade impede a aplicação de uma solução de segurança única e monolítica, exigindo arquiteturas flexíveis que possam operar tanto na nuvem quanto na borda da rede.

Além disso, a aplicação de IoT na agricultura inteligente exemplifica como a segurança de dados é crucial mesmo em setores tradicionais. [Khan *et al.* 2021] discutem sistemas de monitoramento baseados em IoT para fazendas, onde a integridade dos dados transmitidos é vital para a tomada de decisão agronômica, reforçando que a segurança deve permear todas as verticais da IoT, não apenas as industriais ou domésticas.

2.1.1 Conceitos e Arquitetura

A arquitetura tradicional da IoT é frequentemente descrita em um modelo de três camadas principais: a Camada de Percepção (sensores físicos que capturam dados do ambiente), a Camada de Rede (responsável pela transmissão desses dados via protocolos como Wi-Fi, Bluetooth ou 5G) e a Camada de Aplicação (onde os dados são processados e apresentados ao usuário final). No entanto, a literatura recente, aponta para uma evolução necessária desse modelo em direção à Computação de Borda (*Edge Computing*) [Li Shuhong Chen 2021].

No modelo centralizado em nuvem, todos os dados brutos viajam da camada de percepção até servidores remotos, gerando alta latência e consumo excessivo de largura de banda. A arquitetura de Borda e Névoa (*Fog Computing*) desloca a inteligência e o processamento para mais perto da fonte dos dados. É neste ponto arquitetural que o smartphone assume um papel protagonista. Ele deixa de ser apenas uma interface de visualização para se tornar um nó de computação de borda, capaz de filtrar, criptografar e anonimizar dados de dispositivos periféricos (como *wearables*) antes que estes sejam enviados para a internet pública. Essa descentralização é vital para a aplicação de tecnologias de privacidade como a rede Onion, pois permite que o túnel criptografado seja estabelecido localmente no smartphone-gateway, protegendo o fluxo de dados desde a origem física.

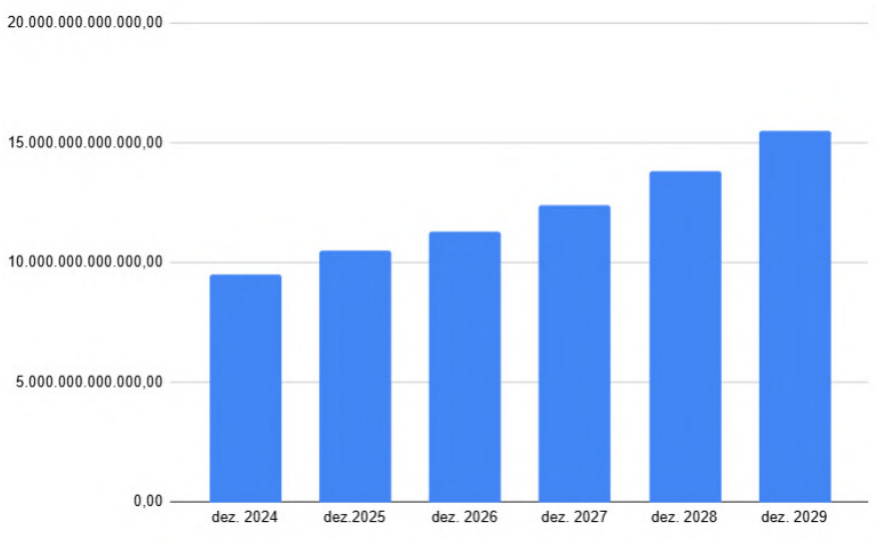
2.1.2 Vulnerabilidades e Desafios de Segurança

A premissa central levantada pela literatura é que os dispositivos IoT são notoriamente vulneráveis, criando uma, superfície de ataque gigantesca. Artigos como o de [Ali Mohamed Abdelrazek 2024] destacam que, sem camadas adicionais de segurança, a comunicação desses dispositivos pode ser facilmente interceptada ou rastreada, expondo padrões de comportamento do usuário. A falta de padronização e o uso de softwares desatualizados em dispositivos de baixo custo agravam esse cenário.

Além das vulnerabilidades de software, destaca-se o problema da análise de tráfego baseada em padrões de metadados. Mesmo que o conteúdo dos dados esteja criptografado, [Azeez

Taiwo O. Odeyemi 2023] demonstram que é possível identificar a natureza dos dispositivos IoT (câmeras, assistentes de voz) apenas analisando o volume e a periodicidade dos pacotes transmitidos. Essa "impressão digital"do tráfego (*fingerprinting*) permite que observadores externos infiram hábitos do usuário, como horários de presença em casa, violando a privacidade sem a necessidade de quebrar a criptografia do conteúdo.

Figura 2.1: *Custo anual estimado de ataques cibernéticos em todo o mundo em trilhões de dólares.*



Fonte: Expressvpn.

2.2 Rede Onion (Tor)

A rede Onion (Tor) é uma rede de sobreposição que permite a navegação e comunicação anônima. Conforme descrito no estudo [Zheng Haonan Yan 2022]: A Practical Anonymous Network Simulation Platform (2022), o tráfego é roteado através de uma série de nós voluntários (Nós reais), onde cada nó conhece apenas o seu antecessor e o seu sucessor, mas nunca o caminho completo. A criptografia é aplicada em camadas, semelhante às camadas de uma cebola, garantindo que o conteúdo da mensagem e a origem sejam ofuscados.

2.2.1 Arquitetura e Funcionamento

A rede Onion (Tor) é uma rede de sobreposição que permite a navegação e comunicação anônima. Conforme descrito no estudo de [Zheng Haonan Yan 2022], o tráfego é roteado através de uma série de nós voluntários (Nós reais), onde cada nó conhece apenas o seu antecessor e o seu sucessor, mas nunca o caminho completo. A criptografia é aplicada em camadas, semelhante às camadas de uma cebola, garantindo que o conteúdo da mensagem e a origem sejam ofuscados.

O funcionamento técnico baseia-se na construção de circuitos virtuais compostos tipicamente por três nós: o nó de guarda (entrada), o nó do meio e o nó de saída. As Autoridades

de Diretório desempenham um papel crucial nesse ecossistema, mantendo uma lista atualizada e assinada de todos os nós reais confiáveis, permitindo que os clientes construam caminhos válidos. No entanto, como ressaltado por [Lauer Kai Gellert 2020] o processo de estabelecimento desses circuitos envolve múltiplos handshakes criptográficos, o que introduz uma latência significativa antes mesmo de o primeiro *byte* de dados úteis ser transmitido, um fator crítico para aplicações IoT.

2.2.2 Mecanismos de Anonimato e Privacidade

O objetivo primário do Tor é a resistência contra a análise de tráfego. O estudo [Zhao 2024] explica que adversários globais (como Provedores de Serviços de Internet - ISPs) tentam correlacionar o tráfego de entrada e saída para quebrar o anonimato. O Tor mitiga isso através da seleção aleatória de caminhos e renovação periódica de circuitos. Além disso, serviços ocultos (*Hidden Services*) permitem que servidores, que podem ser dispositivos IoT operem sem revelar seu endereço IP real, conforme levantado no [Bian Chunjie Cao 2021].

Além disso, serviços ocultos (Hidden Services) permitem que servidores (que podem ser dispositivos IoT) operem sem revelar seu endereço IP real, conforme levantado no survey de Bian et al. (2021) [Bian Chunjie Cao 2021]. Kareem (2024) [Kareem 2024] complementa essa visão, explorando táticas para combater ameaças cibernéticas em ambientes de roteamento Onion, enfatizando que a manutenção do anonimato exige uma vigilância constante contra vetores de ataque emergentes.

Os Onion Services (anteriormente chamados de *Hidden Services*) são particularmente relevantes para o contexto de IoT, pois permitem a comunicação bidirecionalmente anônima. Nesse modelo, o dispositivo IoT, atuando como servidor e o usuário cliente conectam-se através de um ponto de encontro (*Rendezvous Point*) dentro da rede Tor, sem que nenhum dos dois precise revelar seu endereço IP ou localização física. Isso elimina a necessidade de configurações complexas de port forwarding em roteadores domésticos e protege o dispositivo contra varreduras de rede direta, ocultando sua existência na internet pública.

2.2.3 Integração Tor-IoT a Smartphones: Abordagens Existentes

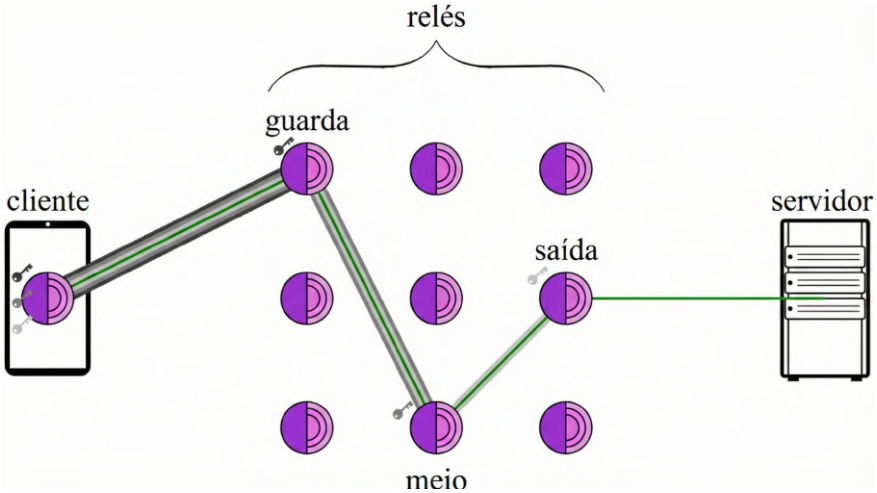
A integração do Tor em smartphones, especificamente no sistema Android, é um campo de estudo crítico. O trabalho de [Arshad Mehdi Hussain 2021], demonstra que, embora o Tor forneça anonimato na rede, o dispositivo em si, o *smartphone* mantém as evidências digitais que podem comprometer a privacidade local. O uso do smartphone como um nó de acesso para outros dispositivos IoT (*tethering* ou controle via app) exige que o tráfego seja forçado através da rede Onion, o que impõe desafios significativos de desempenho, abordados em propostas como o [Shoker 2021], que sugere incentivos para tornar o uso da rede mais escalável para as massas.

Outra abordagem identificada na literatura é a utilização de redes Onion locais e privadas para ambientes industriais, como proposto por [Vinothkumar B. Rajasekar 2021]. Nesse

modelo, adaptável para redes domésticas inteligentes, o smartphone ou um *gateway* dedicado atua como o único ponto de saída para a internet, encapsulando todo o tráfego dos sensores locais. Essa estratégia isola os dispositivos vulneráveis da internet aberta, mas cria um ponto único de falha e de gargalo de desempenho no dispositivo móvel, que precisa gerenciar a criptografia pesada de múltiplos fluxos de dados simultâneos.

Nesse modelo, adaptável para redes domésticas inteligentes, o smartphone ou um *gateway* dedicado atua como o único ponto de saída para a internet, encapsulando todo o tráfego dos sensores locais. Essa estratégia isola os dispositivos vulneráveis da internet aberta, mas cria um ponto único de falha e de gargalo de desempenho no dispositivo móvel, que precisa gerenciar a criptografia pesada de múltiplos fluxos de dados simultâneos.

Figura 2.2: *Diagrama do circuito Tor.*



Fonte: wikipedia.

Capítulo 3

Revisão da Literatura

Este capítulo detalha os procedimentos metodológicos adotados para a elaboração deste trabalho, caracterizado como uma Revisão Bibliográfica. A metodologia foi desenhada para identificar, selecionar e analisar estudos que abordam a intersecção entre a rede Onion, dispositivos IoT e a segurança em *smartphones*. O percurso investigativo pautou-se na busca estruturada na base de dados CAPES(https://www.periodicos.capes.gov.br/) e no *Google Scholar*(https://scholar.google.com.br/), seguida pela aplicação de critérios de inclusão e exclusão para selecionar os trabalhos mais relevantes para a problemática de desempenho e privacidade na computação de borda(*Edge Computing*).

3.1 Formulação da Questão de Pesquisa

A presente revisão bibliográfica norteia-se pela necessidade de compreender a viabilidade da integração entre arquiteturas de anonimato e a *Mobile Edge Computing* (MEC). A questão central formulada para conduzir a investigação foi: "Como a criptografia da *Rede Onion* (Tor-IoT) pode ser aplicada a *smartphones* para assegurar a privacidade e mitigar vulnerabilidades em ecossistemas IoT?". Esta formulação busca explorar não apenas os aspectos teóricos do protocolo Onion, mas especificamente sua implementação prática em ambientes com recursos limitados, onde o smartphone atua como o nó criptográfico central.

3.2 Definição dos Termos de Busca

A busca bibliográfica foi realizada primariamente na base de dados do Portal de Periódicos da CAPES (https://www.periodicos.capes.gov.br/) e no *Google Scholar* (https://scholar.google.com.br/) selecionando estudos que abordassem a intersecção entre segurança de redes, dispositivos móveis e Internet das Coisas. Para garantir a recuperação de documentos alinhados com o objetivo do trabalho, foram aplicadas as seguintes strings de busca exatas, priorizando o idioma inglês devido à sua predominância na literatura técnica de alto impacto:

I. *String* "*The Onion Router*"

II. *String* "*The Onion Router and smartphone*"

Essas chaves foram utilizadas individualmente e em combinação para filtrar artigos que tratassem especificamente da implementação do protocolo Tor em dispositivos móveis, descartando resultados genéricos sobre criptografia de desktop.

3.3 Critérios de Busca e Seleção

A presente revisão bibliográfica norteia-se pela necessidade de compreender a viabilidade da integração entre arquiteturas de anonimato e a computação móvel de borda. A questão central formulada para conduzir a investigação foi: "Como a criptografia da rede Onion (Tor-IoT) pode ser aplicada a *smartphones* para assegurar a privacidade e mitigar vulnerabilidades em ecossistemas IoT?". Esta formulação busca explorar não apenas os aspectos teóricos do protocolo Onion, mas especificamente sua implementação prática em ambientes com recursos limitados, onde o *smartphone* atua como o nó criptográfico central.A metodologia adotada baseou-se na análise qualitativa de obras pertinentes ao tema proposto. O levantamento bibliográfico foi conduzido primordialmente através do Portal de Periódicos da CAPES(https://www.periodicos.capes.gov.br/) e no *Google Scholar*(https://scholar.google.com.br/), utilizando a string de busca: "*The* Onion Router"AND "*internet of things*"AND "*smartphone*". O recorte temporal foi delimitado entre os anos de 2020 e 2025, visando assegurar a seleção de publicações de alto impacto e rigor científico.

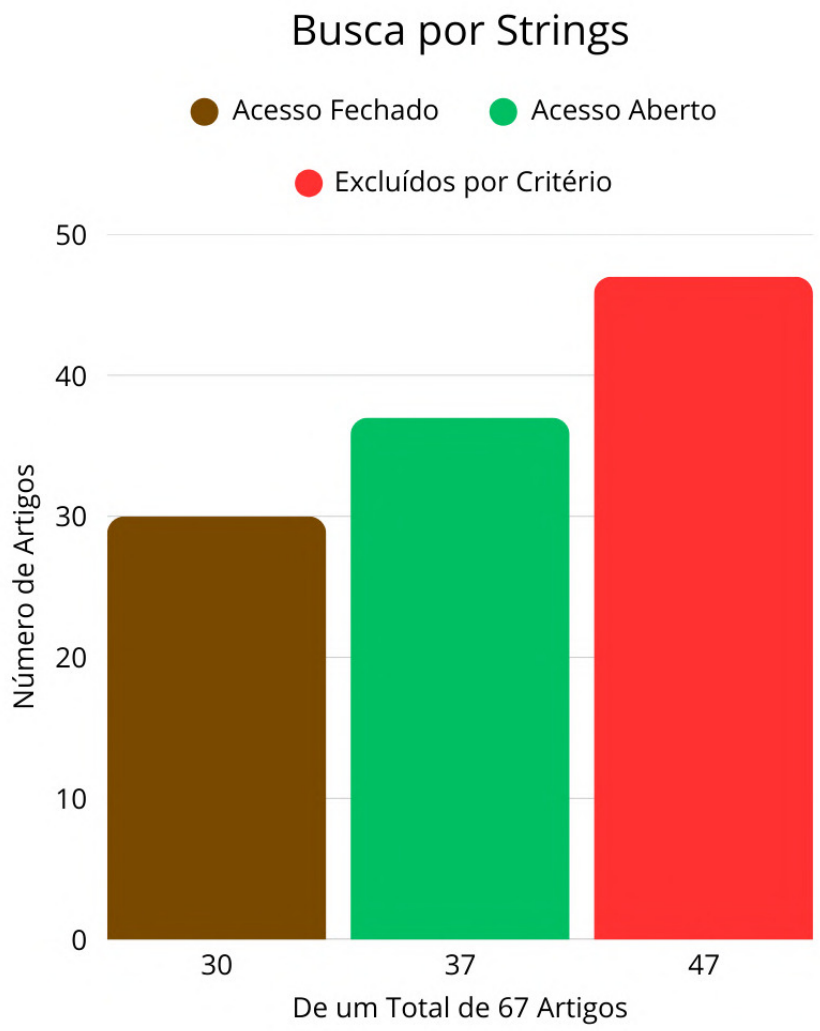


Figura 3.1: Resultados da Fase de Inclusão e Exclusão de Artigos

3.3.1 Critérios de Inclusão

Para a seleção dos materiais, foram estabelecidos os seguintes critérios de inclusão:

I. Os artigos deveriam abordar técnicas diretamente ligadas à rede Onion aplicada à segurança em dispositivos *smartphone* ou estarem relacionados à segurança de dados em ambiente IoT utilizando a rede Onion;

II. Os artigos deveriam ser relevantes para a compreensão e exploração das técnicas utilizadas na rede Onion aplicadas a dispositivos IoT do tipo *smartphone*.

3.3.2 Critérios de Exclusão

Foram descartados os trabalhos que se enquadraram nos seguintes critérios:

I. Artigos que não abordaram diretamente métodos que forneçam informações de segurança utilizando a rede Onion aplicada a dispositivos IoT/*smartphones*;

II. Artigos que não atenderam a critérios mínimos de qualidade acadêmica, apresentando

falta de embasamento teórico, metodologia inadequada, ausência de dados empíricos ou análise insuficiente;

III. Artigos focados exclusivamente em cibersegurança genérica, sem conexão direta com a intersecção entre IoT, *Smartphones* e Rede Onion.

3.4 Processo de Análise

O processo de análise dos dados ocorreu seguindo um fluxo sistemático:

I. Durante um período de 3 meses, foram pesquisados artigos publicados nos periódicos indexados na base de dados mencionada;

II. De forma individual, realizou-se a análise dos títulos e resumos dos artigos para verificar a relevância preliminar e a adequação aos critérios de inclusão estabelecidos;

III. Os artigos que não atenderam aos critérios de inclusão foram excluídos nessas etapas iniciais de triagem;

IV. Após a leitura integral dos artigos selecionados na triagem inicial, foram incluídos nesta Revisão Bibliográfica da Literatura (RBL) os 15 documentos (PDFs) que se mostraram mais relevantes para responder aos objetivos do estudo.

3.5 Metodologia

A revisão da literatura identificou metodologias distintas para a implementação da rede Onion em cenários de IoT, destacando-se a adaptação de *gateways* e o uso de incentivos econômicos. O trabalho de [Vinothkumar B. Rajasekar 2021] propõe uma metodologia baseada em *hardware* dedicado (como *Raspberry Pi*) atuando como roteador de borda, uma arquitetura que pode ser emulada por *smartphones* modernos através de *tethering* seguro. Essa abordagem centraliza o túnel Tor em um único dispositivo, simplificando a configuração dos sensores IoT periféricos.

Complementarmente [Shoker 2021] introduz a metodologia *TorMass*, que sugere um modelo de incentivo econômico para provedores de serviços de anonimato. Essa proposta metodológica visa resolver o problema da escalabilidade e da confiabilidade dos nós de saída, sugerindo que a massificação do uso doméstico (incluindo *smartphones*) depende de uma infraestrutura mais robusta e menos dependente apenas de voluntariado [Zheng Haonan Yan 2022] contribuem com a plataforma de simulação LUNAR, oferecendo um método para validar essas arquiteturas em ambientes controlados antes da implementação física, permitindo testar o comportamento de protocolos de roteamento anônimo sob estresse.

3.6 Resultados/Análise

A análise dos resultados obtidos na literatura revela um cenário complexo onde a segurança teórica colide com limitações práticas de desempenho e forense [Lauer Kai Gellert 2020] demonstram que, embora protocolos otimizados como o T0RTT possam reduzir a latência de estabelecimento de circuitos, o overhead criptográfico inerente à rede Onion continua sendo um gargalo crítico para aplicações de tempo real em dispositivos móveis [Islam Guangjie Liu 2021] corroboram esse achado ao analisar o tráfego VoIP, indicando que a instabilidade do jitter em túneis anônimos degradam severamente a qualidade da experiência do usuário (QoE) em chamadas de voz e vídeo.

Do ponto de vista da segurança ofensiva e forense, os resultados são igualmente desafiadores. Arshad et al. (2021) [Arshad Mehdi Hussain 2021] provam que o sistema operacional Android mantém a evidências digitais persistentes (em memória RAM e armazenamento físico) que podem ser extraídos para inferir atividades do usuário, mesmo quando o tráfego de rede está anonimizado. Adicionalmente [Azeez Taiwo O. Odeyemi 2023] e Li et al. [Li Shuhong Chen 2021] mostram que técnicas avançadas de Machine Learning conseguem classificar e identificar padrões de tráfego malicioso dentro da rede Tor com alta precisão, sugerindo que a "camada de invisibilidade"do Tor não é impenetrável contra análises de tráfego sofisticadas realizadas na borda da rede.

Capítulo 4

Conclusão

Este Trabalho de Conclusão de Curso (TCC) teve como objetivo a investigação e análise da segurança aplicada a dispositivos IoT integrados a smartphones via rede Onion. Fundamentando-se em estudos e pesquisas recentes, foi adotado um processo sistemático de revisão da literatura. Conclui-se que, embora a Rede Onion forneça uma camada robusta de anonimato e criptografia para o tráfego de dados, sua aplicação em smartphones atuando como gateways IoT enfrenta barreiras significativas de desempenho (latência) e consumo de recursos. As vulnerabilidades intrínsecas dos dispositivos IoT (como *firmwares* inseguros) e do próprio sistema operacional móvel (a evidências digitais no Android) significam que o Tor, por si só, não garante imunidade total. Ele deve ser encarado como uma solução de infraestrutura para mitigação de riscos de vigilância de rede, mas não resolve falhas de segurança de endpoint.

4.1 Considerações Finais

A análise evidenciou que a literatura atual propõe otimizações no protocolo para reduzir o *overhead*, mas a discrepância entre os ambientes simulados e a realidade prática dos dispositivos móveis ainda é um obstáculo para a adoção em larga escala [Lauer Kai Gellert 2020].

Em suma, a integração Tor-IoT via *smartphones* apresenta-se como uma tecnologia promissora, porém imatura para aplicações de tempo real e consumo de massa. A proteção oferecida contra a análise de tráfego global é contrabalançada pelo alto custo computacional e energético, além da exposição a ataques de correlação locais e forenses digitais no dispositivo. A viabilidade atual restringe-se a cenários de alta criticidade onde o atraso na comunicação é tolerável em prol da privacidade extrema, não sendo ainda uma solução transparente (*seamless*) para o usuário doméstico comum.

4.2 Trabalhos Futuros

Tendo em vista as limitações e descobertas apresentadas ao longo deste estudo, torna-se evidente que a convergência entre IoT, redes Onion e dispositivos móveis é um campo fértil para novas investigações. As lacunas identificadas, especialmente no que tange ao desempenho e à usabilidade, apontam para a necessidade de pesquisas práticas que possam validar ou refutar as simulações teóricas discutidas. Dessa forma, propõem-se os seguintes desdobramentos como continuação natural deste trabalho:

• Sugere-se fazer a realização de testes empíricos utilizando smartphones como roteadores de borda em redes Tor reais, tendo em vista a necessidade de medir com precisão o impacto no consumo de bateria e na latência de pacotes IoT em cenários de uso cotidiano, superando as limitações das simulações laboratoriais.

•O desenvolvimento de aplicações leves de tunelamento focadas especificamente em protocolos IoT (como MQTT) sobre a rede Onion, tendo em vista a urgência em reduzir o *overhead* de processamento identificado na literatura, tornando a solução viável para dispositivos com recursos de hardware mais restritos.

• Estudos de usabilidade aprofundados, tendo em vista a dificuldade técnica que usuários leigos enfrentam na configuração dessas ferramentas de segurança, buscando simplificar a interface e a experiência do usuário para promover uma adoção mais ampla da privacidade em IoT.

Referências Bibliográficas

[Ali Mohamed Abdelrazek 2024] ALI MOHAMED ABDELRAZEK, S. H. M. R. M. R. A. S. I. H. *Cybercrimes in the Darknet and Their Detections: A Comprehensive Analysis and Future Directions*. 2024. 19 p. 2, 5, 6

[Arshad Mehdi Hussain 2021] ARSHAD MEHDI HUSSAIN, H. T. S. Q. F. I. A. M. Y. J. M. R. *Forensic Analysis of Tor Browser on Windows 10 and Android 10 Operating Systems*. 2021. 141273 p. 2, 8, 14

[Azeez Taiwo O. Odeyemi 2023] AZEEZ TAIWO O. ODEYEMI, C. C. I. A. P. A. N. A. *Cyber Attack Detection in A Global Network Using Machine Learning Approach*. 2023. 6, 14

[Bian Chunjie Cao 2021] BIAN CHUNJIE CAO, L. W. J. Y. Y. Z. C. T. J. *Tor Hidden Services Discovery and Analysis: A Literature Survey*. 2021. 012162 p. 8

[Gușiță *et al.* 2025] GUșIțĂ, B. *et al.* Securing iot edge: a survey on lightweight cryptography, anonymous routing and communication protocol enhancements: B. gușiță et al. *International Journal of Information Security*, Springer, v. 24, n. 3, p. 149, 2025. 5

[Islam Guangjie Liu 2021] ISLAM GUANGJIE LIU, J. Z. W. L. F. U. *VoIP Traffic Detection in Tunneled and Anonymous Networks Using Deep Learning*. 2021. 59783 p. 2, 14

[Kareem 2024] KAREEM, K. M. Guardians of anonymity: Exploring tactics to combat cyber threats in onion routing environments. *arXiv preprint arXiv:2406.07563*, 2024. 8

[Kauser Tauqeer Safdar Malik 2022] KAUSER TAUQEER SAFDAR MALIK, M. H. H. E. A. P. A. S. M. H. K. S. *Windows 10's Browser Forensic Analysis for Tracing P2P Networks' Anonymous Attacks*. 2022. 1251 p. 5

[Khan *et al.* 2021] KHAN, Z. *et al.* Internet of things-based smart farming monitoring system for bolting reduction in onion farms. *Scientific Programming*, Wiley Online Library, v. 2021, n. 1, p. 7101983, 2021. 6

[Lauer Kai Gellert 2020] LAUER KAI GELLERT, R. M. T. H. J. S. S. *T0RTT: Non-Interactive Immediate Forward-Secret Single-Pass Circuit Construction*. 2020. 336 p. 8, 14, 15

[Li Shuhong Chen 2021] LI SHUHONG CHEN, J. Y. E. L. R. *Edge-Based Detection and Classification of Malicious Contents in Tor Darknet Using Machine Learning*. 2021. 1 p. 6, 14

[Shoker 2021] SHOKER, A. *TorMass: Tor for the Masses Domestic and Monetized Anonymous Communication*. 2021. 1216 p. 8, 13

[Vinothkumar B. Rajasekar 2021] VINOTHKUMAR B. RAJASEKAR, B. K. J. P. C. *A secured tor local network for nuclear power plant industry*. 2021. 012111 p. 8, 13

[Zhao 2024] ZHAO, X. S. H. *TOAR: Toward Resisting AS-Level Adversary Correlation Attacks Optimal Anonymous Routing*. 2024. 3640 p. 8

[Zheng Haonan Yan 2022] ZHENG HAONAN YAN, R. W. Z. Z. H. L. X. *LUNAR: A Practical Anonymous Network Simulation Platform*. 2022. 1 p. 7, 13

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Campina Grande - Código INEP: 25137409
R. Tranqüilino Coelho Lemos, 671, Dinamérica, CEP 58432-300, Campina Grande (PB)
CNPJ: 10.783.898/0003-37 - Telefone: (83) 2102.6200

Documento Digitalizado Restrito

Monografia/TCC

Assunto:	Monografia/TCC
Assinado por:	Wosney Penaforte
Tipo do Documento:	Dissertação
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Informação Pessoal (Art. 31 da Lei no 12.527/2011)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Wosney Penaforte Cavalcante**, **DISCENTE (202311210037) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE**, em 29/01/2026 12:57:34.

Este documento foi armazenado no SUAP em 29/01/2026. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1747168
Código de Autenticação: 42d849ccc8