UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Luciano Fernandes da Rocha

O Impacto da Autenticação Mútua e Simultânea com Certificados X.509 no Âmbito do eduroam

Juiz de Fora

2025

Luciano Fernandes da Rocha

O Impacto da Autenticação Mútua e Simultânea com Certificados X.509 no Âmbito do eduroam

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Ciência da Computação. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Edelberto Franco Silva

Juiz de Fora

2025

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

da Rocha, L. F..
O Impacto da Autenticação Mútua e Simultânea com Certificados X.509 no Âmbito do eduroam / Luciano Fernandes da Rocha. – 2025.
70 f. : il.

Orientador: Edelberto Franco Silva
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação, 2025.

1. EAP-TLS 2. eduroam 3. RADIUS 4. ICPEdu 5. Gestão de Identidade e Acesso. Franco Silva, Edelberto, orient. II. TÍTULO.

Luciano Fernandes da Rocha

O Impacto da Autenticação Mútua e Simultânea com Certificados X.509 no Âmbito do eduroam

Dissertação apresentada ao Programa de Pós-graduação em Ciência da Computação da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Ciência da Computação. Área de concentração: Ciência da Computação.

Aprovada em 03 de outubro de 2025.

BANCA EXAMINADORA

Prof. Dr. Edelberto Franco Silva - Orientador
Universidade Federal de Juiz de Fora

Prof. Dr. Alex Borges Vieira
Universidade Federal de Juiz de Fora

Prof. Dr. Jean Carlo Faustino
Rede Nacional de Ensino e Pesquisa

Prof. Dr. Emerson Ribeiro de Mello
Instituto Federal de Santa Catarina

Juiz de Fora, 26/09/2025.

Documento assinado eletronicamente por **Edelberto Franco Silva**, **Professor(a)**, em 17/10/2025, às 14:30, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Emerson Ribeiro de Mello**, **Usuário Externo**, em 20/10/2025, às 14:39, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Alex Borges Vieira**, **Coordenador(a)**, em 22/10/2025, às 15:17, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Jean Carlo Faustino**, **Usuário Externo**, em 11/11/2025, às 14:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no Portal do SEI-Ufjf (www2.ufjf.br/SEI) através do ícone Conferência de Documentos, informando o código verificador **2643279** e o código CRC **847FC318**.

Dedico este trabalho a minha família.

AGRADECIMENTOS

A caminhada até esta dissertação só foi possível graças ao apoio de muitas pessoas e instituições, a quem deixo aqui minha sincera gratidão.

Em especial, agradeço ao meu orientador, Prof. Dr. Edelberto Franco Silva, pela confiança, paciência e orientações que sempre me desafiaram a ir além. Sua dedicação foi essencial para que este trabalho se tornasse realidade.

À minha família, meu alicerce e maior fonte de força. Obrigado pelo carinho, compreensão e incentivo em cada etapa desta jornada.

Aos colegas da Rede Nacional de Ensino e Pesquisa (RNP), que compartilharam conhecimento, ideias e momentos de colaboração que enriqueceram muito esta experiência.

Aos professores do Programa de Pós-Graduação em Ciência da Computação da UFJF, por contribuírem de forma significativa para minha formação.

E à própria UFJF, por oferecer o ambiente e os recursos que tornaram este trabalho possível.

“Prepara-se o cavalo para o dia da batalha, mas o Senhor é que dá a vitória.”
Provérbios 21:31.

RESUMO

A crescente fragilidade de protocolos de autenticação amplamente utilizados, como os métodos EAP-TTLS, especialmente quando utilizam algoritmos vulneráveis, motiva a busca por alternativas mais seguras para redes federadas como a eduroam. No contexto da infraestrutura acadêmica brasileira operada pela RNP, os métodos tradicionais de autenticação baseados em EAP-TTLS com usuário e senha apresentam riscos de segurança significativos. O estado da arte aponta para o EAP-TLS, que emprega certificados digitais para autenticação mútua, como solução mais robusta. No entanto, a literatura carece de avaliações quantitativas do desempenho sobre o impacto da adoção de certificados de uma Infraestrutura de Chaves Públicas (PKI) nacional, como a ICPEdu, nesse cenário. Esta dissertação propõe uma avaliação empírica comparativa entre o método EAP-TLS, que utiliza certificados ICPEdu, e o tradicional EAP-TTLS/PAP. Os resultados qualitativos demonstram um incremento substancial na segurança com a adoção do EAP-TLS, eliminando a suscetibilidade a ataques de roubo de credenciais, por exemplo. Quantitativamente, os experimentos, conduzidos em um ambiente controlado, revelaram que a autenticação via EAP-TLS com certificados ICPEdu gerou um volume de pacotes 29% superior e um tempo total de autenticação acumulado aproximadamente 4% maior em comparação ao método legado, o que fornece dados concretos para a análise sobre o equilíbrio entre o reforço na segurança e o impacto no desempenho da rede.

Palavras-Chave: EAP-TLS. Eduroam. RADIUS. ICPEdu. Gestão de Identidade e Acesso.

ABSTRACT

The increasing vulnerability of widely-used authentication protocols, such as EAP-TTLS methods, especially when they utilize vulnerable algorithms, motivates the search for more secure alternatives for federated networks like eduroam. In the context of the Brazilian academic infrastructure operated by RNP, traditional authentication methods based on EAP-TTLS with a username and password pose significant security risks. The state of the art points to EAP-TLS, which employs digital certificates for mutual authentication, as a more robust solution. However, the literature lacks quantitative performance evaluations on the impact of adopting certificates from a national Public Key Infrastructure (PKI), such as ICPEdu, in this scenario. This dissertation proposes an empirical comparative evaluation between the EAP-TLS method using ICPEdu certificates and the traditional EAP-TTLS/PAP. The qualitative results demonstrate a substantial increase in security with the adoption of EAP-TLS, which eliminates susceptibility to attacks such as credential theft. Quantitatively, the experiments, conducted in a controlled environment, revealed that authentication via EAP-TLS with ICPEdu certificates generated 29% more packet volume and a total accumulated authentication time approximately 4% longer than the legacy method. This provides concrete data to analyze the trade-off between enhanced security and network performance.

Keywords: EAP-TLS. Eduroam. RADIUS. ICPEdu. Identity and Access Management.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AAA	Authentication, Authorization, and Accounting
AC	Autoridade Certificadora
AES	Advanced Encryption Standard
AR	Autoridades de Registro
ASN.1	Abstract Syntax Notation One
CAF	Comunidade Acadêmica Federada
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CRL	Certificate Revocation Lists
DER	Distinguished Encoding Rules
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
IdP	Provedor de Identidade
IoT	Internet das Coisas
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
MS-CHAPv2	Microsoft Challenge-Handshake Authentication Protocol, Version 2
NAS	Network Access Server
OCSP	Online Certificate Status Protocol
OVP	Overhead de Validação PKI
PEAP	Protected EAP
PKI	Public Key Infrastructure
PNAC	Port-Based Network Access Control
RADIUS	Remote Authentication Dial-In User Service
RNP	Rede Nacional de Ensino e Pesquisa
SAML	Security Assertion Markup Language
SP	Provedor de Serviço
TAC	Tempo de Autenticação Completa
TAS	Taxa de Autenticações Simultâneas
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UFJF	Universidade Federal de Juiz de Fora
WAYF	Where Are You From
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

SUMÁRIO

1 INTRODUÇÃO

A segurança e a conectividade tornaram-se pilares indispensáveis para o avanço da ciência e da educação na era digital. Em um ambiente acadêmico marcado pela mobilidade e pela colaboração distribuída, a capacidade de acessar recursos de rede de forma segura, transparente e ubíqua deixou de ser um luxo e passou a constituir uma necessidade fundamental. Nesse contexto, o Brasil, por meio da Rede Nacional de Ensino e Pesquisa (RNP), consolidou um ecossistema robusto de serviços destinados a sustentar as atividades de sua comunidade acadêmica. Dois componentes centrais desse ecossistema são o serviço de *roaming* acadêmico eduroam e a Infraestrutura de Chaves Públicas para Ensino e Pesquisa, a ICPEdu.

O eduroam (*education roaming*) personifica essa evolução. Surgiu na Europa como solução para um desafio persistente: permitir que pesquisadores e estudantes acessassem redes sem fio de instituições visitantes sem a burocracia de criar contas temporárias. Sua premissa original era a mobilidade transparente e segura. Atualmente, constitui um serviço global consolidado, operado no Brasil pela RNP, conectando milhões de usuários em mais de 100 países, com milhares de pontos de acesso distribuídos por todo o território nacional. Contudo, a base de seu sucesso — a simplicidade de uso — também revela sua principal fragilidade: o método de autenticação predominante, o *Extensible Authentication Protocol* (EAP) com *Tunneled Transport Layer Security* (TTLS) e *Password Authentication Protocol* (PAP) — EAP-TTLS/PAP —, ainda depende de credenciais de usuário e senha. Descobertas recentes, como a vulnerabilidade Blast-RADIUS (15), evidenciam a urgência de reavaliar os protocolos empregados nessas redes.

O futuro do eduroam depende da adoção em larga escala do EAP-TLS com certificados digitais, que oferece autenticação mútua e elimina a transmissão de senhas. Essa transição, porém, não é trivial: exige uma infraestrutura de chaves públicas (ICP) confiável, escalável e gerenciável. É nesse cenário que a ICPEdu se torna estratégica. Criada pela RNP como uma Autoridade Certificadora subordinada à ICP-BRASIL, tem como missão fornecer identidades digitais confiáveis para estudantes, professores e pesquisadores, habilitando não apenas acesso seguro a redes, mas também assinatura digital de documentos, acesso a recursos de computação de alto desempenho e integração com serviços governamentais.

Hoje, a ICPEdu é a peça-chave que torna a autenticação EAP-TLS no eduroam não apenas possível, mas escalável e gerenciável em âmbito nacional. Integra-se ao portfólio da RNP — como a Comunidade Acadêmica Federada (CAFe), a Conferência Web e repositórios de dados científicos —, criando um ecossistema coeso de identidade digital. Seu futuro transcende o eduroam: pretende se tornar o pilar para acesso a computação avançada, assinatura de diplomas digitais e serviços governamentais.

Contudo, a transição de senhas para certificados levanta questões críticas de

desempenho e escalabilidade. A autenticação via EAP-TLS, que envolve troca e validação de cadeias de certificados, é inerentemente mais intensiva que a simples verificação de senha. Qual o impacto real desse *overhead* criptográfico no tempo de autenticação? Como o sistema se comporta sob carga de centenas ou milhares de autenticações simultâneas, comum em campi universitários? Esse custo poderia comprometer a experiência do usuário em situações de *roaming*, onde a latência já é fator relevante?

A literatura, embora rica em análises de vulnerabilidades, carece de avaliações quantitativas de desempenho no contexto de uma PKI nacional como a ICPEdu. Essa lacuna entre promessa de segurança e realidade prática precisa ser preenchida para subsidiar decisões informadas de gestores e técnicos.

Dessa forma, este trabalho propõe uma análise empírica do EAP-TLS com certificados ICPEdu, comparado ao EAP-TTLS/PAP, visando aprimorar a segurança em redes sem fio Wi-Fi, com ênfase no eduroam. Por meio de experimentos controlados em ambiente real de autenticação, com coleta de dados diretamente na interface de rede, busca-se determinar a abordagem mais adequada para o eduroam no Barsil, equilibrando segurança avançada e desempenho aceitável.

1.1 Implicações Sociais da Identidade Digital e do Acesso Federado

A fim de posicionar também filosoficamente o espaço em que esta pesquisa se insere e destacar sua contribuição, introduzimos pontos essenciais sobre os quais a relacionamos às implicações sociais da Identidade Digital e do Acesso Federado.

A evolução dos protocolos de autenticação e das infraestruturas de identidade digital, exemplificadas pelo eduroam e pela ICPEdu, ultrapassa as fronteiras técnicas, configurando-se como artefatos sociotécnicos que influenciam diretamente a forma como as comunidades acadêmicas se organizam, colaboram e produzem conhecimento. A migração de sistemas baseados em senhas para modelos fundamentados em certificados digitais representa uma mudança de paradigma cujas implicações transcendem a segurança da informação, afetando dimensões de confiança, acesso e inclusão digital.

Sob a ótica de Manuel Castells, conforme apresentado em *A Sociedade em Rede* (5), vive-se a ascensão de uma nova organização social, sustentada por redes de informação e comunicação. Castells argumenta que tecnologias como o eduroam não apenas operacionalizam a conectividade acadêmica, mas também criam uma "metainstituição" digital, sobrepondo os limites físicos dos campi e permitindo que o conhecimento e seus portadores circulem com mínima fricção. A identidade digital, nesse contexto, transforma-se no verdadeiro passaporte para a participação ativa na sociedade global do conhecimento.

Entretanto, essa reorganização em rede impõe um novo desafio: a construção da confiança nos sistemas digitais. Anthony Giddens, em *As Consequências da Modernidade* (14),

argumenta que as sociedades modernas deslocam a confiança das relações interpessoais e contextos locais para "sistemas peritos" ou "sistemas abstratos". A autenticação tradicional por usuário e senha revela-se frágil por depender da memória individual e por ser suscetível a comportamentos inseguros. Já a adoção de certificados X.509, especialmente via EAP-TLS, materializa essa confiança em estruturas sistêmicas robustas, amparadas por hierarquias de certificação e por criptografia avançada. Nesse novo modelo, a segurança passa a ser uma propriedade intrínseca do sistema, reduzindo o risco e fortalecendo a confiança coletiva.

Adicionalmente, a democratização do acesso, promovida por tecnologias como o eduroam e a ICPEdu, impacta diretamente a distribuição de recursos acadêmicos. O acesso seguro, transparente e ubíquo é fundamental para a equidade acadêmica, pois sistemas fragmentados e inseguros impõem custos cognitivos e de tempo que potencialmente marginalizam indivíduos ou instituições com menor infraestrutura. Ao oferecerem acesso federado seguro, essas tecnologias eliminam barreiras e promovem a inclusão digital, garantindo que pesquisadores de instituições remotas tenham oportunidades equivalentes às de grandes centros, reforçando a justiça social na academia.

Portanto, a decisão de migrar para métodos robustos de autenticação como o EAP-TLS com certificados ICPEdu deve ser entendida não apenas sob o prisma técnico, mas como um investimento estratégico na promoção da confiança sistêmica, alinhamento à sociedade em rede e democratização do acesso ao conhecimento — justificando, assim, a análise do impacto no desempenho como etapa fundamental para sua adoção em larga escala.

1.2 Problema

O problema central desta pesquisa consiste na ausência de dados empíricos que quantifiquem o impacto da adoção da autenticação mútua e simultânea com certificados X.509, por meio do método EAP-TLS, na performance e segurança do serviço eduroam. Embora os métodos baseados em EAP-TTLS/PAP sejam amplamente utilizados, eles apresentam fragilidades inerentes aos mecanismos de autenticação e integridade empregados junto ao protocolo RADIUS, especialmente em redes federadas de grande escala. Nesse contexto, torna-se essencial avaliar a viabilidade técnica e o impacto do uso de certificados digitais confiáveis emitidos pela ICPEdu, considerando aspectos de latência, vazão de pacotes e carga sobre os servidores em cenários reais e simultâneos. Assim, a principal questão de pesquisa que orienta este estudo é:

*"**Qual é o impacto na performance da rede eduroam ao se adotar um modelo de autenticação mútua e simultânea com certificados X.509, em comparação com os métodos tradicionais baseados em credenciais compartilhadas?**".*

1.3 Objetivo

Assim, o objetivo geral desta pesquisa é analisar comparativamente o método EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) utilizando certificados ICPEdu com os métodos de autenticação TTLS (Tunneled TLS) no serviço eduroam. Esta análise visa avaliar suas propriedades de segurança, seu desempenho, e a viabilidade de sua implementação como uma alternativa robusta e mais segura para a autenticação federada.

A pesquisa busca, primordialmente, identificar qual abordagem oferece o melhor equilíbrio entre segurança e impacto, minimizado em métricas de desempenho, como latência e vazão. Além disso, visa verificar a compatibilidade e eficácia da implementação do EAP-TLS com certificados ICPEdu em infraestruturas já existentes, a exemplo do FreeRADIUS, no contexto da autenticação federada do eduroam.

Complementarmente, este trabalho pretende oferecer uma sólida fundamentação técnica que sirva de guia para a migração segura de serviços legados. Para soluções criptográficas modernas. Isso se alinha às recomendações mais recentes da comunidade técnica e aos padrões emergentes do IETF, com o foco principal em capacitar as entidades acadêmicas a fortalecerem seus mecanismos de segurança de autenticação por meio da adoção de certificados digitais confiáveis.

1.4 Contribuições

Este trabalho oferece contribuições significativas tanto para o campo da segurança de redes quanto para a prática de implementação em ambientes acadêmicos, destacando-se por:

- **Análise Comparativa de Segurança e Desempenho da Autenticação no eduroam com Certificados ICPEdu:** Apresentação de uma análise empírica e quantitativa do incremento de segurança e do impacto no desempenho proporcionados pela utilização do método EAP-TLS com certificados pessoais da ICPEdu. Esta avaliação é realizada em comparação direta com os métodos tradicionais (i.e., TTLS), amplamente empregados no serviço eduroam brasileiro. Ao investigar a viabilidade prática do EAP-TLS nesse ambiente federado, a dissertação preenche uma lacuna crítica na literatura e na prática, oferecendo dados concretos sobre a superioridade e as implicações de sua adoção.

- **Adaptação de um *Framework* Metodológico para Avaliação de Autenticação Federada:** Demonstrar a adaptação e aplicação bem-sucedida de um robusto *framework* metodológico de avaliação de performance (originalmente proposto por Gaminara (13)) para as complexidades da autenticação em redes federadas como o

eduroam. Isso inclui o controle de variáveis específicas do processo de validação de PKI, o *roaming* entre instituições e a mensuração de métricas relevantes para a experiência do usuário, servindo como um modelo para futuras análises em ambientes distribuídos.

- **Geração de Dados Empíricos para Suporte à Decisão Estratégica:** Fornecer um conjunto de dados empíricos e análises quantitativas sobre latência, vazão e *overhead* computacional de EAP-TLS com certificados ICPEdu, gerados em um ambiente de teste realista do eduroam. Tais dados são cruciais para subsidiar decisões estratégicas e políticas de segurança da RNP e de outras instituições acadêmicas brasileiras na adoção e escalabilidade de tecnologias de autenticação avançadas, impulsionando a inovação e a confiabilidade da infraestrutura de rede.

1.5 Organização do Texto

O restante deste texto está organizado da seguinte forma: o Capítulo 2 apresenta os fundamentos teóricos e técnicos dos métodos EAP e protocolos de transporte analisados, com ênfase em suas propriedades de segurança e na sua aplicação no contexto do serviço eduroam e da ICPEdu. O Capítulo 3 discute trabalhos relacionados, abordando o estado da arte das pesquisas sobre autenticação segura em redes federadas, destacando as vulnerabilidades existentes e as lacunas que esta dissertação visa preencher. Já o Capítulo 4 detalha o ambiente experimental, a metodologia empregada e os cenários avaliados para a comparação entre os protocolos EAP-TLS, PEAP e TTLS com certificados ICPEdu. Em seguida, o Capítulo 5 apresenta e discute os resultados obtidos. Por fim, o Capítulo 6 conclui este trabalho, apresentando as recomendações práticas para a adoção do EAP-TLS com certificados ICPEdu como uma melhoria no ambiente de autenticação e autorização no eduroam, além de apontar direções para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

A evolução das redes sem fio nas últimas duas décadas transformou radicalmente a forma como a comunidade acadêmica acessa e compartilha informações (25, 11). Esta transformação, embora tenha proporcionado benefícios inegáveis em termos de mobilidade e flexibilidade, também introduziu desafios significativos relacionados à segurança da informação (26, 27, 31). O ambiente acadêmico atual, caracterizado pela crescente digitalização de processos educacionais e de pesquisa, demanda mecanismos de autenticação robustos que possam garantir tanto a proteção de dados sensíveis quanto a facilidade de acesso para usuários legítimos. Neste contexto, a compreensão dos fundamentos tecnológicos que sustentam a segurança em redes sem fio torna-se essencial para qualquer proposta de melhoria dos sistemas existentes.

A trajetória evolutiva dos protocolos de segurança, desde as implementações iniciais vulneráveis até as soluções contemporâneas mais sofisticadas, revela um processo contínuo de identificação e correção de falhas, sempre buscando equilibrar segurança, performance e usabilidade. Portanto, o presente capítulo estabelece as bases conceituais necessárias para compreender o funcionamento e os desafios de segurança enfrentados nos ambientes eduroam, os certificados do ICPEdu.

Inicialmente, examinaremos a evolução histórica dos protocolos de segurança em redes sem fio, analisando as limitações que motivaram cada transição tecnológica. Esta análise histórica não apenas contextualiza o estado atual da tecnologia, mas também revela padrões de vulnerabilidades que persistem em implementações contemporâneas. A compreensão das falhas do WEP, das melhorias introduzidas pelo WPA e WPA2, e das inovações do WPA3 fornece *insights* valiosos sobre as direções futuras da segurança em redes sem fio. Subsequentemente, aprofundaremos nossa análise na arquitetura do IEEE 802.1X (23) e no Protocolo de Autenticação Extensível (EAP) (2), que constituem os pilares tecnológicos sobre os quais o eduroam foi construído. O IEEE 802.1X estabelece um *framework* de controle de acesso baseado em portas que transcende as limitações dos métodos tradicionais de autenticação, enquanto o EAP oferece a flexibilidade necessária para suportar diversos métodos de autenticação, desde credenciais compartilhadas (e.g., PEAP e TTLS, tradicionalmente utilizados no eduroam) até certificados digitais (e.g., EAP-TLS).

Porém, para a compreensão adequada desses protocolos é necessário também o entendimento da infraestrutura de suporte que viabiliza a implementação em larga escala do serviço eduroam. Assim, serão apresentados os conceitos fundamentais de AAA (*Authentication, Authorization, and Accounting*) e sua implementação através do protocolo RADIUS (36), que centraliza as funções de autenticação e autorização. Finalmente, introduziremos os conceitos fundamentais de certificação digital e Infraestrutura de Chaves

Públicas (ICP), com foco específico na ICPEdu como uma solução especializada e nacional para o ambiente acadêmico brasileiro.

Esta abordagem sistemática permitirá não apenas a compreensão individual de cada tecnologia, mas também a visualização das interconexões entre elas e das oportunidades de integração que podem resultar em melhorias significativas de segurança. A relevância desta fundamentação teórica estende-se além dos aspectos puramente técnicos, abrangendo também as implicações estratégicas para a comunidade acadêmica brasileira. A compreensão dos fundamentos tecnológicos é essencial para a tomada de decisões informadas sobre investimentos em infraestrutura de segurança e para o desenvolvimento de políticas que equilibrem adequadamente segurança e usabilidade.

2.1 Evolução dos Protocolos de Segurança em Redes Sem Fio

2.1.1 IEEE 802.1X

O crescimento exponencial no uso de dispositivos móveis nas últimas duas décadas transformou radicalmente o panorama das redes sem fio. Segundo dados da União Internacional de Telecomunicações, o número de assinantes de banda larga móvel saltou de 268 milhões em 2007 para mais de 6,8 bilhões em 2022 (25). Esta expansão trouxe consigo desafios significativos em termos de segurança, uma vez que as redes sem fio locais IEEE 802.11 (às quais é comum relacionar diretamente com o termo Wi-Fi) são, por sua própria natureza, mais vulneráveis que suas contrapartes cabeadas devido ao meio de transmissão compartilhado e aberto.

Diante deste cenário, a partir da evolução dos protocolos envolvidos (18) tornou-se evidente a necessidade de implementar medidas robustas de segurança para proteger as informações trafegadas nessas redes. Foi nesse contexto que o padrão IEEE 802.1X emergiu como uma resposta às crescentes demandas, especialmente considerando a maior exposição às ameaças externas que caracterizam o ambiente sem fio (1, 37).

O IEEE 802.1X estabelece um modelo de autenticação fundamentado no conceito de *portas controladas*, onde cada ponto de conexão – seja uma porta física em redes cabeadas ou uma associação lógica em redes sem fio – funciona como uma barreira que deve ser transposta mediante autenticação adequada. Este mecanismo adiciona uma camada essencial de segurança ao impedir que dispositivos não autorizados estabeleçam qualquer tipo de comunicação com a rede. Uma das características mais relevantes do IEEE 802.1X reside em sua capacidade de interoperabilidade com diferentes tecnologias de criptografia. O padrão suporta tanto com o Protocolo de Integridade Temporal de Chave (TKIP) (reinteradamente considerado inseguro (39)), quanto com o Padrão de Criptografia Avançada (AES), este último amplamente reconhecido por sua robustez criptográfica. Além disso, o 802.1X integra-se naturalmente com outros protocolos da

família IEEE 802, incluindo o IEEE 802.3 (Ethernet) e o IEEE 802.11 (Wi-Fi), oferecendo assim um mecanismo unificado de autenticação que abrange tanto redes cabeadas quanto sem fio (1, 6).

2.1.2 IEEE 802.11i

Para compreender plenamente a relevância do IEEE 802.1X no contexto atual da segurança em redes sem fio, torna-se fundamental examinar a trajetória evolutiva dos protocolos de confidencialidade de dados. Esta análise aborda as deficiências técnicas que motivaram a transição do WEP para o WPA, WPA2 e, mais recentemente, WPA3, destacando como cada fase contribuiu para o desenvolvimento de soluções mais robustas e a consolidação do 802.1X como pilar da autenticação em ambientes corporativos.

Nas fases incipientes das redes de área local sem fio (WLANs), o foco primário dos desenvolvedores era a conectividade funcional, relegando a segurança a um plano secundário. O primeiro protocolo de segurança projetado para este ambiente foi o Wired Equivalent Privacy (WEP), introduzido juntamente com o padrão IEEE 802.11 em 1997. Contudo, o WEP foi construído sobre fundamentos criptográficos frágeis. A principal vulnerabilidade residia no uso do algoritmo de fluxo RC4 com um vetor de inicialização (IV) de apenas 24 bits, o que levava à reutilização de chaves. A análise seminal de (10) detalhou um ataque passivo capaz de recuperar a chave WEP com um número relativamente baixo de pacotes capturados. Outras falhas críticas incluíam o uso de chaves estáticas, uma verificação de integridade fraca baseada em CRC-32 que permitia a alteração maliciosa de pacotes sem detecção (9), e a ausência completa de um mecanismo para gerenciamento de chaves. Devido a estas falhas incorrigíveis, a Wi-Fi Alliance descontinuou oficialmente o WEP em 2004 (46).

Em resposta, o grupo de trabalho IEEE 802.11i desenvolveu o Wi-Fi Protected Access (WPA) como solução interina, lançado em 2003. A principal inovação do WPA à época foi o TKIP, que corrigia as falhas do WEP ao implementar *hashing* de chave por pacote, uma verificação de integridade de mensagem (MIC) mais robusta e um contador de sequência para mitigar ataques de repetição. O WPA introduziu dois modos de operação: o WPA-Personal (WPA-PSK), baseado em chave pré-compartilhada, e o WPA-Enterprise (WPA-EAP), que se integra ao padrão IEEE 802.1X para autenticação por usuário via servidores RADIUS, estabelecendo a base para o controle de acesso em redes corporativas. Porém, diversos trabalhos de pesquisa identificaram falhas que comprometem o TKIP (43, 41). Ainda em 2004, o IEEE ratificou o padrão 802.11i, cuja implementação certificada é conhecida como Wi-Fi Protected Access II (WPA2). O WPA2 representou um avanço criptográfico ao tornar obrigatório o uso do Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), um protocolo que utiliza o robusto Advanced Encryption Standard (AES) (22). O WPA2

também aprimorou a mobilidade com mecanismos de *roaming* eficientes, mantendo a dualidade dos modos Pessoal e Empresarial (802.1X), que se consolidou como padrão de excelência para segurança corporativa. Apesar de sua robustez, novas pesquisas revelaram vulnerabilidades no WPA2, notadamente o ataque *Key Reinstallation Attack* (KRACK), que permite a descriptografia de pacotes em certas condições (45). Para endereçar esta e outras questões, a Wi-Fi Alliance introduziu o WPA3 em 2018. Suas principais melhorias incluem uma autenticação mais robusta com o protocolo *Simultaneous Authentication of Equals* (SAE), que protege contra ataques de dicionário offline e provê *Forward Secrecy*, além de criptografia individualizada em redes abertas através do Wi-Fi Enhanced Open™. Destacamos que a adoção do WPA3 é progressiva e depende da atualização do ecossistema de dispositivos e pontos de acesso, o WPA3 e seu suporte a WPA3-Enterprise não são objeto de estudo direto neste trabalho.

A análise da trajetória evolutiva dos protocolos de segurança para redes sem fio, do WEP ao WPA3, demonstra um padrão reativo no qual novas gerações de protocolos são desenvolvidas primariamente em resposta à descoberta de vulnerabilidades críticas em seus predecessores (19). Esta realidade evidencia que mesmo arquiteturas consideradas robustas podem conter falhas latentes, como exemplificado pelo ataque KRACK (Key Reinstallation Attack) contra o WPA2, que explorou uma vulnerabilidade na negociação do *handshake* mais de uma década após sua ratificação (45). Para além das fragilidades criptográficas, um ponto crítico de vulnerabilidade reside na interface humano-protocolo, especialmente em implementações de WPA2/WPA2-Enterprise. A necessidade de validação manual do certificado do servidor pelo usuário final cria uma oportunidade para ataques de engenharia social, notadamente os ataques do tipo *Evil Twin*, nos quais um ponto de acesso malicioso apresenta um certificado ilegítimo na esperança de que o usuário o aceite sem a devida verificação (20). Esta fragilidade no processo de estabelecimento de confiança justifica a investigação de modelos de autenticação que automatizem ou eliminem a dependência da intervenção do usuário, visando maior resiliência contra tais ataques.

2.2 IEEE 802.1X e Métodos EAP

O padrão IEEE 802.1X apresentado define uma arquitetura de Controle de Acesso à Rede Baseado em Porta (PNAC) para mitigar os riscos de segurança inerentes às redes sem fio, cujo meio de transmissão compartilhado é vulnerável a acessos não autorizados (1, 37). Sua implementação depende de uma infraestrutura de *back-end* que adere ao modelo de Autenticação, Autorização e Contabilização (AAA), comumente materializada pelo protocolo RADIUS (36), o qual interage com serviços de diretório, como o LDAP (40), para validar identidades e aplicar políticas de acesso.

Dentro desta arquitetura, o Protocolo de Autenticação Extensível (EAP), especificado na RFC 3748, atua como um *framework* flexível para a negociação de métodos de

autenticação (2). O EAP é transportado sobre a camada de enlace via *EAP over LAN* (EAPoL), estabelecendo uma interação tripartite: o *Suplicante* (dispositivo cliente), o *Autenticador* (ponto de acesso ou *switch*) que controla a porta, e o *Servidor de Autenticação* (servidor RADIUS) que processa as credenciais e toma a decisão de acesso. A extensibilidade do EAP permite uma diversidade de métodos, detalhados a seguir.

A seguir apresentaremos os métodos EAP relacionados a esta pesquisa, para então introduzir os outros elementos e protocolos envolvidos no processo de autenticação.

2.2.1 EAP-TTLS (EAP-Tunneled TLS)

O EAP-TTLS (12) foi projetado para simplificar a autenticação, eliminando a necessidade de certificados no lado do cliente. Ele opera em um modelo de duas fases, estabelecendo um túnel seguro antes de realizar a autenticação do usuário. Para fins de visualização completa do processo, a Figura 2, herdada de (34), demonstra os passos detalhados para o EAP-TTLS combinado à fase 2 de autenticação via usuário e senha por MSCHAPv2. O fluxo geral pode ser seguido pelas etapas descritas.

Fluxo de Autenticação:

1. **Fase 1 (Túnel Externo):** Ocorre de forma similar à primeira metade do EAP-TLS. O servidor envia seu certificado ao suplicante, que o valida. Esta validação é unidirecional e suficiente para estabelecer um túnel TLS seguro entre o suplicante e o servidor de autenticação.

2. **Fase 2 (Autenticação Interna):** Dentro do túnel criptografado, uma segunda negociação de autenticação é iniciada. O suplicante envia suas credenciais (tipicamente usuário e senha) usando um protocolo legado e menos seguro, como PAP, CHAP ou MS-CHAPv2. Como essa troca ocorre dentro do túnel, as credenciais ficam protegidas contra interceptação na rede sem fio.

Este método equilibra segurança e usabilidade, pois protege credenciais fracas dentro de um túnel forte, sendo ideal para ambientes que suportam múltiplos métodos de autenticação legados.

2.2.2 PEAP (Protected EAP)

Similar ao EAP-TTLS, o PEAP (32) também é um método tunelado de duas fases, amplamente popularizado pela sua integração nativa em sistemas operacionais Microsoft.

Fluxo de Autenticação:

1. **Fase 1 (Túnel Externo):** Assim como no EAP-TTLS, o servidor se autentica para o cliente com um certificado digital, e um túnel TLS é estabelecido para proteger a comunicação subsequente.

2. **Fase 2 (Autenticação EAP Interna):** A principal diferença em relação ao EAP-TTLS é que o PEAP requer que a autenticação da segunda fase seja, obrigatoriamente, outro método EAP. A combinação mais comum é *PEAPv0/EAP-MSCHAPv2*. O suplicante e o servidor realizam uma troca EAP completa dentro do túnel. Embora o EAP-MSCHAPv2 seja popular, ele possui vulnerabilidades criptográficas conhecidas que permitem a recuperação da senha a partir da captura do *handshake*, por meio de ataques de força bruta offline (29).

Apesar da fragilidade de seu método interno mais comum, a proteção oferecida pelo túnel TLS da primeira fase torna o PEAP uma solução viável e de fácil implementação em muitos ambientes corporativos.

O processo de autenticação geral é orquestrado por uma troca de mensagens EAP (Request/Response) que culmina em um veredito de Sucesso ou Falha, emitido pelo servidor de autenticação. Esta arquitetura distribuída, embora ofereça controle granular e trilhas de auditoria detalhadas, introduz uma complexidade operacional que pode levar a pontos de falha na comunicação entre os componentes e em configurações incorretas, exigindo um gerenciamento cuidadoso para garantir sua eficácia e resiliência.

2.2.3 EAP-TLS (*EAP-Transport Layer Security*)

Considerado o padrão-ouro em segurança para EAP, o EAP-TLS (42) implementa autenticação mútua forte baseada em uma Infraestrutura de Chaves Públicas (PKI). Diferente de outros métodos, não há o conceito de túnel, pois todo o processo de autenticação já é inerentemente criptográfico. De maneira geral, os passos indicados na Figura 1 podem ser descritos como segue.

Fluxo de Autenticação:

1. A negociação EAP se inicia e o servidor de autenticação envia seu certificado digital ao suplicante.

2. O suplicante valida a autenticidade do certificado do servidor, verificando sua assinatura contra uma lista de Autoridades Certificadoras (CAs) confiáveis. Esta etapa é crucial para mitigar ataques *man-in-the-middle*.

3. Após validar o servidor, o suplicante envia seu próprio certificado digital para o servidor.

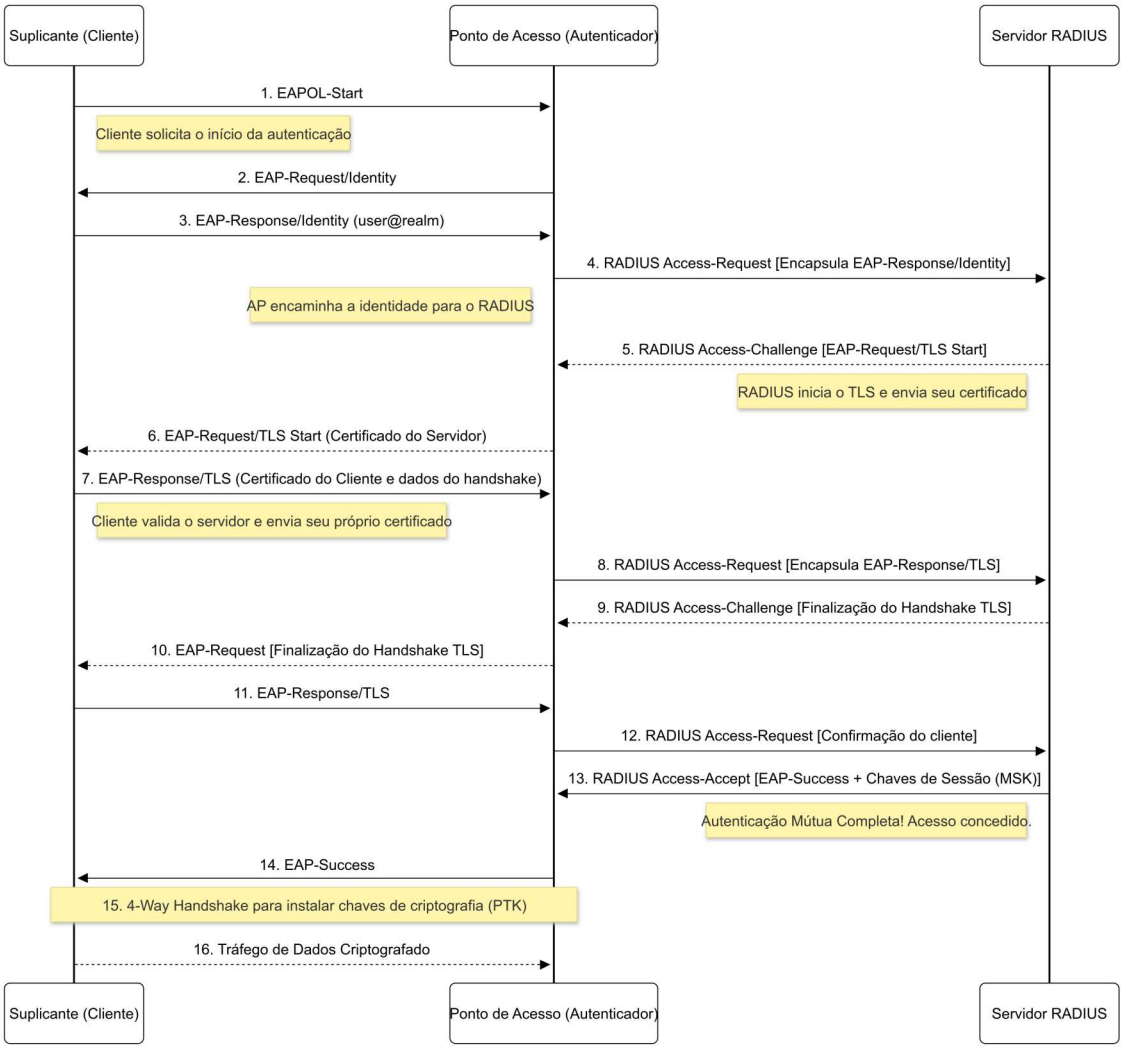

Figura 1 – Fluxo de autenticação para EAP-TLS.

4. O servidor de autenticação valida o certificado do suplicante, completando o processo de autenticação mútua.

5. Com a validação mútua bem-sucedida, um canal seguro é estabelecido e as chaves de sessão criptográfica são geradas para proteger o tráfego de dados.

A principal vantagem do EAP-TLS é a eliminação de credenciais baseadas em senhas, tornando-o imune a ataques de dicionário e roubo de credenciais. Contudo, sua implementação exige um esforço administrativo significativo para emitir, distribuir e gerenciar o ciclo de vida dos certificados em todos os dispositivos clientes. Tal tópico é também tema de discussão durante o texto desta pesquisa, porém mantendo como foco a experimentação e avaliação numérica de tal método no ambiente acadêmico de Wi-Fi federado.

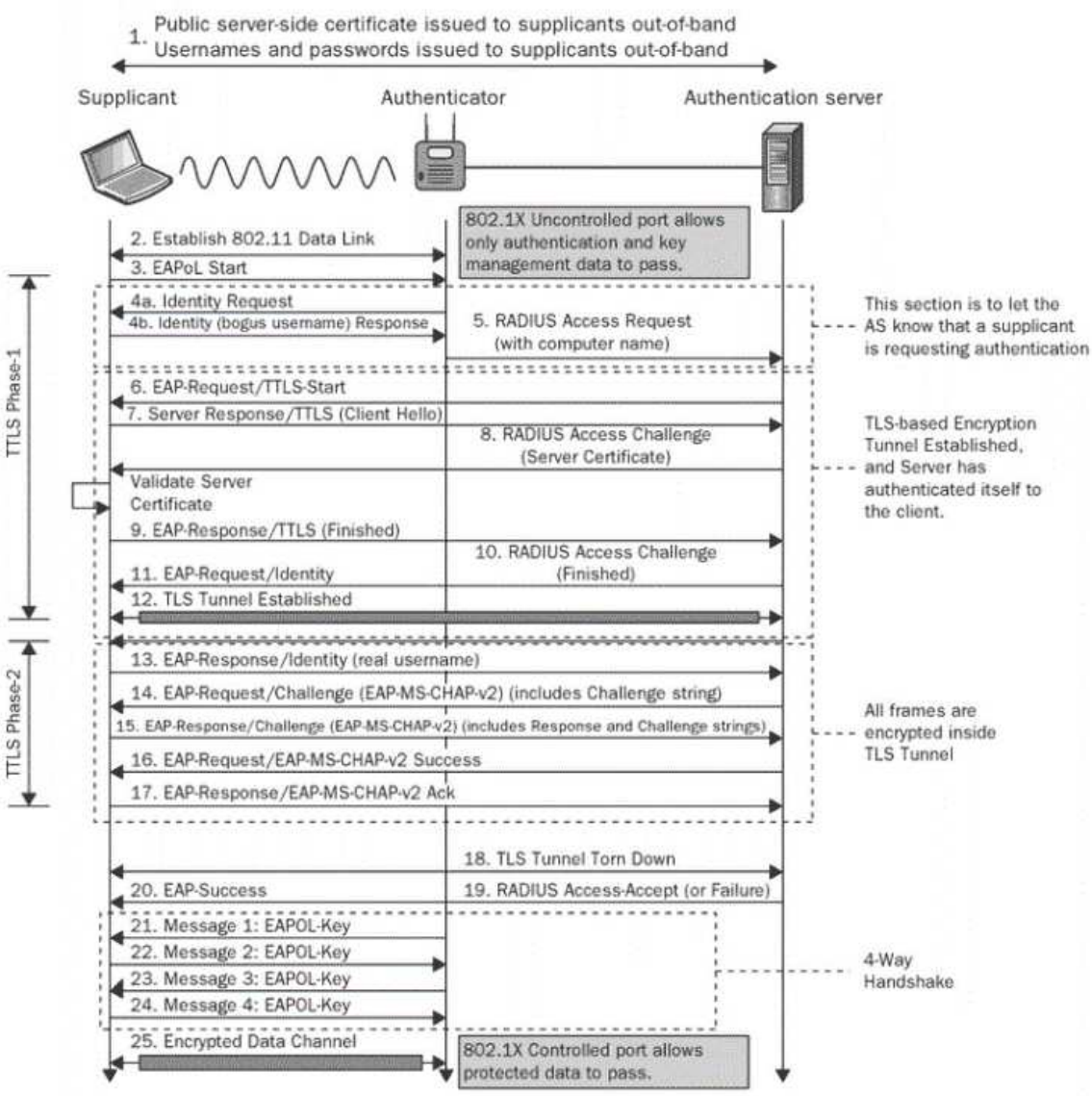

Figura 2 – Fluxo de autenticação para EAP-TTLS. Fonte: Raj (34)

2.2.4 Infraestrutura de AAA

A segurança em redes modernas, especialmente em ambientes corporativos, acadêmicos e distribuídos, transcende a simples proteção do tráfego por meio de criptografia. Ela demanda um modelo estruturado de controle de acesso, capaz de garantir quem pode acessar a rede, quais recursos estão disponíveis para cada entidade autenticada e o registro detalhado das atividades realizadas. Este modelo é consolidado pelo conceito de AAA – *Authentication, Authorization and Accounting*, considerado um pilar essencial na segurança e no gerenciamento de redes. No contexto de redes que utilizam o protocolo IEEE 802.1X, amplamente empregado em redes Wi-Fi corporativas, acadêmicas e em redes cabeadas seguras, o modelo AAA permite a gestão centralizada e eficiente do acesso, garantindo segurança, conformidade e visibilidade operacional. A autenticação garante

que apenas entidades devidamente identificadas possam acessar a rede, prevenindo uso indevido de credenciais. A autorização define os privilégios de cada usuário autenticado, assegurando acesso proporcional ao seu perfil e papel. E o *accounting*/auditoria registra e monitora atividades realizadas, fornecendo subsídios para cobrança, rastreabilidade e outras possibilidade de análise de dados, como, por exemplo, detecção de anomalias (37).

O protocolo RADIUS (*Remote Authentication Dial-In User Service*) desempenha um papel central na implementação prática do modelo AAA em redes modernas, suportanto, inclusive, os métodos EAP apresentados (3, 36). Sua arquitetura segue o modelo cliente-servidor, no qual os dispositivos de rede, como *switches*, controladores Wi-Fi e pontos de acesso (denominados *Network Access Servers* – NAS), atuam como clientes RADIUS, enquanto o servidor AAA centralizado executa as funções de autenticação, autorização e auditoria.

Durante o processo de autenticação, quando um usuário ou dispositivo tenta se conectar à rede, o NAS envia uma mensagem `Access-Request` ao servidor RADIUS, contendo as credenciais fornecidas. O servidor RADIUS processa essa solicitação, validando as credenciais contra seu banco de dados local ou serviços externos, como *Lightweight Directory Access Protocol* (LDAP), Active Directory ou bases SQL. O resultado é retornado na forma de uma mensagem `Access-Accept` (permite acesso) ou `Access-Reject` (nega acesso).

Nesse contexto, o LDAP, definido pela RFC 4511, funciona como o principal protocolo para interação com repositórios de identidade centralizados (40). Operando sobre uma base de dados hierárquica (*Directory Information Tree* - DIT), onde cada entrada representa um objeto descrito por um conjunto de atributos, o LDAP provê uma interface padronizada para consulta e gerenciamento de identidades. Em sistemas de controle de acesso à rede os servidores RADIUS (36) atuam como clientes LDAP, consultando o diretório para validar a existência de um usuário e recuperar atributos necessários ao processo de autenticação. É fundamental destacar esta separação de responsabilidades, onde o LDAP atua exclusivamente como um *backend* de armazenamento de identidade, enquanto a lógica do protocolo de autenticação (e.g., um método EAP específico) é executada pelo servidor RADIUS, que utiliza os dados obtidos do diretório para completar o processo.

2.3 eduroam

O eduroam (education roaming) é um serviço que atua sobre uma infraestrutura de *roaming* global e federado, e que provê acesso à rede sem fio para a comunidade de ensino e pesquisa, conectando milhares de instituições em mais de 100 países (17). Sua arquitetura é fundamentada em uma federação hierárquica de servidores RADIUS e um modelo de confiança distribuída, permitindo que um usuário de uma instituição de origem

(*Home Institution*) se autentique na rede de uma instituição visitada (*Visited Institution*) utilizando suas credenciais institucionais. O mecanismo de roteamento das solicitações de autenticação é viabilizado pelo uso do identificador no formato `user@realm`, que permite ao RADIUS local encaminhar o pedido ao servidor da instituição de origem do usuário através da federação (47).

Tecnicamente, o eduroam implementa o padrão IEEE 802.1X para controle de acesso e utiliza o EAP para a autenticação em si. Os métodos EAP mais prevalentes na federação são os tunelados, como PEAP e EAP-TTLS, que estabelecem um canal TLS seguro para proteger a autenticação interna. Tipicamente, o método interno utilizado é o MS-CHAPv2, escolhido por sua ampla compatibilidade e integração com serviços de diretório legados. Contudo, esta escolha representa um comprometimento de segurança, uma vez que o MS-CHAPv2 possui vulnerabilidades criptográficas conhecidas que o tornam suscetível a ataques de dicionário offline para recuperação de senhas (29), representando um risco significativo para as credenciais dos usuários da federação. É importante destacar que o método EAP-TLS é suportado por implemntações do protocolo RADIUS (e.g., FreeRADIUS[1]), porém não utilizado atualmente na federação brasileira, o que fomenta a importância desta pesquisa.

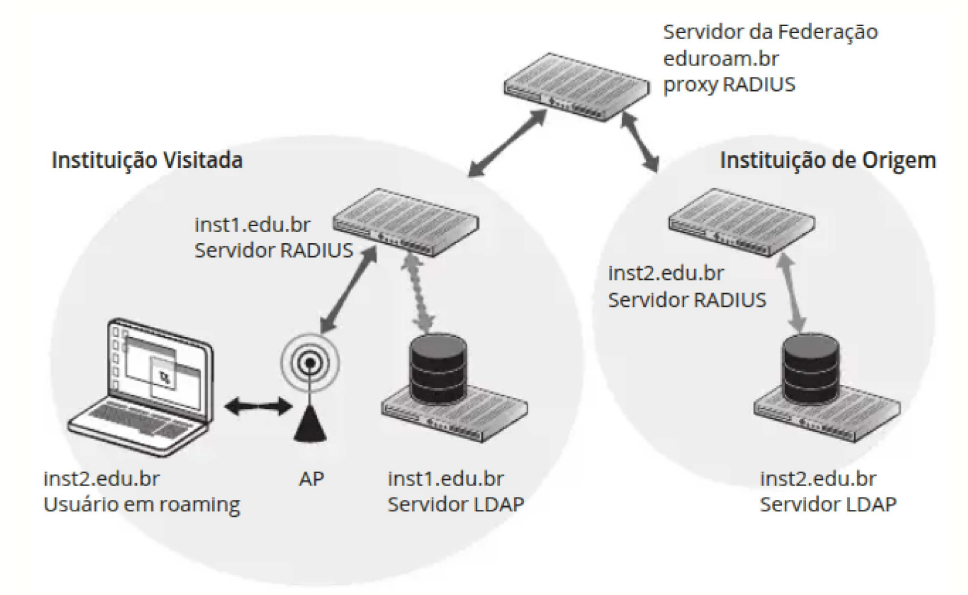

Figura 3 – Estrutura da hierarquia no eduroam para autenticação e roaming. Fonte: Saade et al. (37)

A Figura 3 exemplifica um usuário visitando a inst1.edu.br, e com o seu usuário, através do *realm* @inst2.edu.br, sua requisição de autenticação é encaminhada para verificação em sua instituição de origem. Uma vez confirmadas as credenciais do usuário na inst2.edu.br, um pacote do tipo `Access-Accept` é encaminhado ao AP, neste caso,

[1] `https://www.freeradius.org/`

responsável por liberar o acesso à rede local da instituição visitada. Nesse cenário, protocolos EAP, RADIUS são utilizados. O usuário tem o encaminhamento da mensagem de solicitação de autenticação ponta a ponta encaminhada pelo protocolo EAP de primeira fase, por exemplo, o EAP-TTLS, e localmente na inst2.edu.br, é verificada a segunda fase do EAP, com, por exemplo, verificação da credencial pelo desafio armazenado em MS-CHAPv2. Essa troca de mensagens acontece por meio do protocolo RADIUS, apoiado no IEEE 802.1X.

2.4 ICPEdu

A segurança de identidades digitais em ambientes distribuídos depende de um *framework* de confiança robusto. No Brasil, este ecossistema é regulamentado pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), instituída pela Medida Provisória nº 2.200-2 (33). Para atender às necessidades específicas do setor de ensino e pesquisa, a Rede Nacional de Ensino e Pesquisa (RNP) desenvolveu e opera a ICPEdu, uma infraestrutura de chaves públicas (ICP) própria e independente da ICP-Brasil, construída com base nos padrões globais de PKI (28, 35). A ICPEdu estabelece sua própria cadeia de confiança, desde a raiz, para o ambiente acadêmico.

O projeto ICPEdu representa um esforço contínuo da Rede Nacional de Ensino e Pesquisa (RNP) para viabilizar a implantação de uma infraestrutura de chaves públicas acadêmica (28, p. 42). Seus principais objetivos são:

- **Uso acadêmico:** Viabilizar o uso de certificação digital para autenticação de pessoas e equipamentos dentro das instituições.
- **Autenticação:** Promover a autenticação segura em ambientes digitais.
- **Cultura em Certificação Digital:** Desenvolver e difundir o conhecimento sobre certificação digital na comunidade acadêmica, através de treinamento e pesquisa.
- **Aplicações:** Criar e implementar softwares e ferramentas para otimizar o uso da ICP em instituições de ensino e pesquisa.

Historicamente, o projeto ICPEdu iniciou-se em 2003 com o desenvolvimento do Sistema de Gerenciamento do Ciclo de Vida de Certificados Digitais (SGCI). Marcos importantes incluem a introdução do Módulo de Segurança Criptográfica (HSM) em 2005, a criação do piloto da AC Raiz em 2006, e o lançamento de um serviço experimental em 2007, que envolveu seis instituições. A partir de 2008, o projeto entrou em uma fase de implantação em larga escala e aprimoramentos contínuos, com credenciamentos e proposição de novos modelos de adesão entre 2010 e 2013 (28, p. 42-43).

A estrutura da ICPEdu é hierárquica, composta por Autoridades Certificadoras (ACs) e Autoridades de Registro (ARs), análogo ao modelo ICP-Brasil, mas adaptado

ao ecossistema acadêmico. No topo da cadeia de confiança está a AC Raiz ICPEdu, que certifica as ACs subordinadas. Para certificados pessoais, destaca-se a AC Pessoa ICPEdu, responsável pela emissão de certificados digitais para indivíduos (professores, pesquisadores, alunos, técnicos administrativos) vinculados às instituições. As Autoridades de Registro (ARs) atuam como ponto de contato com o usuário, realizando a verificação de identidade. A integração com a Comunidade Academica Federada (CAFe) é crucial para a validação da identidade federada antes da emissão do certificado.

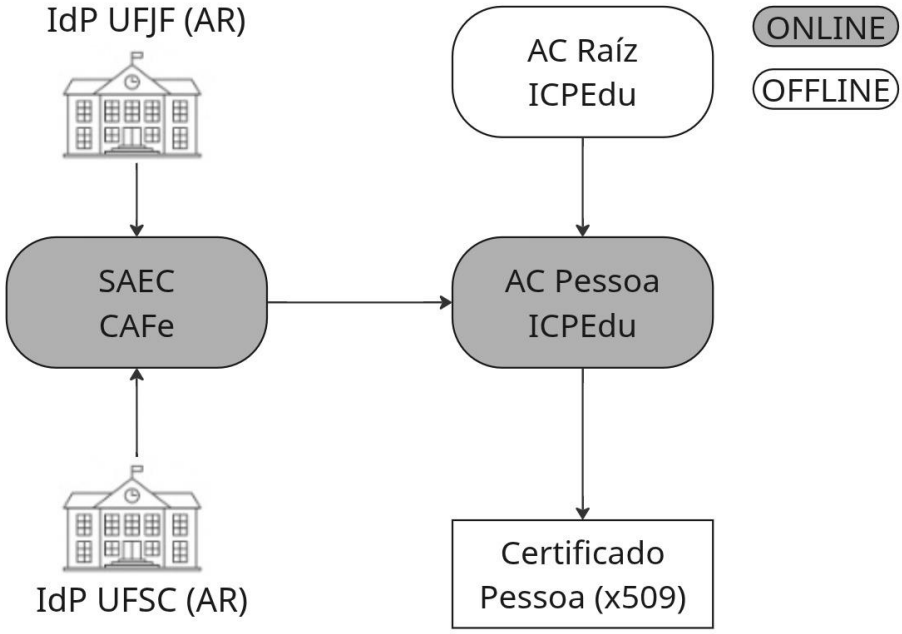

Figura 4 – Cadeia de Certificação do ICPEdu para Certificados Pessoais.

A Figura 4 ilustra a cadeia de certificação para certificados pessoais dentro da ICPEdu, demonstrando sua hierarquia própria e independente. A AC Raiz opera como a raiz de confiança, enquanto a AC Pessoa e outras entidades subordinadas integram essa estrutura.

2.4.1 Padrão X.509

A base da confiança digital é o certificado digital, uma estrutura de dados que liga criptograficamente uma identidade a uma chave pública, com sua autenticidade atestada pela assinatura de uma Autoridade Certificadora (AC). O padrão de fato para o formato desses certificados é o ITU-T X.509 (24), que define uma estrutura rigorosa de campos para garantir interoperabilidade e segurança. Entre os campos mais críticos, destacam-se:

- **Subject e Issuer:** Identificam, respectivamente, o titular e o emissor do certificado através de um *Distinguished Name* (DN). Esses campos são a base para a construção das cadeias de confiança.

- **Subject Public Key Info:** Contém a chave pública do titular e o algoritmo associado (e.g., RSA, ECDSA), constituindo o núcleo criptográfico do certificado.
- **Validity:** Define o período de validade do certificado (datas *Not Before* e *Not After*), sendo fundamental para o gerenciamento do ciclo de vida da credencial.
- **Signature:** A assinatura digital da AC sobre os campos anteriores, que garante a integridade e autenticidade do certificado.

Para garantir a interoperabilidade, os dados são estruturados usando a notação *Abstract Syntax Notation One* (ASN.1) e codificados em formato binário determinístico via *Distinguished Encoding Rules* (DER), assegurando que a representação binária seja sempre idêntica e, assim, validável criptograficamente.

2.4.2 Evolução do X.509: v1, v2 e v3

O padrão de certificados X.509 evoluiu significativamente para atender às crescentes demandas de sistemas distribuídos, com a versão 3 sendo a base de toda a PKI moderna.

Versão 1 (1988): Estabeleceu o formato fundamental, contendo os campos essenciais mencionados anteriormente. Sua principal limitação era a falta de flexibilidade; não havia como adicionar informações contextuais ou identificar de forma unívoca emissores e titulares caso seus nomes fossem reutilizados ao longo do tempo. Era um modelo funcional, porém rígido.

Versão 2 (1993): Introduziu os campos *Issuer Unique Identifier* e *Subject Unique Identifier*. O objetivo era resolver a ambiguidade de nomes (DNs), fornecendo um identificador único para o emissor e o titular. No entanto, esta versão teve pouca adoção, pois a comunidade técnica percebeu que uma solução mais genérica e extensível era necessária.

Versão 3 (1996): Representou a maior evolução do padrão ao introduzir o campo **Extensions**. Este campo é um contêiner para informações adicionais que definem restrições, políticas e atributos avançados, conferindo a flexibilidade que faltava nas versões anteriores. As extensões são a base para a funcionalidade da PKI moderna, sendo as mais importantes definidas no perfil da IETF para a internet (7):

- **Key Usage:** Define os propósitos criptográficos da chave (e.g., `digitalSignature`, `keyEncipherment`).
- **Extended Key Usage:** Especifica os usos em nível de aplicação (e.g., `serverAuth` para TLS, `emailProtection`).

- **Subject Alternative Name (SAN):** Permite associar múltiplas identidades (como nomes de domínio, endereços de e-mail ou IPs) a um único certificado, sendo essencial para aplicações web modernas.
- **Authority Key Identifier e Subject Key Identifier:** Ajudam a construir e validar cadeias de certificados de forma inequívoca, especialmente quando emissores possuem múltiplas chaves.

A versão 3 transformou o certificado de um simples atestado de identidade em um instrumento de política e autorização altamente flexível.

2.4.3 Modelo PKI

A Infraestrutura de Chaves Públicas (PKI) é o ecossistema de tecnologias, políticas e procedimentos que gerencia o ciclo de vida dos certificados digitais. Embora existam diferentes modelos de confiança, o mais comum é o **modelo hierárquico**.

- **Autoridade Certificadora Raiz (AC Raiz):** O ponto de confiança fundamental da hierarquia. Seu certificado é autoassinado e distribuído para as partes confiantes (e.g., embutido em sistemas operacionais e navegadores). A chave privada da AC Raiz é o ativo mais crítico, sendo mantida em altíssimo nível de segurança, geralmente offline.
- **Autoridades Certificadoras Intermediárias (ACs Intermediárias):** São certificadas pela AC Raiz (ou por outra AC Intermediária superior) e formam a cadeia de confiança. Elas são responsáveis pela emissão de certificados para as entidades finais. Essa estrutura limita o impacto de um comprometimento: se uma AC Intermediária for comprometida, apenas os certificados emitidos por ela são afetados, e seu certificado pode ser revogado pela autoridade superior.
- **Autoridades de Registro (ARs):** Atuam como intermediárias que validam a identidade dos solicitantes em nome de uma AC, separando a função de verificação da função criptográfica de emissão.
- **Validação de Status:** Um pilar da PKI é a capacidade de invalidar um certificado antes de seu vencimento. Isso é feito publicando seu número de série em uma Lista de Certificados Revogados (CRL) ou através do Online Certificate Status Protocol (OCSP) (38), que permite uma consulta de status em tempo real.

2.4.4 ICPEdu: Aplicação da PKI no Ecossistema de Ensino e Pesquisa

A ICPEdu é uma infraestrutura de chaves públicas (ICP) própria e independente da ICP-Brasil, estabelecendo sua própria cadeia de confiança desde a raiz para o ambiente

acadêmico (25, 32). Seu propósito fundamental é viabilizar e fortalecer o uso acadêmico de certificação digital, capacitando e apoiando a comunidade de ensino e pesquisa, o que a distingue no cenário das PKIs nacionais. A ICPEdu emite certificados X.509 v3, os quais podem explorar plenamente o campo de extensões para agregar valor, inclusive incorporando atributos institucionais (e.g., vínculo, curso, departamento) extraídos de sistemas de gestão de identidade. Estes atributos permitem a implementação de políticas de autorização granulares e a integração segura com serviços federados, como o eduroam, tornando o certificado um instrumento multifuncional de identidade digital que vai além da simples autenticação.

A versatilidade da ICPEdu estende-se à capacidade de emitir diversos tipos de certificados digitais, atendendo tanto às necessidades de indivíduos quanto de serviços e equipamentos dentro das instituições acadêmicas. Conforme os objetivos do projeto, a certificação digital é viabilizada para a autenticação de pessoas e equipamentos. Na prática, a ICPEdu oferece suporte à emissão de certificados que abrangem desde o uso pessoal – como os utilizados para assinatura e cifragem de e-mails – e, embora sua aplicação principal hoje seja para usuários, sua infraestrutura pode ser modificada para a emissão de certificados para outras aplicações em serviços e equipamentos, como as que garantem a segurança de comunicações SSL/TLS.

A fim de ilustrar o processo de geração do certificado pessoal para o usuário no âmbito do ICPEdu, serão apresentados os as entidades e o fluxo de interação entre elas.

O fluxo representado na Figura 5 contempla tanto as etapas no serviço ICPEdu, representando a emissão (setas 1, 7, 8 e 9), quanto na CAFe, representando a identificação e validação (setas de 2 a 6). O fluxo em questão foi reproduzido neste documento conforme a descrição existente na página oficial do serviço ICPEdu Pessoal[2].

1. O usuário acessa o portal e solicita o certificado digital, iniciando o processo de emissão;

2. A identificação do usuário é realizada através da federação CAFe, nessa etapa o usuário seleciona sua instituição de origem. A lista de instituições é apresentada com base nas informações mantidas pelo servidor WAYF (*Where Are You From*) da RNP. O WAYF é responsável pela chamada descoberta de serviço, onde o usuário indica qual sua instituição, e onde ele irá se autenticar;

3. Uma vez selecionada a instituição, a identificação do usuário é realizada através do provedor de identidade (IdP) da instituição;

4. O IdP verifica e autentica o usuário consultando a base LDAP da instituição;

[2] `http://ajuda.rnp.br/icpedu/cp/certificado-pessoal`

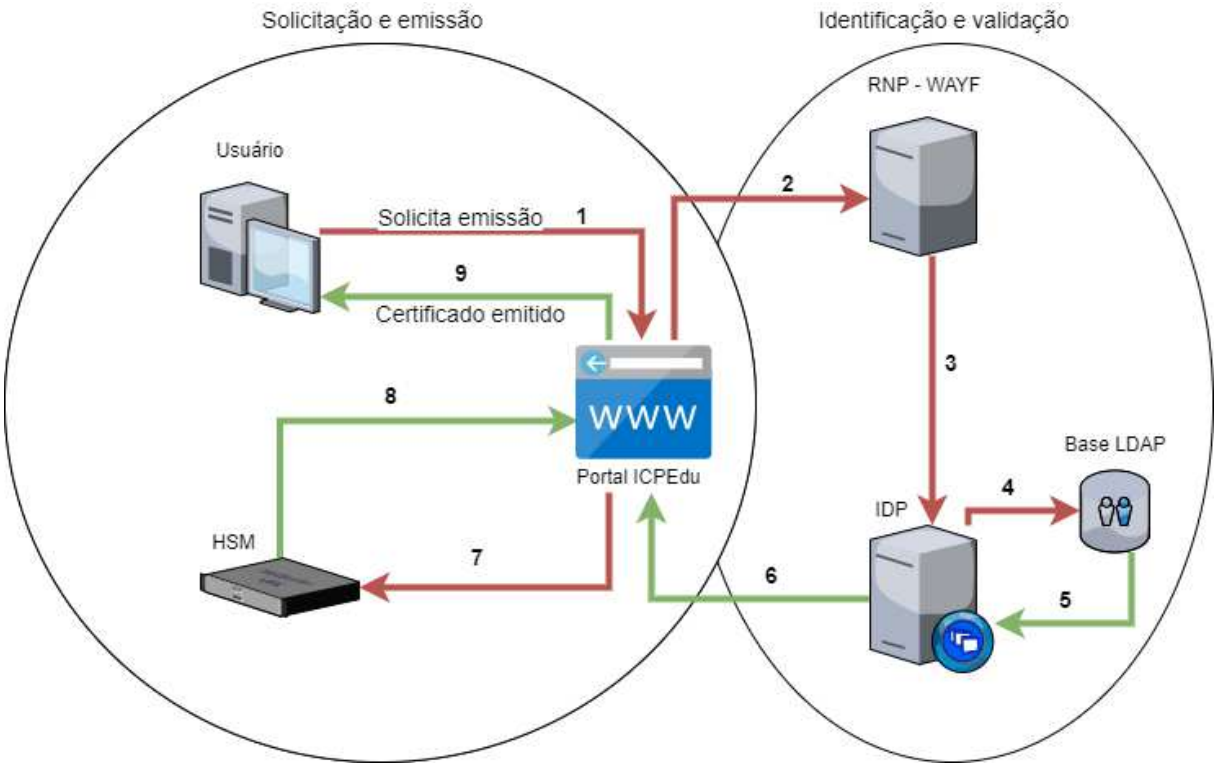

Figura 5 – Fluxo de emissão do Certificado Pessoal da ICPEdu. Fonte: (35).

5. Validado a existência do usuário, a base LDAP retorna os metadados do usuário para o IDP, contendo o nome completo, e-mail, CPF e data de nascimento;

6. O IdP retorna ao portal fornecendo os dados recebidos da base LDAP;

7. O portal gera as chaves públicas e privadas a serem fornecidas para o usuário e com os dados recebidos do IDP, gera uma requisição de certificado e encaminha para a assinatura pelo HSM. Sendo o HSM, do Inglês, *Hardware Security Module*, os dispositivos físicos que fornecem segurança extra para chaves criptográficas, como um certificado digital;

8. O HSM, equipamento criptográfico especializado, possui a chave privada da AC Pessoa (Autoridade Certificadora da ICPEdu) e com ela assina o certificado do usuário. A utilização do equipamento garante que a chave privada da AC nunca seja exposta;

9. Por fim, o portal empacota o certificado recebido do HSM e a chave privada gerada para o usuário em um arquivo protegido por senha no formato PKCS #12, e o disponibiliza para *download* pelo usuário.

2.5 Conclusão

portanto, este capítulo estabeleceu a fundamentação teórica necessária para a compreensão do restante deste trabalho. Além dos protocolos de segurança Wi-Fi, passando pela arquitetura IEEE 802.1X, métodos EAP e a infraestrutura AAA, foram também detalhadas as estruturas e os objetivos dos serviços eduroam e da ICPEdu como uma infraestrutura de chaves públicas autônoma e especializada para o ambiente acadêmico brasileiro.

Agora é possível seguirmos para o próximo capítulo, que aprofundará a discussão sobre os trabalhos relacionados. A partir dessa fundamentação teórica, o próximo capítulo aborda as vulnerabilidades específicas que motivam esta pesquisa e a relação dos certificados ICPEdu com EAP-TLS como uma resposta a esses desafios.

3 TRABALHOS RELACIONADOS

A literatura recente sobre segurança em redes sem fio acadêmicas tem destacado vulnerabilidades presentes nos sistemas de autenticação federada, especialmente no serviço eduroam (16, 31, 30). Este capítulo apresenta os principais estudos que identificaram fragilidades em métodos tradicionais de autenticação, além de propor encaminhamentos para mitigação e apontar lacunas que motivam esta dissertação. Inicialmente, são discutidos trabalhos sobre ataques às tecnologias empregadas pelo eduroam e WPA2-Enterprise; em seguida, abordam-se iniciativas de mitigação e, por fim, a identificação da lacuna de investigação que esta pesquisa busca preencher.

3.1 Vulnerabilidades no WPA2-Enterprise/eduroam

O trabalho seminal de Brenza et al. (4), demonstra a fragilidade que pode existir na configuração do cliente (suplicante) em ambientes WPA2-Enterprise, como o eduroam. Guias de configuração com flexibilização ou erros em relação à escolha da segurança, unido à falta de conhecimento por parte do usuário, abre brechas para a exploração e indução ao acesso em redes inseguras pelo usuário. No momento do trabalho, em 2015, foi constatado que uma grande parcela dos dispositivos clientes não possuia o certificado de CA raiz necessário para autenticar na rede, mas ainda assim conseguia acessá-la. Isso se deve, principalmente, à aceitação indiscriminada e automática de certificados TLS dos servidos RADIUS aos quais o usuário está se autenticando. À época, os autores realizaram um ataque que explorou esse fato, e utilizando o comportamento padrão de dispositivos sem fio, pôde capturar dados de autenticação. Para tanto, criaram um ponto de acesso falso e executaram um ataque do tipo homem-no-meio (*Man in the Middle* - MITM), demonstrando a eficiência da manipulação dos dados quando, mesmo utilizando certificados TLS (i.e., para os métodos de fase 1: TTLS e PEAP, neste caso), as mensagens puderam ser interceptadas pelo atacante. Para fins da análise de impacto, os autores realizaram uma contagem sobre os possíveis afetados em sua instituição. Os resultados mostram que de um total de dispositivos de 507 dispositivos, 52% eram vulneráveis, sendo que desse total, 20% dos dispositivos vulneráveis usavam ainda somente o método PAP como método de autenticação interna e, portanto, estavam vazando dados de autenticação de forma não criptografada (e.g., a senha).

Destacando um trabalho mais recente (2022), com a mesma linha de investigação, Palamà et al. retratam uma avaliação experimental atualizada e importante das vulnerabilidades do eduroam. Através de uma metodologia que envolveu 37 participantes considerados tecnicamente qualificados da Universidade de Roma, os autores demonstraram, empiricamente, que as falhas de segurança documentadas na literatura acadêmica persistem de forma alarmante na prática cotidiana. A principal contribuição metodológica

do estudo reside na transição de análises puramente teóricas para uma avaliação experimental com usuários reais. Os autores implementaram um ataque do tipo Evil Twin utilizando hostapd-wpe (48) e FreeRADIUS, configurando um ponto de acesso malicioso que simulava perfeitamente uma rede eduroam legítima. A escolha de participantes com formação técnica em engenharia elétrica e da computação, muitos com conhecimento em cibersegurança, torna os resultados ainda mais significativos, pois demonstra que mesmo usuários qualificados são vulneráveis a ataques relativamente simples. Os autores mostram uma taxa de comprometimento de 45,9% dos participantes (17 de 37), obtida através de ataques completamente passivos - onde os usuários mantinham dispositivos no bolso sem interação ativa - evidenciando a gravidade das configurações padrão inseguras. Este resultado é particularmente preocupante quando consideramos que o eduroam serve aproximadamente 30 milhões de usuários em mais de 100 países, sugerindo que milhões de credenciais acadêmicas estão potencialmente expostas a ataques similares.

Uma das descobertas mais significativas do estudo refere-se às diferenças marcantes de segurança entre plataformas. A taxa de comprometimento de 68,2% em dispositivos Android contrastou drasticamente com a resistência completa (0%) demonstrada pelos dispositivos iOS. Esta disparidade não é meramente técnica, mas reflete filosofias fundamentalmente diferentes de design de segurança. Como contramedidas propostas pelos autores há, principalmente, indicações de melhorias incrementais nas configurações existentes - como tornar a validação de certificados padrão no Android ou melhorar a informação sobre ciberataques aos usuários finais. Embora válidas, essas propostas não abordam a vulnerabilidade fundamental dos métodos baseados em credenciais compartilhadas, que permanece como um ponto de falha sistêmico independentemente de melhorias na interface ou educação do usuário.

Os autores ainda realizam uma publicação com mais resultados e uma análise mais aprofundada sobre o mesmo conjunto de dados de (31), mas agora também sobre um cenário diferente e menos controlado. Conforme apresentado em (30), os autores agora conduziram um experimento em um ambiente mais proximo ao real de uma instituição com eduroam. Eles chamaram esse experimento de “in-the-wild”, e o realizaram na Universidade de Bresci, também na Itália. Os resultados confirmam os achados do trabalho anterior.

Já em Hue et al. (21), são apresentadas falhas relacionadas ao WPA2-Enterprise, mais especificamente com foco no ambiente utilizado pela federação eduroam e seu ambiente que provê auxílio á configuração de acesso ao serviço, chamado de CAT (*Configuration Assistant Tool*) [1]. A partir do eduroam CAT um usuário pode encontrar sua instituição e realizar o download de auxiliares da configuração inicial de acesso à rede. Nessas configurações são obtidos, por exemplo, os certificados para conexão com o servidor RADIUS da instituição. Os autores consideraram 7045 instituições em 54 países/regiões, e coletaram

[1] `https://eduroam.org/configuration-assistant-tool-cat/`

7.275 instruções de configuração de 2.061 instituições. os resultados demonstraram que a maioria dessas instruções leva a configurações inseguras, e quase 86% deles poderiam sofrer roubos de credenciais em pelo menos um sistema operacional. Um dos pontos de destaque nos resultados foram os parâmetros TLS usados por servidores de autenticação de grande parte das instituições, que apresentaram o que os autores chamaram de "práticas perigosas", como o uso de certificados expirados, versões obsoletas de TLS, algoritmos de assinatura fracos e casos suspeitos de reutilização de chaves privadas entre instituições. Tais achados reforçam ainda mais a necessidade de utilização de certificados válidos e mantidos por infraestruturas de chaves públicas confiáveis, como os da ICPEdu, tanto para o usuário final quanto para comunicação entre servidores RADIUS na federação.

Já em um momento ainda mais recente (2024), com a ampla divulgação de uma falha histórica, chamada agora de BlastRADIUS por Goldberg et al. (15), lançou-se luz sobre uma relação ainda mais fundamental sobre as falhas sistêmicas em protocolos de autenticação amplamente utilizados. Esta vulnerabilidade, presente no protocolo RADIUS há décadas, demonstra como construções criptográficas *ad hoc* podem comprometer a segurança de infraestruturas críticas. O ataque em questão explora uma vulnerabilidade no protocolo RADIUS que permite a um atacante *man-in-the-middle* forjar respostas Access-Accept válidas para requisições de autenticação. A vulnerabilidade baseia-se na exploração de colisões do algoritmo de *hash* MD5 e na construção *ad hoc* para mensagens de *Response Authenticator* do RADIUS, permitindo que um atacante transforme uma resposta de rejeição em uma de aceitação sem conhecimento do segredo compartilhado entre cliente e servidor. A gravidade desta vulnerabilidade é amplificada por sua ampla adoção em diversos equipamentos de rede, como *switches*, roteadores, até pontos de acesso e VPNs vendidos nos últimos anos. Além do eduroam, que processou 8,4 bilhões de autenticações em 2024 [2], o protocolo é fundamental para provedores de acesso à Internet, seja em ambientes *Fiber to the Home* (FTTH), autenticação 802.1X e Wi-Fi, até autenticação 5G, além de outros.

Apresentando um pouco mais sobre o cenário de falha explorado, os autores realizaram a otimização o ataque MD5 *chosen-prefix* para produzir colisões online em menos de cinco minutos, demonstrando viabilidade prática mesmo com as limitações temporais de sessões RADIUS. Esta otimização representa uma evolução significativa das técnicas de ataque, tornando a exploração em tempo real não apenas possível, mas praticamente inevitável para atacantes bem equipados. A implementação bem-sucedida do ataque contra FreeRADIUS, Okta, Cisco ASA e Linux PAM demonstra que a vulnerabilidade não é específica de implementação, mas inerente ao protocolo. Para o eduroam especificamente, a vulnerabilidade BlastRADIUS representa uma ameaça existencial. A natureza federada do sistema, onde múltiplos servidores RADIUS encaminham requisições através de

[2] `https://eduroam.org/eduroam-hits-a-new-record-8-4-billion-authentications-in-2024/`

hierarquias nacionais e internacionais, multiplica as oportunidades de exploração. Um atacante posicionado em qualquer ponto da cadeia de encaminhamento pode comprometer autenticações, potencialmente afetando usuários de instituições distantes geograficamente. Como mitigação, os próprios autores do trabalho demonstram a utilização da autenticação de cada mensagem como uma solução, e no guia da empresa InkBridge Networks [3] (dos autores do FreeRadius) (8) é afirmado que soluções que utilizam TLS não estão sucetíveis ao ataque.

A análise conjunta dos estudos revela padrões sistêmicos preocupantes que transcendem falhas específicas de implementação. Ambas as vulnerabilidades exploram a dependência de algoritmos e construções criptográficas que eram consideradas seguras quando implementadas, mas que se tornaram inadequadas com o avanço das técnicas de ataque. O uso de MD5 no RADIUS e as vulnerabilidades do MS-CHAPv2 no EAP-TTLS/PEAP exemplificam como a inércia tecnológica pode perpetuar riscos de segurança. Os ataques Evil Twin documentados e a possibilidade de forjamento de respostas RADIUS, por exemplo, demonstram falhas fundamentais nos mecanismos de estabelecimento e validação de confiança. Em ambos os casos, atacantes podem se fazer passar por entidades legítimas explorando fraquezas nos protocolos de autenticação mútua. Propostas para melhorar interfaces de configuração, embora válidas, não abordam o problema fundamental de que usuários finais não deveriam ser responsáveis por decisões críticas de segurança. A complexidade inerente da validação de certificados torna improvável que melhorias na interface eliminem completamente configurações incorretas. Além disso, a persistência do uso de RADIUS/UDP e métodos EAP vulneráveis, apesar da disponibilidade de alternativas mais seguras, demonstra a resistência sistêmica à adoção de melhorias de segurança. Fatores como compatibilidade com sistemas legados, custos de migração e inércia organizacional perpetuam o uso de tecnologias inseguras.

As vulnerabilidades sistêmicas documentadas convergem para uma conclusão: *"métodos de autenticação baseados em credenciais compartilhadas e protocolos com construções criptográficas proprietárias são fundamentalmente inadequados para ambientes de acessos federados em redes Wi-Fi"*. Diante desta realidade, a literatura e a prática têm convergido para uma solução que elimina sistematicamente estas vulnerabilidades, a autenticação baseada em certificados digitais através do protocolo EAP-TLS.

3.2 Mitigação

O trabalho de Zhang et al. (49) fornece a validação matemática necessária em relação à robustez do método EAP-TLS como uma solução robusta para as vulnerabilidades sistêmicas identificadas. Tal pesquisa transcende análises empíricas ao oferecer provas

[3] `https://www.inkbridgenetworks.com/`

formais de que o protocolo, quando corretamente implementado, elimina sistematicamente as classes de vulnerabilidades que afetam métodos tradicionais.

A análise formal demonstra matematicamente que o EAP-TLS elimina completamente a possibilidade de *credential harvesting* (roubo de credenciais) através de sua arquitetura baseada em certificados. Diferentemente dos métodos tradicionais onde credenciais compartilhadas podem ser interceptadas e reutilizadas (21), o EAP-TLS utiliza um processo de autenticação mútua, onde tanto cliente quanto servidor devem apresentar certificados válidos. Esta validação mútua impossibilita que um atacante *Evil Twin*, por exemplo, obtenha sucesso em sua personificação de ponto de acesso eduroam sem possuir um certificado válido emitido por uma Autoridade Certificadora confiável.

Os autores empregaram o cálculo pi aplicado (*applied pi calculus*), uma linguagem formal desenvolvida para descrever e analisar sistemas concorrentes e protocolos criptográficos, para especificar formalmente as interações entre o UE, a rede de serviço e a rede doméstica. A verificação foi realizada com ProVerif, um verificador automático que analisa propriedades como autenticação e confidencialidade, considerando um adversário no modelo Dolev-Yao — onde o atacante controla totalmente o canal de comunicação, mas não viola criptografia perfeita. Os resultados confirmam que o protocolo garante autenticação mútua mesmo sob essa ameaça extrema.

Tal validação teórica é corroborada por evidências empíricas, como a resistência de implementações que forçam a validação rigorosa de certificados a ataques práticos de interceptação de credenciais, apresentado por (31, 8). Desta forma, a arquitetura EAP-TLS, quando corretamente implementada, representa uma solução definitiva para as fragilidades de autenticação discutidas. Assim, nesta pesquisa adotamos como premissa que as propriedades de segurança fundamentais do EAP-TLS são uma questão resolvida, permitindo que o foco da investigação se desloque da validação de sua segurança para os desafios de otimização, usabilidade e implementação em larga escala.

3.3 Discussão e Direcionamento

Com a segurança do EAP-TLS firmemente estabelecida, e considerando a clara direção do ecossistema para soluções baseadas em certificados, emerge uma lacuna crítica na literatura: a ausência de avaliações rigorosas de performance do EAP-TLS em contextos de implementação específicos. Essa lacuna é particularmente relevante no cenário brasileiro, onde a ICPEdu oferece uma oportunidade para a implementação de autenticação baseada em certificados no eduroam.

A transição de análises de segurança para avaliações de performance é um passo natural e necessário. Embora as propriedades criptográficas do EAP-TLS sejam matematicamente garantidas, sua viabilidade prática em diversos contextos depende de características de performance que podem variar significativamente entre implementações,

infraestruturas PKI e ambientes operacionais. Essa realidade torna a avaliação experimental de performance não apenas relevante, mas essencial para decisões informadas sobre a adoção em larga escala.

O trabalho de Gaminara (13) estabelece um modelo sistemático para a avaliação comparativa de performance em protocolos de aplicação relacionados à comunicação segura. A saber, são eles: o TLS, DTLS e QUIC. Na pesquisa realizada, são fornecidas métricas multidimensionais (i.e., tempo de estabelecimento de conexão, *Time To First Byte* - TTFB, *throughput*, *overhead* computacional e escalabilidade de conexões simultâneas) por meio de uma metodologia experimental replicável. Este *framework* permite simulações controladas de condições de rede (e.g., latência, largura de banda, perda de pacotes) e análise estatística robusta, estabelecendo valores-base importantes para o comportamento de tais protocolos. Porém, o ambiente validado pelo autor é restrito à *web*, focando em aplicações do tipo *HTTP*, e acrescido de um pequeno cenário de rede ponto a ponto em *Mininet* [4] para avaliação do desempenho do *handshake* dos protocolos.

Assim, foi percebida uma lacuna específica, a qual nesta pesquisa visamos preencher: *"a ausência de estudos que avaliem a performance do EAP-TLS utilizando certificados de infraestruturas PKI nacionais, notadamente no contexto de autenticação nas redes Wi-FI acadêmica"*.

Infraestruturas como a ICPEdu possuem características únicas (cadeias de certificação, algoritmos, distribuição geográfica e políticas de revogação) que podem impactar a performance. Além disso, o ambiente acadêmico brasileiro apresenta especificidades como a distribuição geográfica das instituições que fazem parte do serviço, a diversidade de dispositivos e padrões de uso. Por fim, o Brasil possui a maior rede eduroam dentre todos os integrantes da consórcio global, se comparada em número de pontos de acesso, o que torna necessária a avaliação dos impactos da adoção de outros métodos de segurança.

Assim, esta pesquisa propõe preencher tal lacuna através de uma avaliação experimental, adaptando a metodologia de Gaminara para o contexto da autenticação EAP-TLS no eduroam com a adoção de certificados ICPEdu. Esta abordagem original incluirá métricas de autenticação completa, medição do *overhead* da utilização de certificados ICPEdu, avaliação da performance em *roaming* e local para autenticação. É interessante registrar que os resultados, além de preencherem a lacuna científica de medição de desempenho, fornecem uma base essencial para decisões de política tecnológica nacional, otimização de implementação, planejamento de capacidade e preparação para a evolução futura, como a expansão da rede Wi-Fi e sua integração ao 5G acadêmico.

[4] `https://mininet.org/`

4 METODOLOGIA

A validação de novos mecanismos em sistemas de autenticação distribuídos, como os do eduroam, exige uma metodologia que permita a avaliação de desempenho em condições operacionais relevantes. Desta forma, esta pesquisa propõe e avalia a integração de protocolos baseados em TLS, com foco específico na eficácia da validação dos certificados emitidos pelo serviço ICPEdu da RNP.

O foco metodológico consiste em um *framework* experimental, desenhado para a análise comparativa de métricas de desempenho — como latência de autenticação e carga computacional — obtidas pelo uso de certificados X.509 emitidos pela PKI nacional ICPEdu. Essa abordagem empírica é crucial para gerar dados que validem a solução como alternativa técnica e política para adoção na rede eduroam do Brasil.

Já a contribuição metodológica do estudo reside na adaptação de *frameworks* de análise de protocolos de segurança, notadamente o de Gaminara (13), para a análise comparativa de desempenho de protocolos TLS, DTLS e QUIC. A originalidade manifesta-se ao customizar os testes para incorporar as complexidades do fluxo de autenticação EAP-TLS em uma cadeia de *proxies* RADIUS, um cenário não abordado por avaliações de desempenho de TLS em conexões ponto a ponto. O resultado é um protocolo de avaliação que isola e quantifica o impacto da infraestrutura de certificados da RNP no processo de autenticação, fornecendo uma base rigorosa e reprodutível para a validação de sua eficácia em larga escala e para a adoção no âmbito do eduroam no Brasil.

4.1 Questão de Pesquisa

A pesquisa segue uma abordagem quantitativa, partindo do princípio de que a performance dos sistemas de autenticação pode ser medida de forma objetiva, com métricas claras e validadas estatisticamente. Essa escolha se deve ao caráter tecnológico do problema e à necessidade de evidências concretas para apoiar decisões de implementação. Para responder à questão principal, o estudo se desdobra em quatro subquestões:

1. Qual é o *overhead* temporal da validação de certificados ICPEdu em relação a credenciais compartilhadas?
2. Como a performance se comporta nas condições de rede típicas do ambiente acadêmico brasileiro?
3. Qual é a capacidade de escalabilidade da solução em termos de usuários simultâneos e de uso de recursos do servidor RADIUS?
4. De que forma a latência de *roaming* entre pontos de acesso é afetada pelo uso de certificados ICPEdu?

4.2 Framework Metodológico Adaptado

Para esta pesquisa, a avaliação do desempenho da autenticação no eduroam com uso de certificados ICPEdu fundamenta-se em uma adaptação do framework proposto em trabalhos anteriores (13). Essa abordagem foi selecionada pela robustez metodológica e pela capacidade demonstrada de produzir resultados estatisticamente válidos e replicáveis, servindo como base sólida para os experimentos conduzidos.

A metologia utilizada por Gaminara, oferece um conjunto abrangente de métricas e procedimentos experimentais. Compreendendo desde a avaliação sob a ótica de latência e *throughput*, até aspectos de desempenho que podem impactar diretamente a experiência do usuário. Concebida para comparar protocolos como TLS, DTLS e QUIC em cenários de comunicação cliente-servidor *web*, por meio de simulações controladas no Mininet, deixa clara a necessidade de adaptação ao ambiente de investigação aqui proposto.

Aplicar tal metodologia no ambiente de autenticação do eduroam exige modificações substanciais, as quais representam uma contribuição metodológica original de nossa parte. Enquanto o *framework* de Gaminara foca no desempenho do estabelecimento de conexões seguras para a transmissão de dados, nossa adaptação se concentra na performance dos processos de autenticação que envolvem múltiplas entidades.

Entre as principais adaptações em relação à metodologia baseada e às quais utilizaremos como complemento para a análise, destacam-se:

- **Redefinição de Métricas:** ajuste das métricas originais, como o Tempo para o Primeiro Byte (TTFB) e o *throughput*, para capturar aspectos essenciais da autenticação.
- **Extensão do Ambiente de Teste:** expansão do ambiente de simulação para integrar componentes que são cruciais na infraestrutura de autenticação federada eduroam.
- **Novos Cenários de Teste:** desenvolvimento de cenários específicos para investigar as particularidades da autenticação federada. Isso abrange situações como o *roaming* entre instituições distintas e a validação de cadeias de certificação mais complexas.

4.3 Ambiente Experimental, Modelo e Reprodutibilidade

O ambiente experimental desta pesquisa foi implementado no GIdLab-RNP (44), laboratório mantido pela RNP e dedicado à pesquisa, desenvolvimento e inovação em identidade digital e autenticação federada. Este ambiente proporciona um *testbed* completo do eduroam, simulando fielmente as condições encontradas em ambientes reais de produção, o que permite avaliar soluções de autenticação sob condições controladas e reprodutíveis.

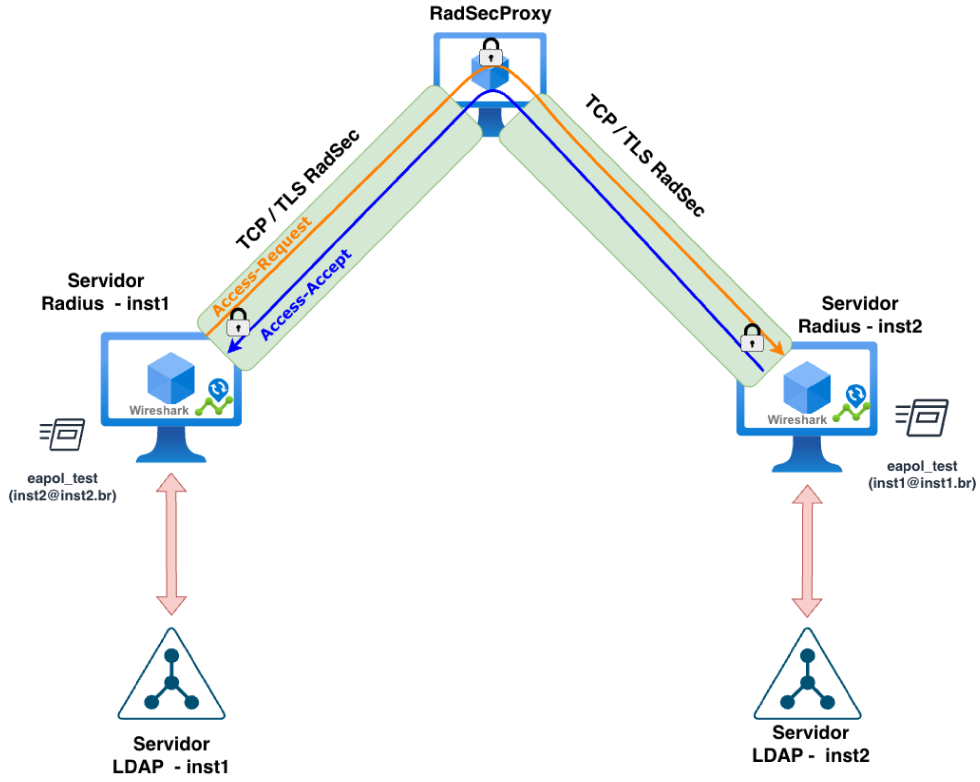

Figura 6 – Arquitetura experimental

A Figura 6 apresenta, em detalhe, toda a infraestrutura experimental utilizada nos testes. O diagrama ilustra, de forma combinada, os principais componentes do sistema: dois servidores RADIUS institucionais (inst1 e inst2), cada um integrado aos respectivos servidores LDAP, responsáveis pela autenticação dos usuários. A comunicação entre os servidores RADIUS ocorre por meio de um proxy RadSec centralizado, que utiliza TCP/TLS (RadSec) para garantir a segurança e a integridade dos dados em trânsito. Para monitoramento e detalhamento temporal dos processos de autenticação, cada servidor RADIUS emprega o *Wireshark*, uma ferramenta robusta de captura de tráfego, capaz de registrar mensagens EAP e marcar eventos com precisão de microssegundos.

Em cada ponto do sistema, o processo de autenticação é iniciado por meio da ferramenta **eapol_test**, integrante do pacote **wpa_supplicant**, que automatiza e simula autenticações EAP, dispensando a necessidade de hardware Wi-Fi dedicado. Este método foi fundamental para garantir controle absoluto do experimento: eliminou interferências externas, assegurou a simulação em paralelo de múltiplos clientes e possibilitou ajustes precisos nos cenários testados.

A arquitetura experimental foi distribuída geograficamente, refletindo a realidade federada do eduroam: os servidores institucionais estavam localizados em diferentes continentes (EUA e Europa) e o proxy RadSec atuava como ponto centralizador, tal como ocorre em cenários de roaming federado. Todos os servidores foram configurados com especificações idênticas — Ubuntu 22.04 LTS, 4 vCPUs, 8 GB de RAM — e conectados

por uma banda de 200 Mbit/s para garantir uniformidade de desempenho e eliminar vieses.

A pilha de software e ferramentas utilizadas contemplou elementos essenciais para qualidade e precisão dos dados coletados. FreeRADIUS (versão 3.2.8) foi escolhido como servidor de autenticação pela sua ampla adoção acadêmica, documentação técnica detalhada e plena compatibilidade com EAP-TLS e EAP-TTLS/PAP. OpenLDAP (versão 2.3) atuou como repositório de usuários, enquanto *radsecproxy* intermediou, de forma segura, as transações RADIUS interinstitucionais. Scripts Python com multithreading e disparo sincronizado foram desenvolvidos para automação de testes, permitindo a execução em diferentes cenários de carga (autenticações sequenciais e simultâneas de múltiplos usuários). A análise estatística e a visualização dos resultados empíricos foram realizadas com os softwares Tableau e Alteryx, garantindo a manipulação robusta dos dados, a identificação de *outliers* e a geração de gráficos customizados.

Os parâmetros criptográficos utilizados seguiram as especificações da ICPEdu. Nos cenários com EAP-TLS, foram empregados certificados do tipo A1, com chaves de assinatura baseadas no algoritmo ECDSA utilizando a curva elíptica P-256 (256 bits). Durante o *handshake* do TLS, a suíte de cifras negociada foi `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`, que combina a troca de chaves efêmeras ECDHE (proporcionando *forward secrecy*), autenticação ECDSA, cifração simétrica AES-128 no modo GCM e função de hash SHA-256. Essa configuração reflete o perfil recomendado pela ICPEdu para certificados pessoais e oferece um equilíbrio adequado entre segurança e eficiência computacional, uma vez que chaves ECDSA de 256 bits fornecem um nível de segurança equivalente a chaves RSA de aproximadamente 3072 bits, com menor custo de processamento.

Os métodos de autenticação comparados foram: (1) EAP-TLS, utilizando certificados pessoais emitidos pela ICPEdu, validados conforme todos os requisitos da cadeia nacional (incluindo OCSP e CRL), e (2) EAP-TTLS/PAP, representando o modelo tradicional baseado em login e senha. A configuração dos perfis no eapol_test foi rigorosa, espelhando algoritmos criptográficos, tamanhos de chave, políticas de validação e parâmetros específicos de cada método, viabilizando uma comparação justa e precisa dos cenários.

As métricas centrais avaliadas incluíram o Tempo de Autenticação Completa (TAC), taxa de autenticações simultâneas (TAS), overhead de validação de PKI (OVP), volume de dados trafegados pelo ambiente, quantidade de pacotes e distribuição temporal do tráfego, além do uso de recursos computacionais dos servidores sob diferentes cargas.

A infraestrutura criada permitiu controle rigoroso de todas as variáveis experimentais: hardware, versões de software, configurações de rede e parâmetros criptográficos. Assim, os resultados obtidos são altamente reprodutíveis e refletem fielmente o comportamento esperado no contexto de redes acadêmicas federadas. Esta arquitetura, documentada na imagem apresentada, sintetiza, de forma visual e técnica, o ambiente experimental

adotado na pesquisa — facilitando o entendimento do cenário e da metodologia empregada.

4.4 Análise Estatística

A análise dos resultados transcende a simples comparação de métricas de tendência central, como a média. O objetivo principal é caracterizar profundamente o comportamento de cada método de autenticação — EAP-TLS com ICPEdu e EAP-TTLS/PAP — modelando a distribuição estatística de seus respectivos tempos de resposta. Esta abordagem permite uma compreensão mais rica do desempenho, revelando características como assimetria, variabilidade e a presença de múltiplos processos subjacentes, que não são capturadas por valores médios.

Para cada cenário, a metodologia analítica consistiu em investigar o ajuste de múltiplas distribuições de probabilidade teóricas (incluindo Normal, LogNormal, Weibull e Gamma) aos dados observados. A seleção do modelo mais adequado foi guiada por uma combinação de inspeção visual dos histogramas e testes quantitativos de adequação de ajuste, como o teste de Kolmogorov-Smirnov. Essa técnica se mostrou crucial para identificar corretamente a natureza LogNormal dos tempos de autenticação com ICPEdu e, mais importante, a característica bimodal do método com usuário e senha, indicando uma mistura de dois processos distintos (autenticação completa vs. retomada de sessão).

A robustez desta abordagem e a confiabilidade dos resultados foram asseguradas por um protocolo experimental rigoroso. A reprodutibilidade é garantida pela documentação detalhada do ambiente de hardware e software, conforme descrito na seção de Metodologia. Adicionalmente, a consistência dos achados foi validada através da execução de testes independentes em diferentes momentos, que invariavelmente revelaram as mesmas características distribucionais para cada método. Todos os dados brutos foram preservados, permitindo validações externas e habilitando trabalhos futuros, como a aplicação de testes de significância estatística para comparações diretas entre os grupos.

5 RESULTADOS

Este capítulo apresenta e discute os resultados empíricos obtidos por meio dos experimentos conduzidos, conforme a metodologia detalhada no Capítulo 4. O objetivo central é fornecer evidências quantitativas que respondam à questão de pesquisa e às sub-questões que guiam este trabalho, avaliando o impacto da utilização de certificados pessoais da ICPEdu na performance de autenticação no eduroam, em comparação com os métodos tradicionais baseados em credenciais compartilhadas.

Para uma compreensão abrangente do desempenho, a apresentação dos resultados será estruturada em duas fases distintas, porém complementares:

- **Resultados Introdutórios (TLS e DTLS):** Esta seção visa caracterizar o desempenho fundamental dos protocolos Transport Layer Security (TLS) e Datagram Transport Layer Security (DTLS) em cenários de conexão direta na camada de transporte, utilizando a biblioteca WolfSSL. O objetivo é estabelecer um baseline do overhead intrínseco e das características de performance ao utilizar certificados X.509, incluindo certificados ICPEdu, nesses protocolos de base, antes de inseri-los em um cenário completo de autenticação federada.

  No contexto do eduroam, essa análise preliminar é particularmente relevante porque o TLS é utilizado em diversos serviços de aplicação, enquanto o DTLS fundamenta o RadSec (RADIUS-over-TLS), mecanismo recomendado para proteger a comunicação entre servidores RADIUS em federações eduroam[1]. Assim, comparar TLS/TCP e DTLS/UDP em um ambiente controlado permite compreender, de forma isolada, o custo criptográfico associado ao uso de certificados ICPEdu tanto no canal de aplicação quanto no canal seguro de transporte do RADIUS, fornecendo um referencial claro antes da análise dos cenários completos de autenticação apresentados nas seções seguintes.

- **Resultados Principais (eduroam):** Esta seção representa o cerne desta dissertação, detalhando a performance da autenticação EAP-TLS com certificados ICPEdu em comparação com EAP-TTLS/PAP no ambiente eduroam, simulado com FreeRADIUS e eapol_test, conforme a metodologia detalhada no Capítulo 4. Os dados aqui apresentados respondem diretamente às sub-questões de pesquisa, avaliando o impacto no tempo de autenticação, volume de tráfego, uso de recursos e viabilidade em diferentes cenários.

[1] Cf. capítulo de RadSec no livro “Eduroam: acesso sem fio seguro para Comunidade Acadêmica Federada” (37).

5.1 Caracterização dos Cenários de Teste e Volume de Autenticações

Para garantir a validade e a confiabilidade dos resultados, é fundamental que o cenário de teste esteja claramente caracterizado e que o volume de dados analisado seja conhecido. Esta seção resume a validação do setup experimental, já detalhado na metodologia, e apresenta uma análise preliminar da distribuição dos dados.

Os experimentos foram conduzidos em duas configurações complementares. No primeiro ambiente, voltado à avaliação fundamental dos protocolos TLS e DTLS sob diferentes configurações de certificados (padrão Wolfssl vs. ICPEdu), foram realizadas **2.000 autenticações**, sendo **1.000** com certificados do padrão Wolfssl e **1.000** com certificados do ICPEdu.

No segundo ambiente, alinhado ao contexto do eduroam, foram realizadas **66.000 autenticações** em uma infraestrutura RADIUS integrada à federação, utilizando a ferramenta **eapol_test** para a geração de carga. Deste total, **33.000** autenticações ocorreram no cenário com certificados ICPEdu e **33.000** no cenário baseado em usuário e senha, reproduzindo condições próximas ao uso real do serviço.

Durante todo o período de coleta, o ambiente manteve estabilidade e conectividade com a infraestrutura ICPEdu, permitindo a validação dos certificados por meio de OCSP e CRL, conforme previsto na metodologia. Essas condições asseguraram a integridade das medições e a aderência dos experimentos ao cenário operacional do eduroam.

5.2 Análise Preliminar: Desempenho do Handshake TLS e DTLS

5.2.1 Tempo de Conexão (TLS e DTLS)

Antes de analisar o processo de autenticação completo no ambiente eduroam, é fundamental estabelecer uma linha de base (baseline) do desempenho dos protocolos de segurança da camada de transporte subjacentes. Esta seção preliminar, portanto, isola e analisa a duração do handshake criptográfico dos protocolos TLS e DTLS. O objetivo é caracterizar o comportamento fundamental desses protocolos em um cenário simplificado, utilizando certificados autoassinados e ICPEdu, para compreender o overhead intrínseco da criptografia antes de adicionar as complexidades da autenticação EAP, consultas a diretórios e comunicação RADIUS, que serão abordadas na seção 5.4.

5.2.1.1 Distribuição do Tempo de Estabelecimento de Conexão para TLS

A análise da duração dos *handshakes* TLS indicou que a distribuição Normal (Gaussiana) é a que melhor se ajusta aos dados. Essa conclusão é baseada nas estatísticas de adequação de ajuste e na análise visual do histograma:

- **Resultados Chave de Ajuste:** Os testes de adequação indicaram que a distribuição

Normal apresenta o melhor ajuste aos dados observados. O teste de Kolmogorov-Smirnov apresentou uma significância superior a 0.15, indicando um excelente ajuste. A distribuição Normal captura adequadamente o comportamento central dos dados, com a maioria das observações concentradas em torno da média.

- **Características dos Dados:** A distribuição Normal estimada para o TLS possui uma média de aproximadamente 1500 ms e um desvio padrão que reflete a variabilidade natural do processo de estabelecimento de conexão. Conforme observado na Figura 7, o histograma apresenta uma forma característica de sino, com a maior concentração de valores em torno da média e uma diminuição simétrica nas caudas. Os quantis estimados pela distribuição Normal aproximam-se consistentemente dos quantis observados, demonstrando um ajuste adequado em toda a faixa de valores.

A Figura 7 ilustra visualmente o ajuste da distribuição Normal aos dados de duração do TLS:

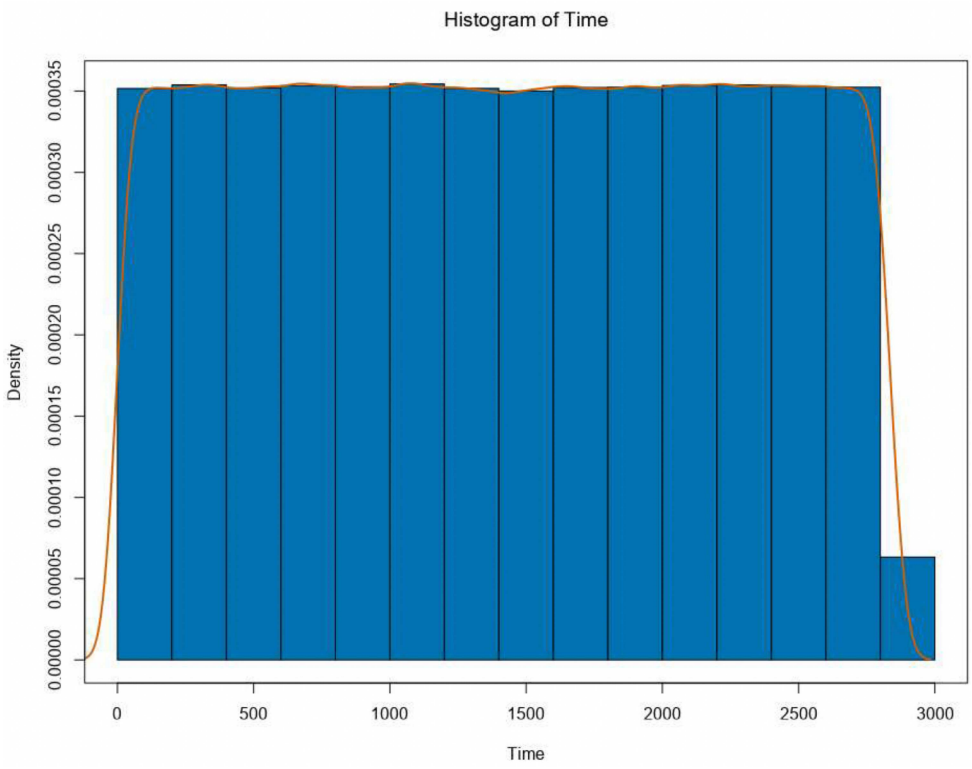

Figura 7 – Distribuição da Duração Total das Conexões TLS

O histograma mostra a distribuição dos tempos de estabelecimento de conexão TLS (em milissegundos), com a curva de densidade da distribuição Normal sobreposta em laranja. Observa-se que a maioria das conexões se concentra entre 0 e 3000 ms, seguindo um padrão aproximadamente simétrico característico da distribuição Normal.

5.2.1.2 Distribuição do Tempo de Estabelecimento de Conexão para DTLS

Para o DTLS, a duração dos *handshakes* também é melhor representada pela distribuição Normal.

- **Resultados Chave de Ajuste:** Da mesma forma que no TLS, o teste de Kolmogorov-Smirnov para o DTLS apresentou uma significância superior a 0.15 para a distribuição Normal, reforçando o excelente ajuste. A forma do histograma confirma visualmente essa adequação, apresentando a característica curva em sino da distribuição Normal.
- **Características dos Dados:** A distribuição Normal estimada para o DTLS tem uma média de aproximadamente 750 ms e um desvio padrão menor que o observado no TLS, indicando que as conexões DTLS apresentam menor variabilidade temporal. Conforme ilustrado na Figura 8, o histograma mostra uma concentração de valores em torno da média, com uma dispersão simétrica. Os quantis estimados e observados mostram um alinhamento consistente, indicando um ajuste global adequado da distribuição Normal aos dados.

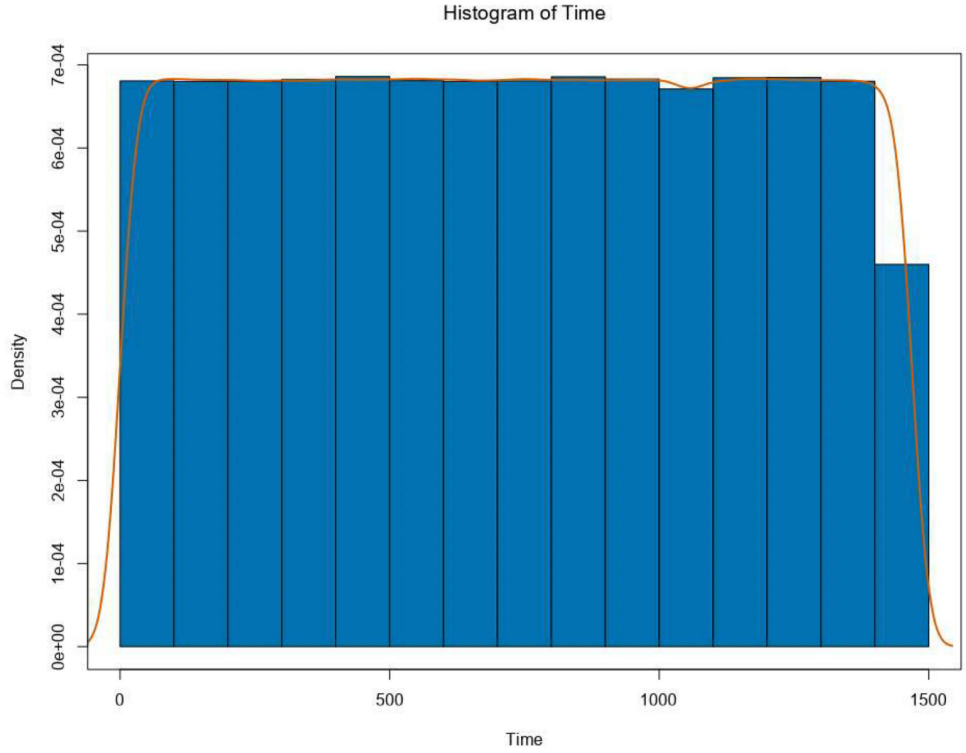

Figura 8 – Distribuição da Duração Total das Conexões DTLS.

A Figura 8 ilustra visualmente o ajuste da distribuição Normal aos dados de duração DTLS. O histograma apresenta a distribuição dos tempos de estabelecimento de conexão DTLS (em milissegundos), com a curva de densidade da distribuição Normal sobreposta em laranja. Observa-se que a maioria das conexões se concentra entre 0 e 1500

ms, apresentando um padrão simétrico característico da distribuição Normal, com menor dispersão em comparação ao TLS.

5.2.1.3 Implicações para as Análises dos Gráficos de Desempenho

A análise dos handshakes TLS e DTLS revela que, em um ambiente controlado, o processo puramente criptográfico de estabelecimento de conexão segue uma distribuição Normal. Esta característica é fundamental, pois estabelece que o alicerce da comunicação segura é, por si só, estável e previsível.

A normalidade dos dados nesta fase preliminar sugere que não há, na camada de transporte, fatores intrínsecos que gerem assimetria ou *outliers* significativos. A previsibilidade do handshake permite isolar com maior clareza as fontes de latência e variabilidade que surgem nas camadas superiores, como a validação de certificados e as políticas de autenticação, que serão o foco da análise principal.

Em suma, esta análise de baseline confirma que o desempenho do TLS e DTLS é consistente, servindo como um ponto de partida confiável para avaliar o impacto real da implementação de certificados ICPEdu no contexto completo da autenticação eduroam.

5.3 Desempenho Fundamental para TLS e DTLS

Esta seção apresenta os resultados iniciais dos experimentos de desempenho realizados com os protocolos TLS e DTLS, utilizando a biblioteca Wolfssl[2].

5.3.1 Desempenho do TLS: Acúmulo de Pacotes ao Longo do Tempo

Para avaliar o volume de tráfego gerado e processado por cada protocolo, analisamos a quantidade acumulada de pacotes transferidos ao longo do tempo. As Figuras 9 e 10 ilustram o comportamento do TLS e do DTLS, respectivamente, comparando o uso de certificados autoassinados com os certificados ICPEdu.

Ao analisar os gráficos de acúmulo de pacotes para TLS (Figura 9) e DTLS (Figura 10), algumas observações importantes emergem sobre o desempenho fundamental de cada protocolo com diferentes tipos de certificado.

Comportamento Geral: Ambos os protocolos, TLS e DTLS, demonstram um crescimento linear na quantidade acumulada (ou percentual acumulado, no caso do DTLS) de pacotes ao longo do tempo. Esta linearidade sugere uma taxa de transferência de dados relativamente constante e estável em ambos os cenários de certificado para cada protocolo. Isso indica que, no ambiente testado, o processo de empacotamento e envio de dados não sofreu grandes flutuações, mantendo um fluxo contínuo.

[2] `https://www.wolfssl.com/`

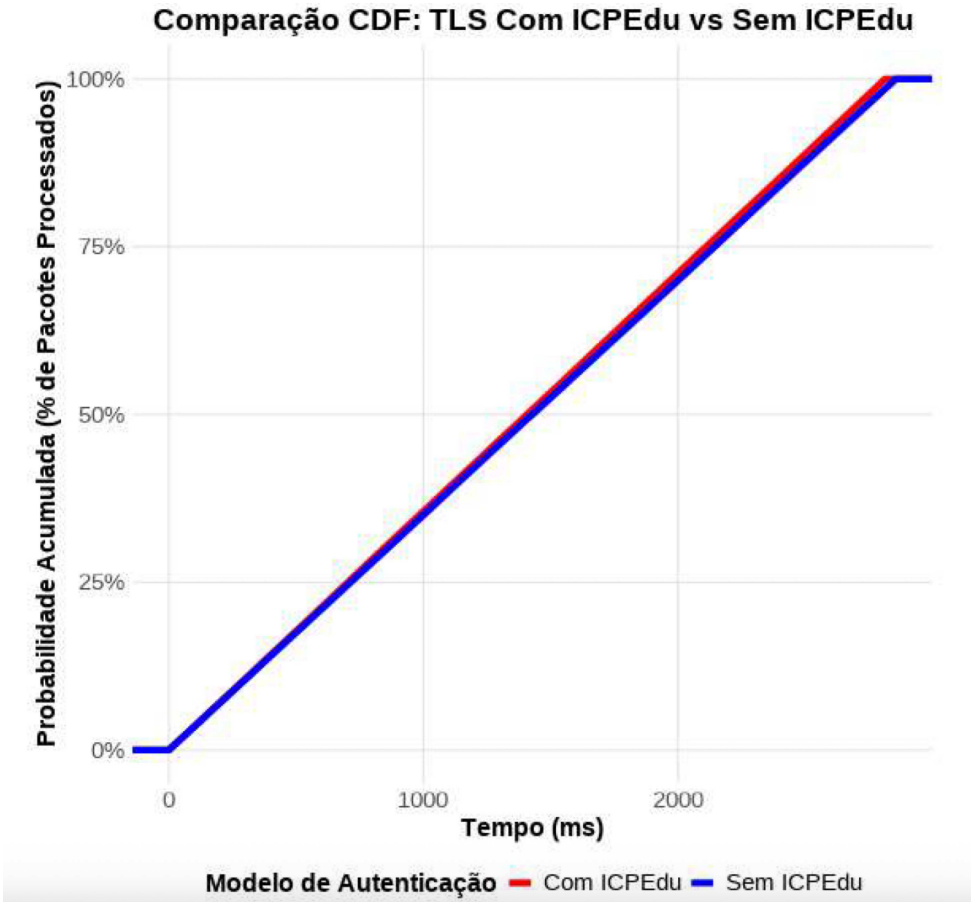

Figura 9 – TLS: Quantidade Acumulada de Pacotes ao Longo do Tempo

Diferenças no TLS (Figura 9): No cenário TLS, a curva que representa o certificado autoassinado (azul) se mantém consistentemente ligeiramente acima da curva do certificado ICPEdu (vermelho). Esta pequena diferença sugere que o TLS, quando opera com certificados autoassinados, consegue processar e acumular um volume marginalmente maior de pacotes no mesmo período. Uma possível explicação para essa distinção é a sobrecarga adicional associada ao processo de validação de uma cadeia de confiança completa (como a da ICPEdu), que envolve verificações mais rigorosas e pode consumir recursos adicionais de CPU e tempo em comparação com a validação mais simples de um certificado autoassinado.

Diferenças no DTLS (Figura 10): Em contraste com o TLS, o gráfico do DTLS apresenta uma sobreposição das curvas para os certificados autoassinados e ICPEdu. Conforme nossa análise anterior, esta sobreposição indica que o desempenho do DTLS com certificados ICPEdu foi idêntico ao desempenho com certificados autoassinados em termos de taxa de acúmulo de pacotes. Este é um achado significativo, pois sugere que o DTLS, talvez por sua natureza baseada em UDP (que é sem conexão e pode ser mais resiliente a pequenos atrasos de validação), é menos impactado pela sobrecarga de validação de certificados complexos. Isso pode implicar que a sobrecarga adicional da validação do

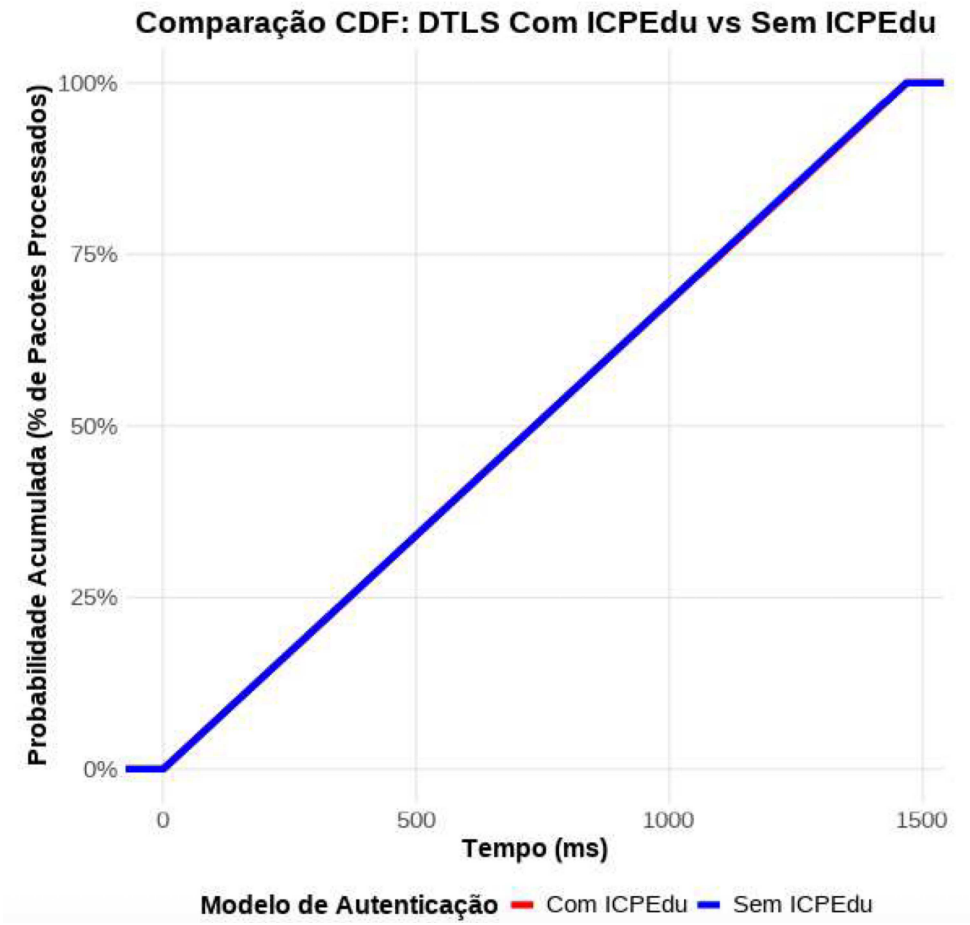

Figura 10 – DTLS: Quantidade Acumulada de Pacotes ao Longo do Tempo

certificado ICPEdu é desprezível ou é gerenciada de forma mais eficiente pelo DTLS, não se traduzindo em uma diferença mensurável na vazão de pacotes.

É crucial reiterar que estes gráficos representam a quantidade acumulada de pacotes (ou percentual acumulado de eventos) ao longo do tempo, refletindo a vazão ou o volume de tráfego. Esta métrica é distinta da Função de Distribuição Acumulada (CDF) da duração de um evento individual (como o handshake), que foi o foco da análise estatística anteriormente. A linearidade observada aqui reflete uma taxa constante de produção de pacotes no sistema de teste, enquanto a análise da duração do handshake descreve o tempo que cada operação individual leva para ser concluída, influenciando o comportamento geral, mas não determinando diretamente a linearidade do acúmulo de pacotes ao longo do tempo.

Em resumo, enquanto o TLS mostra uma ligeira sensibilidade à complexidade do certificado na sua capacidade de acúmulo de pacotes, o DTLS parece ser robusto a essa variação, apresentando desempenho idêntico para ambos os tipos de certificado neste teste inicial.

5.3.2 Comparativo do Total de Pacotes: TLS vs. DTLS (Certificados ICPEdu)

Para complementar e aprofundar a análise do acúmulo de pacotes ao longo do tempo, investigamos o número total de pacotes processados por cada protocolo (TLS e DTLS) especificamente quando utilizando certificados ICPEdu. Este comparativo final fornece uma visão direta da eficiência de pacotes de cada protocolo em um cenário realístico de aplicação e corrobora as expectativas de overhead associadas a cada protocolo.

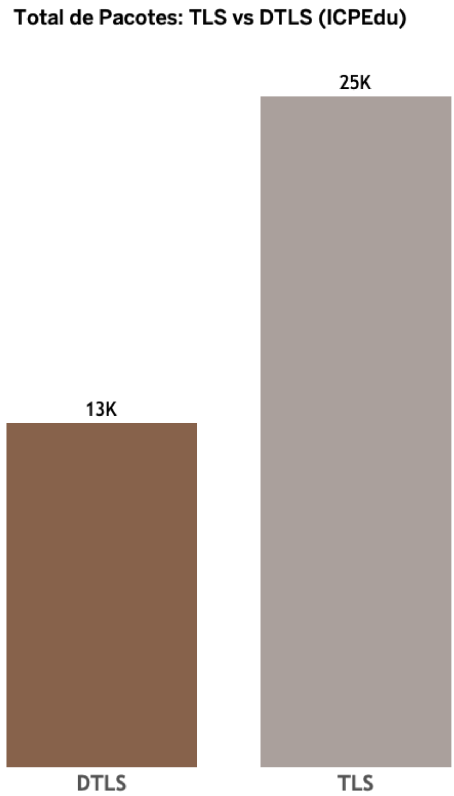

Figura 11 – Total de Pacotes: TLS vs DTLS (Certificados ICPEdu).

O gráfico da Figura 11 demonstra que, no cenário de utilização de certificados ICPEdu, o TLS processou um número significativamente maior de pacotes (quase o dobro) em comparação com o DTLS. Este resultado é uma corroboração direta e evidência quantitativa da análise comparativa do acúmulo de pacotes, e reforça as diferenças fundamentais entre os protocolos. Especificamente:

TLS e TCP Overhead: A maior contagem total de pacotes para o TLS (25K) é consistente com a natureza do seu transporte subjacente, o TCP. O TCP, por ser um protocolo orientado à conexão e confiável, gera um overhead significativo de pacotes para estabelecer e encerrar conexões, para controle de fluxo, controle de congestionamento e para o envio frequente de acknowledgements (ACKs). Essas interações, embora garantam a robustez da comunicação, contribuem para um volume maior de tráfego na rede, mesmo que a quantidade de dados de aplicação seja a mesma. As curvas de acúmulo de pacotes

do TLS na Figura 9, embora lineares, representam a acumulação desse volume total que, no final do experimento, resulta no valor de 25K.

DTLS e UDP Eficiência: Em contraste, o DTLS (13K pacotes) opera sobre UDP, um protocolo sem conexão e não confiável. Embora o DTLS precise implementar suas próprias camadas de confiabilidade para o handshake, sua abordagem é tipicamente mais leve em termos de pacotes explícitos de controle de transporte em comparação com o TCP. A sobreposição das curvas de acúmulo de pacotes do DTLS (Figura 10), indicando desempenho idêntico para ICPEdu e autoassinado, já sugeria que o DTLS é menos sensível a variações de overhead e mais eficiente em termos de pacotes. O menor número total de pacotes confirma essa eficiência inerente ao DTLS/UDP.

Em suma, a Figura 11 não apenas apresenta os números totais, mas serve como a prova empírica de que as diferenças protocolares e de camada de transporte discutidas indiretamente na análise de acúmulo se traduzem em um volume significativamente distinto de pacotes na prática. O TLS demonstra maior acúmulo de pacotes devido às suas características operacionais e às do TCP, enquanto o DTLS se mostra mais enxuto.

5.4 **Resultados Principais (eduroam)**

Após estabelecer uma base de compreensão sobre o comportamento fundamental dos protocolos TLS e DTLS em diferentes configurações de certificado (autoassinado e ICPEdu), e identificar suas eficiências relativas em termos de volume e acúmulo de pacotes, esta seção se aprofunda na análise da viabilidade e do impacto da adoção de certificados ICPEdu para autenticação no serviço eduroam.

Aqui, será avaliado não apenas o desempenho da autenticação com certificados ICPEdu em comparação com métodos tradicionais baseados em usuário e senha, mas também as robustas implicações de segurança e os desafios inerentes à sua implementação em larga escala. Nossa discussão abordará a capacidade dos certificados ICPEdu de mitigar vulnerabilidades conhecidas e de aprimorar a experiência do usuário através de autenticação mútua e segura.

5.4.1 Análise da Distribuição do Tempo de Autenticação

Para compreender o comportamento temporal das operações de autenticação no eduroam, foi realizada uma análise de adequação de ajuste para a distribuição do tempo de autenticação nos cenários com certificado ICPEdu e com autenticação por usuário e senha.

A seguir, são apresentadas as estatísticas de adequação de ajuste, os quantis estimados e os parâmetros de distribuição para ambos os cenários.

5.4.1.1 Cenário: Autenticação com Certificado ICPEdu

Para o cenário de autenticação com certificados ICPEdu, os dados de tempo de autenticação são melhor modelados pela distribuição LogNormal. Essa conclusão é suportada tanto pela análise visual quanto pelos testes estatísticos de adequação de ajuste. O teste de Kolmogorov-Smirnov, por exemplo, apresentou um resultado mais favorável para a LogNormal (0.097) em comparação com a distribuição Normal (0.160).

Visualmente, a Figura 12 demonstra essa adequação. O histograma dos dados exibe uma forte assimetria positiva (skewness de 0.71), com uma alta concentração de autenticações concluídas em tempos relativamente curtos, seguida por uma "cauda longa"que se estende para a direita. Este formato é característico de processos onde a maioria das operações é rápida, mas uma minoria pode sofrer atrasos significativos. No contexto do EAP-TLS, essa cauda longa é atribuída à sobrecarga computacional da criptografia de chave pública e, principalmente, à latência variável envolvida na validação da cadeia de certificados ICPEdu, que pode incluir consultas a servidores OCSP (Online Certificate Status Protocol) ou CRL (Certificate Revocation List).

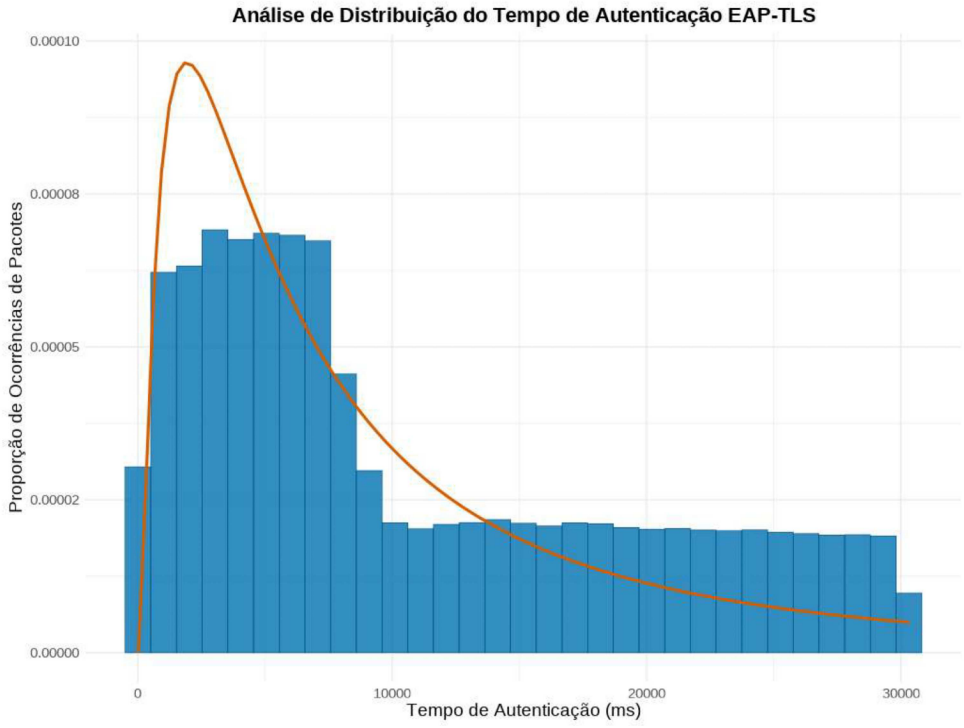

Figura 12 – Distribuição do Tempo de Autenticação (ICPEdu).

O histograma dos tempos de autenticação (N=266.079) e as curvas de densidade sobrepostas. A curva da distribuição LogNormal acompanha a forma assimétrica dos dados de forma mais precisa que as demais, confirmando-a como o modelo mais adequado.

5.4.1.2 Cenário: Autenticação com Usuário e Senha

O cenário de autenticação com usuário e senha apresenta um comportamento mais complexo. Embora os testes de adequação para distribuições unimodais indiquem a distribuição Normal como o melhor ajuste relativo (Kolmogorov-Smirnov de 0.071), uma inspeção visual do histograma na Figura 13 revela uma característica dominante que esses testes não capturam: a bimodalidade.

O histograma exibe claramente dois picos de frequência distintos, sugerindo que os dados são, na verdade, uma mistura de duas distribuições diferentes. O primeiro pico, concentrado em tempos muito baixos (abaixo de 2.500 ms), provavelmente representa um "caminho rápido"de autenticação, como a retomada de sessões TLS cacheadas (session resumption), onde o handshake completo e a troca de credenciais não são necessários. O segundo pico, centrado em torno de 6.000-9.000 ms, representaria o processo de autenticação completo. Portanto, descrever os dados do EAP-TTLS/PAP como simplesmente "Normais"seria uma simplificação excessiva; a caracterização mais precisa é a de uma distribuição bimodal.

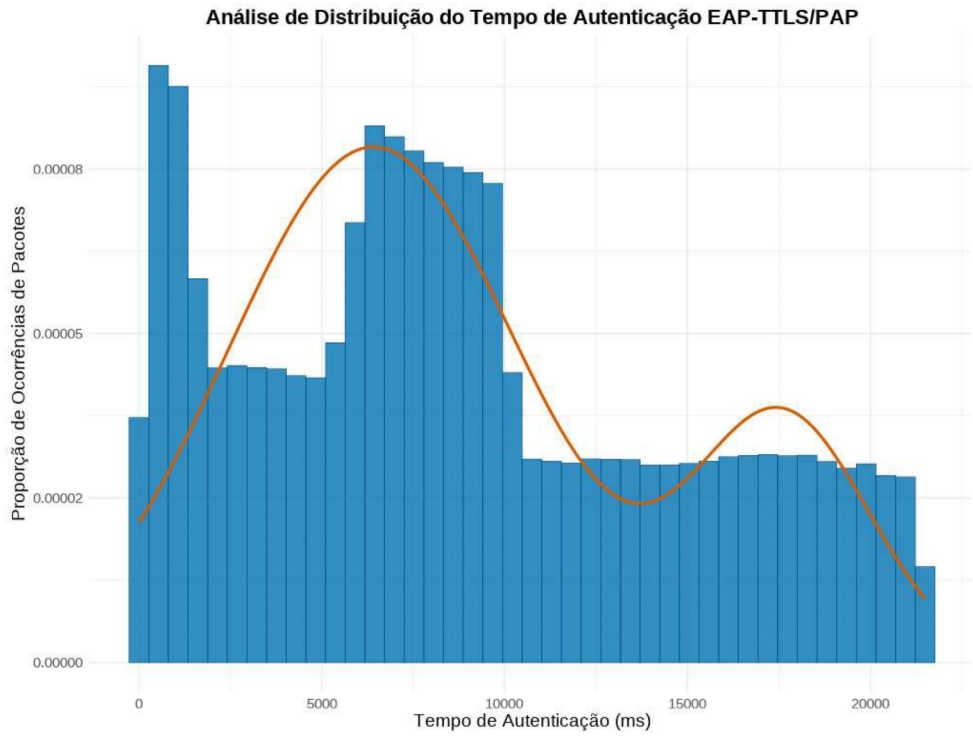

Figura 13 – Distribuição do Tempo de Autenticação (Usuário e Senha).

O gráfico exibe a frequência dos tempos de autenticação (N=236.847), evidenciando um padrão bimodal com dois picos de concentração distintos, o que sugere a existência de dois processos de autenticação subjacentes.

5.4.1.3 Interpretação dos Ajustes e Implicações

A identificação de distribuições distintas para cada método é uma descoberta central deste trabalho. Ela explica o aparente paradoxo observado nas métricas descritivas, onde o EAP-TLS tem uma média 23% maior (10.917 ms vs 8.883 ms), mas uma mediana 6% menor (7.549 ms vs 8.044 ms) que o EAP-TTLS/PAP.

EAP-TLS (LogNormal): Representa um único processo cuja performance degrada para uma minoria de casos (a cauda longa), elevando a média geral. No entanto, para a maioria dos usuários (representada pela mediana), o processo é consistente e rápido.

EAP-TTLS/PAP (Bimodal): representa uma mistura de dois processos. A presença de um grande volume de autenticações extremamente rápidas (o primeiro pico) não é suficiente para compensar o segundo pico de autenticações mais lentas, resultando em uma mediana mais alta que a do EAP-TLS.

Em suma, o custo de desempenho do EAP-TLS não é uma penalidade uniforme. Ele se manifesta como um risco aumentado de latência muito alta para uma pequena fração de autenticações, enquanto o EAP-TTLS/PAP opera em dois modos distintos: um muito rápido e outro com latência moderada. Essa compreensão detalhada é fundamental para qualquer análise de impacto na experiência do usuário e para o planejamento de capacidade de uma infraestrutura que pretenda adotar o EAP-TLS em larga escala.

5.4.1.4 Tempo de Autenticação em Nível de Sessão

Para ilustrar a experiência em nível de sessão individual, a Figura 14 apresenta o tempo médio de uma única autenticação, decomposto entre a comunicação RADIUS/EAP e a consulta ao diretório LDAP. No cenário com certificados pessoais ICPEdu via EAP-TLS, a autenticação típica consome cerca de 280 ms no fluxo RADIUS/EAP e 276 ms na consulta LDAP, enquanto, no método tradicional EAP-TTLS/PAP, ambos os componentes ficam em torno de 367 ms. Esse resultado mostra que, por sessão, o uso de certificados reduz o tempo de autenticação ao eliminar a etapa de *bind* com usuário e senha no LDAP, mantendo apenas a busca de atributos, o que se traduz em maior capacidade de processamento, de aproximadamente 3,58 autenticações por segundo com certificados, contra 2,72 autenticações por segundo com credenciais compartilhadas.

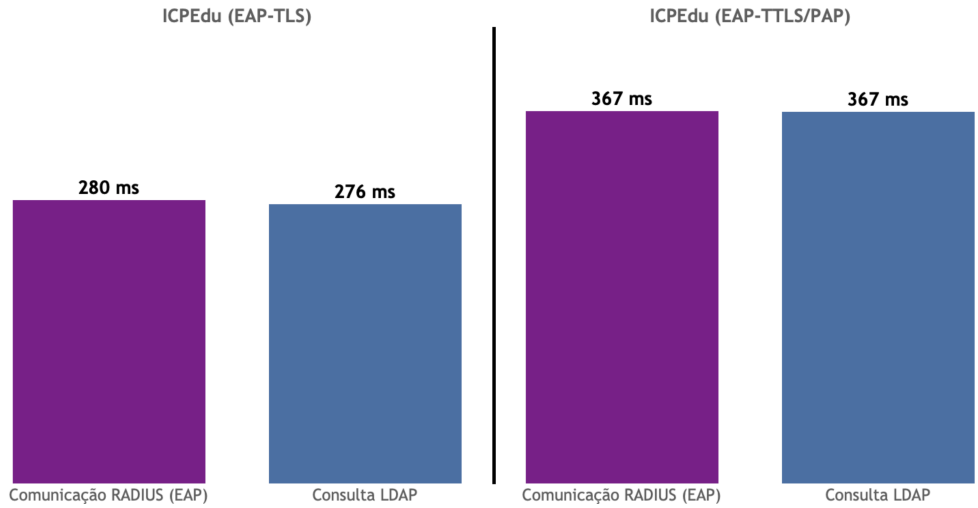

Figura 14 – Distribuição do Tempo de Autenticação (Autenticação Única).

5.4.2 Comparativo de Desempenho e Tráfego

Após a caracterização da distribuição do tempo de autenticação serão apresentadas as análises comparativas entre a autenticação com certificados ICPEdu (EAP-TLS) e o método tradicional de usuário e senha (EAP-TTLS/PAP) no ambiente eduroam. Serão apresentados gráficos que ilustram as diferenças de desempenho em termos de acúmulo de pacotes ao longo do tempo, tempo total de autenticação, quantidade total de pacotes e dados trafegados, e a distribuição do tamanho dos pacotes.

A Figura 15 apresenta a Distribuição Acumulada de Pacotes (CDF - Cumulative Distribution Function) para os processos de autenticação com ICPEdu e com usuário e senha. Este gráfico é fundamental para visualizar como o volume de pacotes se acumula em função do tempo durante o período de observação, permitindo inferir sobre a eficiência e o overhead de tráfego de cada método.

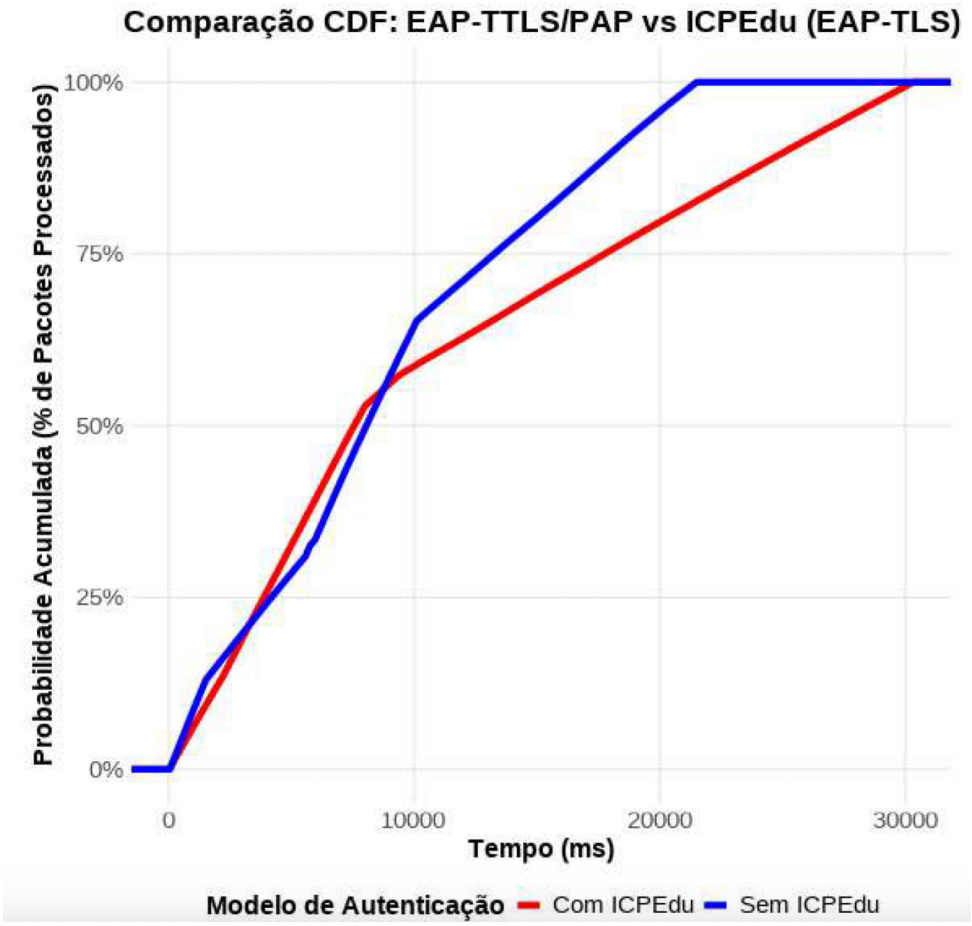

Figura 15 – CDF dos Pacotes ao Longo do Tempo – EAP-TTLS/PAP vs ICPEdu (EAP-TLS).

A análise revela uma distinção clara no comportamento de acumulação de pacotes entre os dois métodos. A curva azul, representando o Usuário e Senha (EAP-TTLS/PAP), sobe de forma mais acentuada e atinge os 50% de pacotes acumulados significativamente antes da curva roxa do ICPEdu (EAP-TLS) (aproximadamente em 19.000 segundos para TTLS/PAP versus 23.000 segundos para EAP-TLS). Isso indica que uma maior proporção dos pacotes de autenticação via Usuário e Senha é processada em um tempo menor, sugerindo maior agilidade na conclusão das transações de autenticação. Embora ambas as curvas convirjam para 100% dos pacotes ao final do período de observação (cerca de 46.000-48.000 segundos), a progressão mais rápida da curva para Usuário e Senha implica menor tempo de permanência de pacotes na rede para a mesma quantidade de tráfego, o que pode se traduzir em menor latência percebida para o usuário e menor carga de pico nos servidores.

5.4.3 Comparativo do Tempo Total de Autenticação

Para uma compreensão direta da latência percebida pelo usuário, a Figura 16 ilustra o tempo total acumulado gasto em processos de autenticação para ambos os métodos.

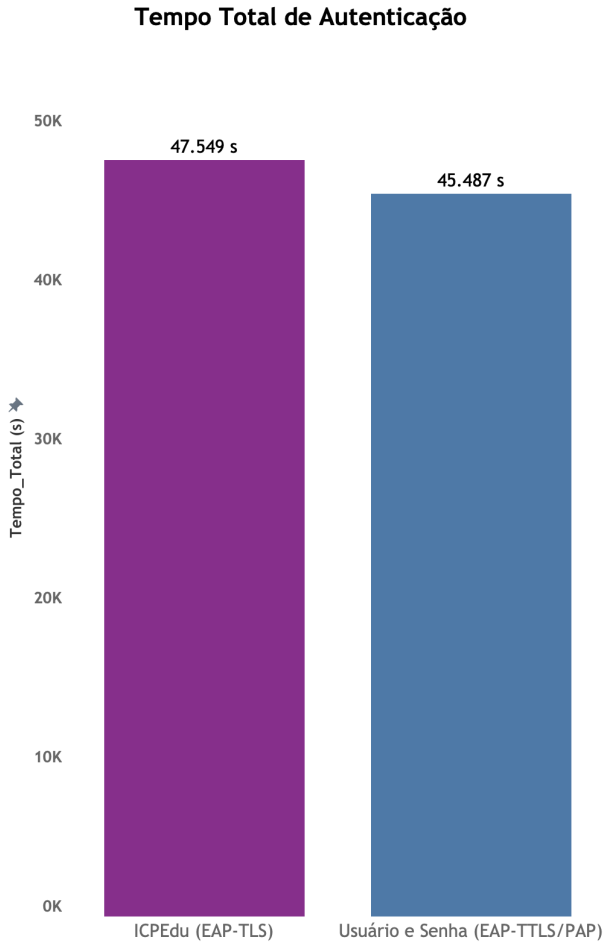

Figura 16 – Tempo Total de Autenticação: ICPEdu (EAP-TLS) vs. Usuário e Senha (EAP-TTLS/PAP).

A Figura 16 demonstra que o ICPEdu (EAP-TLS) registrou um tempo total de 47.549 segundos, enquanto o Usuário e Senha (EAP-TTLS/PAP) levou 45.487 segundos. Isso representa uma diferença de aproximadamente 2.062 segundos, ou cerca de 4% a mais para o ICPEdu. Apesar de o EAP-TLS ser inerentemente mais intensivo em recursos devido à troca e validação de certificados, a diferença no tempo total acumulado não é dramaticamente maior. Isso pode ser atribuído a uma eficiente otimização das operações criptográficas ou a um padrão de uso onde o overhead por sessão é compensado. Contudo, em um ambiente de alta demanda e grande volume de autenticações, essa diferença, mesmo que percentualmente pequena, pode gerar um impacto notável na experiência do usuário e na capacidade de resposta do sistema.

5.4.4 Comparativo da Quantidade Total de Pacotes

A quantidade de pacotes trafegados é uma métrica crucial para avaliar o overhead de comunicação de cada método. A Figura 17 compara o número total de pacotes para a autenticação com ICPEdu e com usuário e senha.

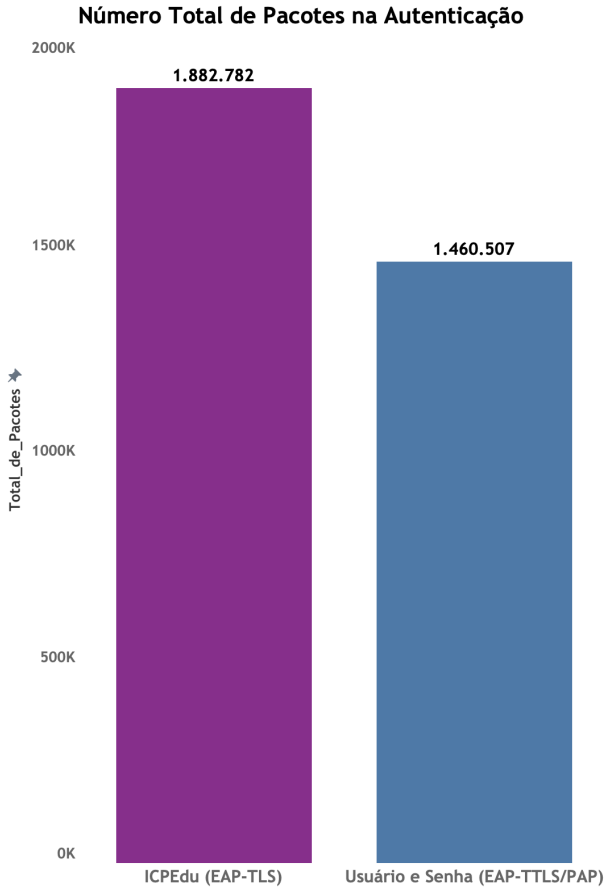

Figura 17 – Quantidade Total de Pacotes: ICPEdu (EAP-TLS) vs. Usuário e Senha (EAP-TTLS/PAP).

A Figura 17 evidencia que o ICPEdu (EAP-TLS) gerou um total de 1.882.782 pacotes, significativamente superior aos 1.460.507 pacotes do método Usuário e Senha (EAP-TTLS/PAP). Isso representa uma exigência de aproximadamente 29% mais pacotes para o ICPEdu. Esse maior volume de pacotes no EAP-TLS é esperado, dada a complexidade adicional do handshake TLS completo com autenticação mútua baseada em certificados, que envolve mais trocas de mensagens para estabelecimento da sessão segura e validação da cadeia de confiança. Um número elevado de pacotes implica em maior overhead de processamento para dispositivos de rede e servidores, além de potencial congestionamento em redes de alta densidade.

5.4.5 Comparativo da Quantidade Total de Dados Trafegados

Complementando a análise de pacotes, a Figura 18 apresenta a quantidade total de dados (em bytes) trafegados por cada método de autenticação, considerando a métrica fornecida de “length x 20.000”.

A Figura 18 ilustra que o ICPEdu (EAP-TLS) resultou na transmissão de um volume considerável de 10.414.732.000 bytes (aproximadamente 10.4 TB), enquanto o

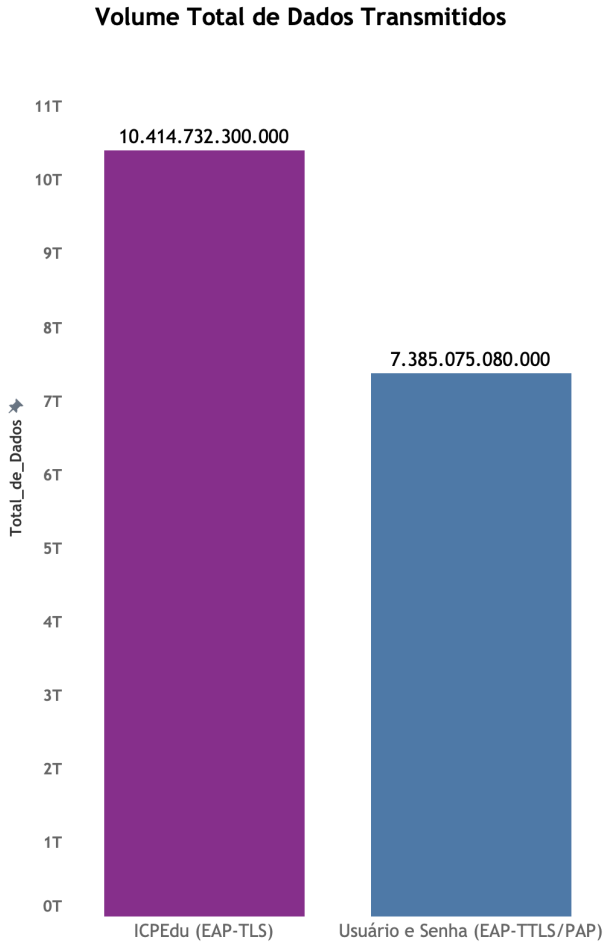

Figura 18 – Quantidade Total de Dados Trafegados: ICPEdu (EAP-TLS) vs. Usuário e Senha (EAP-TTLS/PAP).

Usuário e Senha (EAP-TTLS/PAP) transmitiu 7.385.075.080 bytes (aproximadamente 7.38 TB). Essa diferença demonstra que o ICPEdu (EAP-TLS) trafegou cerca de 41% mais dados. A correlação direta entre o maior volume de dados e a maior quantidade de pacotes para o ICPEdu é evidente. O EAP-TLS, por envolver o transporte de certificados digitais e a negociação de parâmetros criptográficos complexos, gera pacotes com maior conteúdo útil (payload) e maior overhead, resultando em um consumo de largura de banda substancialmente maior. Isso tem implicações significativas para a capacidade da infraestrutura de rede e para o gerenciamento de recursos, especialmente em redes com tráfego intenso.

5.4.6 Comparativo do Tamanho dos Pacotes

Para entender a distribuição do tamanho dos pacotes (payload) e identificar possíveis outliers, a Figura 19 utiliza um boxplot para comparar os cenários ICPEdu e Usuário e Senha.

A Figura 19 compara a distribuição do tamanho dos pacotes para ambos os métodos.

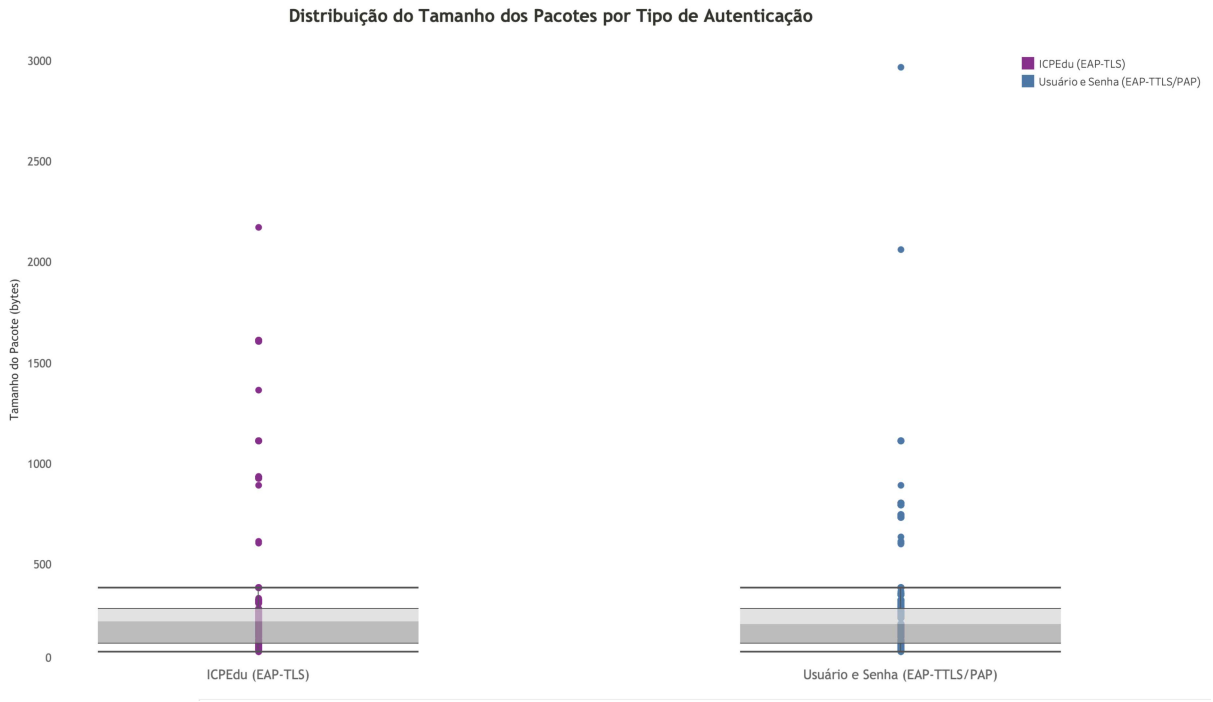

Figura 19 – Distribuição do Tamanho dos Pacotes: ICPEdu (EAP-TLS) vs. Usuário e Senha (EAP-TTLS/PAP).

No caso do ICPEdu (EAP-TLS), a distribuição é visivelmente mais ampla, com pacotes tendendo a ser significativamente maiores, predominantemente na faixa de 100 a 500 bytes, mas com uma concentração notável de pacotes acima de 500 bytes, podendo se estender até aproximadamente 2200 bytes. As estatísticas de quartis (mediana, Q1, Q3) para ICPEdu são consistentemente mais elevadas. Em contraste, o método Usuário e Senha (EAP-TTLS/PAP) concentra a maioria de seus pacotes em tamanhos menores, predominantemente abaixo de 500 bytes. Embora ambos os métodos apresentem outliers com tamanhos de pacotes maiores (inclusive acima de 2000 bytes), a densidade de pacotes pequenos é muito maior para Usuário e Senha, e seus quartis são substancialmente menores. Isso reflete o maior overhead criptográfico e de certificação do EAP-TLS, que exige a inclusão de dados adicionais nos pacotes, como certificados digitais e informações de sessão TLS, resultando em pacotes de maior tamanho.

6 CONCLUSÃO

Este trabalho teve como maior motivação a adoção de um método mais robusto para autenticação de usuários acadêmicos. Além de um referencial teórico e de embasamento para a pesquisa, os resultados da avaliação em um ambiente equivalente a uma federação eduroam real mostraram que o método EAP-TLS sobre o método tradicional EAP TTLS/PAP é possível de ser adotado. Foram identificadas características que podem ser levadas em consideração no momento na decisão de sua adoção em relação a desempenho, mas deixando claro o ganho em relação à segurança para o usuário final. Este trabalho se baseou para a análise a possibilidade de utilização de certificados ICPEdu no ambiente eduroam.

Em relação aos resultados númericos, a análise detalhada apresentada reforça as características distintas de desempenho e tráfego entre a autenticação com certificados ICPEdu (EAP-TLS) e a autenticação baseada em usuário e senha (EAP-TTLS/PAP) no contexto do eduroam. Enquanto o método ICPEdu (EAP-TLS) oferece um nível superior de segurança, especialmente pela autenticação mútua e a robustez da infraestrutura de chave pública, ele o faz com um custo notavelmente maior em termos de recursos de rede. Isso se manifesta em um número significativamente maior de pacotes e um volume substancialmente superior de dados trafegados (cerca de 41% a mais), além de pacotes de maior tamanho. Embora o tempo total acumulado de autenticação seja apenas marginalmente maior, o maior consumo de recursos por transação pode impactar a escalabilidade e a eficiência em redes de alta densidade e volume. Em conjunto, os resultados agregados de 33 mil autenticações e a análise de uma sessão típica indicam que o EAP-TLS com certificados pessoais ICPEdu aumenta a capacidade de autenticação em cerca de 24% por segundo, com impacto acumulado de apenas aproximadamente 4% no tempo total, o que reforça a viabilidade prática da migração mesmo em cenários de alta carga no eduroam.

Por outro lado, o método Usuário e Senha (EAP-TTLS/PAP) demonstra uma eficiência de rede superior, exigindo menos pacotes e um volume de dados consideravelmente menor. Sua agilidade na acumulação de pacotes ao longo do tempo (evidenciada pela CDF) sugere um comportamento mais leve, o que pode ser vantajoso em cenários em que a otimização da largura de banda e a minimização da carga sobre os servidores RADIUS são prioritárias. Contudo, é fundamental reconhecer que essa eficiência vem à custa da robustez de segurança oferecida pela autenticação mútua baseada em certificados.

A escolha entre os dois métodos, portanto, deve ser uma decisão estratégica que pondera os requisitos de segurança (onde ICPEdu se destaca) versus a eficiência e escalabilidade da rede (onde Usuário e Senha tem vantagens). Para futuras implantações do eduroam ou aprimoramentos em infraestruturas existentes, a compreensão desses trade-offs

é crucial para otimizar tanto a segurança quanto o desempenho da rede.

Respondendo à questão de pesquisa e às subquestões, temos:

Questão de Pesquisa: *"Como a utilização de certificados pessoais da ICPEdu impacta a performance de autenticação no eduroam em comparação com os métodos tradicionais baseados em credenciais compartilhadas".*

Resposta: A utilização de certificados pessoais da ICPEdu, aliada ao protocolo EAP-TLS, confere um incremento substancial na segurança da autenticação no eduroam, superando as vulnerabilidades dos métodos baseados em credenciais compartilhadas. Contudo, essa robustez é acompanhada por um impacto mensurável na performance de rede, manifestado em um maior volume de pacotes e dados trafegados por transação e um tempo total de autenticação acumulado ligeiramente superior. O estudo demonstra que o EAP-TLS com ICPEdu é tecnicamente viável e mais seguro, mas demanda maior capacidade de processamento e banda da infraestrutura de rede para manter a qualidade de serviço.

E as quatro subquestões:

1. Qual é o *overhead* temporal da validação de certificados ICPEdu em relação a credenciais compartilhadas?

   Resposta: O *overhead* temporal da validação de certificados ICPEdu, intrínseco ao processo de autenticação EAP-TLS, resultou em um tempo total de autenticação acumulado aproximadamente 4% maior em comparação ao método EAP-TTLS/PAP baseado em usuário e senha. Embora esta diferença possa ser considerada marginal em transações individuais, em ambientes de alta demanda e grande volume de autenticações, o impacto acumulado pode exigir considerações de otimização de infraestrutura.

2. Como a performance se comporta nas condições de rede típicas do ambiente acadêmico brasileiro?

   Resposta: Nas condições de rede simuladas, representativas do ambiente acadêmico, a performance do EAP-TLS com certificados ICPEdu evidenciou uma pegada de recursos significativamente maior. Observou-se um aumento de aproximadamente 29% na quantidade total de pacotes e um volume de dados trafegados cerca de 41% superior em comparação com o EAP-TTLS/PAP. Além disso, a análise do tamanho dos pacotes revelou que o EAP-TLS tende a gerar pacotes de maior dimensão, predominantemente na faixa de 100 a 500 bytes, e com uma presença notável de pacotes acima de 500 bytes, estendendo-se até 2200 bytes, refletindo o overhead criptográfico e de certificação. Estes resultados indicam que o ambiente acadêmico deve estar preparado para suportar essa carga adicional na rede.

3. Qual é a capacidade de escalabilidade da solução em termos de usuários simultâneos e uso de recursos do servidor RADIUS?

   Resposta: Embora este estudo não tenha mensurado diretamente a Taxa de Autenticações Simultâneas (TAS) ou o Overhead de Validação PKI (OVP) de forma isolada, a análise do maior volume de pacotes e dados por transação no EAP-TLS com ICPEdu sugere uma demanda computacional e de rede mais elevada para o servidor RADIUS. Consequentemente, para manter a capacidade de escalabilidade em cenários de alta concorrência de usuários simultâneos, a solução exige um dimensionamento mais robusto da infraestrutura de autenticação e dos servidores RADIUS, bem como otimizações em processos de validação de certificados.

4. De que forma a latência de *roaming* entre pontos de acesso é afetada pelo uso de certificados ICPEdu?

   Resposta: A latência de *roaming* entre pontos de acesso não foi um foco direto de medição neste estudo. No entanto, considerando o aumento de aproximadamente 4% no tempo total de autenticação e o maior volume de dados trafegados para o EAP-TLS com ICPEdu, é plausível inferir que, dependendo da implementação específica e das condições da rede, a latência percebida durante o processo de reconexão em cenários de *roaming* possa ser ligeiramente maior em comparação com o EAP-TTLS/PAP. Estudos dedicados seriam necessários para quantificar precisamente esse impacto.

As contribuições deste trabalho de dissertação abrangem a análise comparativa de segurança e desempenho da autenticação no eduroam com certificados ICPEdu, fornecendo uma análise empírica e quantitativa que preenche uma lacuna na literatura e na prática ao oferecer dados concretos sobre a superioridade e as implicações de sua adoção. Também foi realizada a adaptação de um robusto framework metodológico de avaliação de performance para as complexidades da autenticação em redes federadas como o eduroam, que pode servir como modelo para futuras análises em ambientes distribuídos. Por fim, gerou-se um conjunto de dados empíricos e análises quantitativas sobre latência, vazão e overhead computacional de EAP-TLS com certificados ICPEdu.

Como trabalhos futuros visa-se ainda, aprofundar a investigação da integração do EAP-TLS com certificados ICPEdu em novos ambientes tecnológicos emerge como prioridade, particularmente em redes 5G e soluções de Internet das Coisas (IoT) acadêmicas. Nestes cenários, a alta demanda por escalabilidade requer uma avaliação mais detalhada da Taxa de Autenticações Simultâneas (TAS) e do Overhead de Validação PKI (OVP) sob condições de alta concorrência e carga no servidor RADIUS. Além disso, a comparação do desempenho do EAP-TLS com outros métodos de autenticação modernos, especialmente aqueles desenvolvidos para ecossistemas 5G, e a exploração de otimizações no processo de validação de certificados poderiam gerar *insights* valiosos para o aprimoramento contínuo

da segurança e da eficiência em redes de próxima geração. Por fim, para facilitar a adoção em larga escala dessa tecnologia promissora, estudos de usabilidade e o aprimoramento dos processos de emissão e gestão de certificados ICPEdu para usuários finais são igualmente relevantes.

REFERÊNCIAS

1 (2020). Ieee standard for local and metropolitan area networks–port-based network access control. *IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018)*, pages 1–289.

2 Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and Levkowetz, H. (2004). Extensible authentication protocol (eap). RFC 3748, IETF.

3 Aboba, B. and Calhoun, P. (2003). Rfc3579: Radius (remote authentication dial in user service) support for extensible authentication protocol (eap).

4 Brenza, S., Pawlowski, A., and Pöpper, C. (2015). A practical investigation of identity theft vulnerabilities in eduroam. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 1–11.

5 Castells, M. (1999). *A Sociedade em Rede*. Paz e Terra, São Paulo.

6 Chen, J.-C. and Wang, Y.-P. (2005). Extensible authentication protocol (eap) and ieee 802.1 x: tutorial and empirical experience. *IEEE communications magazine*, 43(12):supl–26.

7 Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W. (2008). Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. RFC 5280, IETF. Define o perfil de uso de certificados X.509 v3 para a Internet.

8 DeKok, A. (2024). inkbridgenetworks.com. `https://www.inkbridgenetworks.com/web/content/2557?unique=47be02c8aed46c53b0765db185320249ad873d95`. [Accessado em 17/09/2025].

9 Edney, J. and Arbaugh, W. A. (2003). *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Addison-Wesley Professional.

10 Fluhrer, S., Mantin, I., and Shamir, A. (2001). Weaknesses in the key scheduling algorithm of rc4. In *Selected Areas in Cryptography. SAC 2001. Lecture Notes in Computer Science, vol 2259*. Springer.

11 Frank, L. R., Galletta, A., Carnevale, L., Vieira, A. B., and Silva, E. F. (2024). Intelligent resource allocation in wireless networks: Predictive models for efficient access point management. *Computer Networks*, 254:110762.

12 Funk, P. and Blake-Wilson, S. (2008). Extensible authentication protocol tunneled transport layer security authenticated protocol version 0 (eap-ttlsv0). RFC 5281, IETF.

13 Gaminara, A. (2022). *Performance and security evaluation of TLS, DTLS and QUIC security protocols*. PhD thesis, Politecnico di Torino.

14 Giddens, A. (1991). *As Consequências da Modernidade*. Editora UNESP, São Paulo.

15 Goldberg, S., Haller, M., Heninger, N., Milano, M., Shumow, D., Stevens, M., and Suhl, A. (2024a). RADIUS/UDP considered harmful. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 7429–7446, Philadelphia, PA. USENIX Association.

16 Goldberg, S., Haller, M., Heninger, N., Milano, M., Shumow, D., Stevens, M., and Suhl, A. (2024b). {RADIUS/UDP} considered harmful. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 7429–7446.

17 GÉANT Association (2025). eduroam: The global wi-fi roaming service for research and education. Online. Dados de cobertura e estatísticas. Disponível em: `https://www.eduroam.org`.

18 Halbouni, A., Ong, L.-Y., and Leow, M.-C. (2023). Wireless security protocols wpa3: A systematic literature review. *IEEE access*, 11:112438–112450.

19 He, C. and Mitchell, J. C. (2011). Security analysis and improvement of ieee 802.11i. *Security and Communication Networks*, 4(5):557–574.

20 Hollick, M., Tews, E., Martin, J., Rihl, A., von Malorny, P., and Hering, L. (2008). Usable and secure wireless lan authentication? a-priori trust and the dangers of misconfigured 802.1x. In *Proceedings of the 2008 ACM CoNEXT Conference*, pages 1–6. ACM.

21 Hue, M. H., Debnath, J., Leung, K. M., Li, L., Minaei, M., Mazhar, M. H., Xian, K., Hoque, E., Chowdhury, O., and Chau, S. Y. (2021). All your credentials are belong to us: On insecure wpa2-enterprise configurations. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1100–1117.

22 IEEE (2004). *IEEE Std 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements*. IEEE Standards Association.

23 IEEE (2020). *IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control*. IEEE Standards Association. IEEE Std 802.1X-2020.

24 International Telecommunication Union (2019). Recommendation itu-t x.509: Information technology – open systems interconnection – the directory: Public-key and attribute certificate frameworks. Technical report, ITU-T. Padrão internacional para certificados de chave pública.

25 International Telecommunication Union (2023). Measuring digital development: Facts and figures 2023. Technical report, ITU, Geneva. Disponível em: `https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/`.

26 Kwon, S. and Choi, H.-K. (2020). Evolution of wi-fi protected access: Security challenges. *IEEE Consumer Electronics Magazine*, 10(1):74–81.

27 Lotfy, A. Y., Zaki, A. M., Abd-El-Hafeez, T., and Mahmoud, T. M. (2021). Privacy issues of public wi-fi networks. In *The international conference on artificial intelligence and computer vision*, pages 656–665. Springer.

28 Marcelo Carlomagno Carlos, Jeandre Monteiro Sutil, C. T. M. J. G. K. D. P. and Spagnuelo, B. (2014). ICPEdu Introdução a Infraestrutura de Chaves Públicas e Aplicações. *Rede Nacional de Ensino e Pesquisa*.

29 Marlinspike, M. and Hulton, D. (2012). Divide and conquer: Cracking ms-chapv2 with a 100% success rate. DEF CON 20 Hacking Conference. Apresentação detalhando a quebra do protocolo MS-CHAPv2.

30 Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., and Bianchi, G. (2023). Attacks and vulnerabilities of wi-fi enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications*, 212:129–140.

31 Palamà, I., Amici, A., Gringoli, F., and Bianchi, G. (2022). "careful with that roam, edu": experimental analysis of eduroam credential stealing attacks. In *2022 17th Wireless On-Demand Network Systems and Services Conference (WONS)*, pages 1–7. IEEE.

32 Palekar, A., Simon, D., Zorn, G., Salowey, J., and Zhou, H. (2004). Protected eap protocol (peap) version 2. Internet-draft, IETF. draft-josefsson-pppext-eap-tls-eap-05.

33 Presidência da República do Brasil (2001). Medida provisória nº 2.200-2, de 24 de agosto de 2001. Diário Oficial da União. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

34 Raj, V. (2024). Eap-tls vs. eap-ttls/pap. [Accessado em 17/09/2025].

35 Rede Nacional de Ensino e Pesquisa (RNP) (2024). Icpedu - serviço de certificados digitais. Website Oficial. Disponível em: `https://www.rnp.br/servicos/servicos-avancados/icpedu`.

36 Rigney, C., Willens, S., Rubens, A., and Simpson, W. (2000). Remote authentication dial in user service (radius). RFC 2865, IETF.

37 Saade, D. C. M., Carrano, R. C., Silva, E. F., and Magalhães, L. (2013). Eduroam: Acesso sem fio seguro para a comunidade acadêmica federada. *Rede Nacional de Ensino e Pesquisa*.

38 Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C. (2013). X.509 internet public key infrastructure online certificate status protocol - ocsp. RFC 6960, IETF.

39 Schepers, D., Ranganathan, A., and Vanhoef, M. (2019). Practical side-channel attacks against wpa-tkip. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pages 415–426.

40 Sermersheim, J. (2006). Lightweight directory access protocol (ldap): The protocol. RFC 4511, IETF.

41 Sheldon, F. T., Weber, J. M., Yoo, S.-M., and Pan, W. D. (2012). The insecurity of wireless networks. *IEEE Security & Privacy*, 10(4):54–61.

42 Simon, D., Aboba, B., and Hurst, R. (2008). The eap-tls authentication protocol. RFC 5216, IETF.

43 Tews, E. and Beck, M. (2009). Practical attacks against wep and wpa. In *Proceedings of the second ACM conference on Wireless network security*, pages 79–86.

44 Trindade, L. M., Farias, J., Ribeiro Filho, A., Sousa, F., and Wangham, M. S. (2024). Serviço gidlab: Impulsionando a pesquisa experimental em gestão de identidade. *XV Computer on the Beach*.

45 Vanhoef, M. and Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in wpa2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1313–1328. ACM.

46 Wi-Fi Alliance (2004). Wi-fi alliance announces wep is officially retired. Press Release.

47 Wierenga, K., Winter, S., and Koren, T. (2010). The eduroam architecture for network roaming in academic and research communities. Technical Report GN3-NA3-T4-AF, TERENA. Documento de definição da arquitetura do eduroam.

48 Wright, J. and Antoniewicz, B. (2025). hostapd-wpe | Kali Linux Tools — kali.org. `https://www.kali.org/tools/hostapd-wpe/`. [Accessed 16-07-2025].

49 Zhang, J., Yang, L., Cao, W., and Wang, Q. (2020). Formal analysis of 5g eap-tls authentication protocol using proverif. *IEEE access*, 8:23674–23688.