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

A FALSIFICAÇÃO DO IDENTIFICADOR DE CHAMADAS ATUANDO COMO UM PERMISSOR DAS FRAUDES TELEFÔNICAS

Gustavo Gomes de Arruda e Annderson Weshleen Confessor de Sousa Alves

Orientador: José Antônio Cândido Borges da Silva

Campina Grande, fevereiro de 2025

A FALSIFICAÇÃO DO IDENTIFICADOR DE CHAMADAS ATUANDO COMO UM PERMISSOR DAS FRAUDES TELEFÔNICAS

Gustavo Gomes de Arruda e Annderson Weshleen Confessor de Sousa Alves

---

José Antônio Cândido Borges da Silva
Orientador

Éwerton Rômulo Silva Castro
Membro da Banca

Marcelo Portela Sousa
Membro da Banca

Campina Grande, Paraíba, Brasil
Março/2025

Catalogação na fonte:
Ficha catalográfica elaborada por Gustavo César Nogueira da Costa - CRB 15/479

A778f Arruda, Gustavo Gomes de

A falsificação do identificador de chamadas atuando como um permissor das fraudes telefônicas / Gustavo Gomes de Arruda, Annderson Weshleen Confessor de Sousa Alves. - Campina Grande, 2025.

26 f. : il.

Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Telemática) - Instituto Federal da Paraíba, 2024.

Orientador: Prof. José Antônio Cândido Borges da Silva.

1. Telemática 2. Fraudes telefônicas 3. STIR/SHAKEN - protocolo de segurança 4. Infraestrutura de Chaves Públicas - PKI I. Alves, Annderson Weshleen Confessor de Sousa II Silva, José Antônio Cândido Borges da III.Título.

CDU 621.3

Agradecimentos

Agradecemos ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), *Campus* Campina Grande, pelo suporte acadêmico essencial para a conclusão do curso e pela formação proporcionada ao longo dessa jornada.

Expressamos nossa gratidão ao nosso orientador, José Antônio Cândido Borges da Silva, aos membros da banca, Éwerton Rômulo Silva Castro e Marcelo Portela Sousa, e a todos os professores do *campus*, cujo conhecimento e dedicação foram fundamentais para o nosso desenvolvimento acadêmico e profissional.

Aos nossos familiares, pelo apoio incondicional, paciência e incentivo contínuo, somos profundamente gratos. Seu suporte foi essencial para que superássemos os desafios desta etapa.

Por fim, agradecemos aos colegas do curso de Telemática pelo companheirismo e troca de aprendizados, tornando essa caminhada mais enriquecedora.

Resumo

Este trabalho investiga o protocolo STIR/SHAKEN como solução técnica para combater fraudes telefônicas e falsificação do identificador de chamadas. Por meio de uma revisão sistemática da literatura, foram analisados cinco artigos científicos que discutem seus principais benefícios, limitações e perspectivas futuras, com ênfase na adoção do protocolo no Brasil. O estudo destaca que, embora o STIR/SHAKEN seja eficaz na autenticação de chamadas e na redução de *robocalls*, sua implementação enfrenta desafios como a dependência da Infraestrutura de Chaves Públicas (*Public Key Infrastructure* - PKI), dificuldades de integração com redes legadas e altos custos operacionais. No contexto brasileiro, a liderança da ABR Telecom e a supervisão da Anatel representam um esforço relevante para mitigar fraudes telefônicas. Este trabalho também aborda alternativas tecnológicas, como o *Caller ID Verification* (CIV), que ampliam as possibilidades de aplicação do STIR/SHAKEN em diferentes cenários. Conclui-se que o sucesso do protocolo dependerá da adesão global, de investimentos contínuos em pesquisa e da evolução regulatória para garantir a segurança das comunicações em um ambiente digital cada vez mais dinâmico.

Palavras-chave: STIR/SHAKEN, fraudes telefônicas, autenticação de chamadas, telecomunicações, PKI, robocalls, Caller ID Verification.

Abstract

This study investigates the STIR/SHAKEN protocol as a technical solution to combat telephone fraud and caller ID spoofing. Through a systematic literature review, five scientific articles were analyzed to discuss its main benefits, limitations, and future perspectives, with an emphasis on the protocol's adoption in Brazil. The study highlights that while STIR/SHAKEN is effective in call authentication and reducing robocalls, its implementation faces challenges such as the dependency on Public Key Infrastructure (PKI), difficulties in integrating with legacy networks, and high operational costs. In the Brazilian context, the leadership of ABR Telecom and the supervision of Anatel represent a significant effort to mitigate telephone fraud. This study also explores technological alternatives, such as Caller ID Verification (CIV), which expand the applicability of STIR/SHAKEN in different scenarios. It concludes that the success of the protocol will depend on global adoption, continuous investment in research, and regulatory advancements to ensure the security of communications in an increasingly dynamic digital environment.

Keywords: STIR/SHAKEN, telephone fraud, call authentication, telecommunications, PKI, robocalls, Caller ID Verification.

Sumário

1 Introdução 10
2 Fundamentação Teórica 11
2.1 Objetivo Geral e Específicos 11
2.2 Caller ID e Suas Vulnerabilidades 11
2.3 Infraestrutura de Chaves Públicas (PKI) 12
3 Fundamentação Teórica 13
3.1 VoIP e SIP: Benefícios e Desafios 13
3.2 O Papel do SS7 nas Telecomunicações 13
3.3 Arquitetura Zero-Trust 14
3.4 Protocolo STIR 15
3.5 Protocolo SHAKEN 16
3.6 Funcionamento do STIR/SHAKEN 16
3.7 Desafios e Limitações do STIR/SHAKEN 17
3.8 Impacto Global e Perspectivas Futuras 18
4 Metodologia 18
4.1 Representação Gráfica do Processo 18
4.2 Critérios de Inclusão e Exclusão 19
4.3 Processo de Busca e Seleção 19
4.4 Organização e Análise dos Dados 20
4.5 Comentários e Análise 20
5 Resultados e Discussão 21
5.1 Artigo 1: Spoofing Against Spoofing 22
5.2 Artigo 2: Strategic Spam Call Control and Fraud Management 22
5.3 Artigo 3: How to Shut Down Robocallers 22
5.4 Artigo 4: Dynamic Public Key Certificates 23
5.5 Artigo 5: Towards Zero-Trust VoIP Architecture 23
6 Discussão Geral 23
6.1 Implementação do STIR/SHAKEN no Brasil 24
6.2 Impacto Global e Lições de Outras Implementações 25
6.3 Perspectivas Futuras 26
7 Conclusão 26
8 Referências Bibliográficas 28

Lista de Abreviaturas

- **ABR Telecom** - Associação Brasileira de Recursos em Telecomunicações
- **ACM** - *Association for Computing Machinery* (Associação para Máquinas de Computação)
- **Anatel** - Agência Nacional de Telecomunicações
- **CA** - *Certificate Authority* (Autoridade Certificadora)
- **CIV** - *Caller ID Verification* (Verificação de Identidade do Chamador)
- **FCC** - *Federal Communications Commission* (Comissão Federal de Comunicações)
- **FTC** - *Federal Trade Commission* (Comissão Federal de Comércio)
- **IETF** - *Internet Engineering Task Force* (Força-Tarefa de Engenharia da Internet)
- **IEEE** - *Institute of Electrical and Electronics Engineers* (Instituto de Engenheiros Eletricistas e Eletrônicos)
- **IP** - *Internet Protocol* (Protocolo de Internet)
- **JSON** - *JavaScript Object Notation* (Notação de Objetos JavaScript)
- **NIST** - *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia)
- **PBX** - *Private Branch Exchange* (Central Telefônica Privada)
- **PKI** - *Public Key Infrastructure* (Infraestrutura de Chaves Públicas)
- **PRISMA** - *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (Itens Preferenciais para Relatar Revisões Sistemáticas e Meta-Análises)
- **PSTN** - *Public Switched Telephone Network* (Rede Telefônica Comutada Pública)
- **RA** - *Registration Authority* (Autoridade de Registro)
- **RFC** - *Request for Comments* (Solicitação de Comentários)

- **SHAKEN** - *Signature-based Handling of Asserted Information using toKENs* (Manipulação Baseada em Assinatura de Informações Afirmadas Usando Tokens)
- **SIP** - *Session Initiation Protocol* (Protocolo de Iniciação de Sessão)
- **SS7** - *Signaling System No. 7* (Sistema de Sinalização Nº 7)
- **STIR** - *Secure Telephony Identity Revisited* (Identidade Segura de Telefonia Revisitada)
- **VA** - *Validation Authority* (Autoridade de Validação)
- **VoIP** - *Voice over Internet Protocol* (Voz sobre Protocolo de Internet)

1 Introdução

A falsificação do identificador de chamadas, conhecida como *Caller ID Spoofing*, é uma técnica amplamente explorada por fraudadores para mascarar a origem real de ligações telefônicas. Essa prática permite que criminosos utilizem números falsificados para enganar as vítimas, fazendo com que chamadas pareçam originadas de instituições legítimas, como bancos, órgãos governamentais e empresas de grande porte. Dessa forma, é possível induzir usuários a fornecerem informações sigilosas, realizarem pagamentos fraudulentos ou até mesmo concederem acesso indevido a sistemas protegidos. Além disso, essa técnica tem sido utilizada para espalhar desinformação e realizar ataques coordenados, aumentando ainda mais os riscos associados às comunicações telefônicas.

O impacto dessa técnica é expressivo, tanto para indivíduos quanto para empresas e operadoras de telecomunicações. De acordo com a empresa de segurança Hiya, apenas em 2018 foram registradas aproximadamente 85 bilhões de chamadas falsificadas em todo o mundo, evidenciando a escala do problema e a necessidade urgente de soluções eficazes (McEachern e Burger, 2019). O aumento do uso de tecnologia *Voice over IP* (VoIP) facilitou ainda mais a execução do *Caller ID Spoofing*, uma vez que chamadas originadas por protocolos digitais podem ser manipuladas com maior facilidade. Nesse cenário, mecanismos tradicionais de identificação de chamadas se tornam obsoletos, exigindo novas abordagens para garantir a segurança das comunicações.

Diante dessa problemática, diversos países têm adotado medidas para mitigar o impacto dessa fraude. No Brasil, a Agência Nacional de Telecomunicações (Anatel) determinou a implementação do protocolo de autenticação e identificação de chamadas, conhecido como *Secure Telephony Identity Revisited/Signature-based Handling of Asserted Information Using Tokens* (STIR/SHAKEN), denominado no país como Origem Verificada. Inicialmente prevista para o final de 2024, a implementação do protocolo teve seus primeiros testes iniciados nesse período, e algumas operadoras passaram a adotá-lo voluntariamente. No entanto, a obrigatoriedade foi postergada para 2025, permitindo que operadoras ajustem suas infraestruturas para garantir a implementação integral do sistema.

O STIR/SHAKEN tem como principal objetivo autenticar chamadas telefônicas e fornecer aos consumidores informações adicionais sobre a origem das ligações, incluindo o nome da empresa emissora, logotipo, motivo da chamada e um selo de autenticação. Com isso, busca-se reduzir fraudes, bloqueando chamadas suspeitas antes que cheguem ao destinatário e restaurando a confiança dos usuários no sistema de telecomunicações. Até outubro de 2024, 33 operadoras aderiram ao programa, incluindo Claro, TIM, Vivo, Oi e Algar, comprometendo-se a autenticar pelo menos 10% do tráfego mensal de chamadas no país, o que representa aproximadamente 2,2 bilhão de ligações autenticadas por mês (TELESÍNTESE, 2024b). No entanto, desafios técnicos e estruturais, como a compatibilidade com dispositivos e a necessidade de adaptações nas redes, levaram ao adiamento da obrigatoriedade do protocolo para 2025.

Embora eficaz, o protocolo enfrenta desafios relacionados à escalabilidade e à compatibilidade com redes legadas, como o sistema *Signaling System No. 7* (SS7). Reguladores internacionais, como a *Federal Communications Commission* (FCC), já exigem sua implementação nos Estados Unidos, com resultados promissores. No entanto, questões como a dependência de uma Infraestrutura de Chaves Públicas (*Public Key Infrastructure* - PKI) e a integração em ambientes não baseados em IP permanecem como barreiras significativas (Wang et al., 2023).

Além dos prejuízos financeiros, a falsificação do identificador de chamadas compromete a confiança pública nas telecomunicações. A Ofcom, reguladora de telecomunicações do Reino Unido, recomenda que os consumidores adotem práticas de verificação, como retornar às chamadas suspeitas, para mitigar os riscos associados.

Dessa forma, o STIR/SHAKEN representa um avanço importante no combate às fraudes telefônicas. Desenvolvido com base em padrões como as *Request for Comments* (RFCs) do *Internet Engineering Task Force* (IETF), o protocolo utiliza certificação digital para autenticar chamadas e já demonstra eficácia em redes baseadas em *Internet Protocol* (IP), utilizando o *Session Initiation Protocol* (SIP), abrangendo tanto linhas fixas quanto móveis. Contudo, sua aplicação global requer esforços coordenados entre operadoras, reguladores e a indústria de telecomunicações.

2 Fundamentação Teórica

2.1 Objetivo Geral e Específicos

O objetivo geral deste trabalho é analisar os mecanismos adotados pelo mercado de telecomunicações, com foco no protocolo STIR/SHAKEN, para combater a falsificação do identificador de chamadas, destacando sua eficácia, limitações e perspectivas futuras.

Os objetivos específicos incluem:

- Identificar publicações acadêmicas e técnicas relevantes que abordem o protocolo STIR/SHAKEN e sua aplicação prática;
- Avaliar a relevância, eficácia e impacto das soluções discutidas na literatura para combater fraudes relacionadas ao identificador de chamadas;
- Sintetizar e apresentar os resultados da pesquisa em um formato de revisão sistemática da literatura, destacando as lacunas e avanços no campo.

2.2 Caller ID e Suas Vulnerabilidades

O *Caller ID* foi introduzido como uma funcionalidade projetada para exibir o número de origem de uma chamada telefônica, visando aumentar a transparência e a confiança nas comunicações. No entanto, essa tecnologia apresenta vulnerabilidades que possibilitaram

o surgimento de práticas fraudulentas, como o *Caller ID Spoofing*. Essa técnica consiste na falsificação do número exibido no identificador de chamadas, permitindo que criminosos façam chamadas fraudulentas aparentando ser de fontes legítimas. Essa manipulação é amplamente explorada em diferentes tipos de golpes, como *phishing*, em que vítimas são induzidas a fornecer informações sensíveis sob o pretexto de um contato oficial; extorsões, nas quais ameaças são realizadas a partir de números falsificados para coagir as vítimas ao pagamento de valores; e a disseminação de desinformação, onde chamadas automáticas são utilizadas para espalhar mensagens enganosas com intenções maliciosas.

Segundo McEachern e Burger (2019), o *Caller ID Spoofing* desempenha um papel central no aumento do volume de *robocalls*, chamadas telefônicas automatizadas que, frequentemente, têm fins fraudulentos. Em 2018, essa prática resultou em um total de 85 bilhões de chamadas globais, comprometendo significativamente a confiança dos usuários nas comunicações telefônicas. As *robocalls* são amplamente utilizadas em golpes de engenharia social, onde criminosos empregam mensagens pré-gravadas para induzir vítimas a fornecerem informações sensíveis, efetuarem pagamentos indevidos ou acreditarem em informações enganosas. Esse cenário evidencia a necessidade de soluções mais robustas para mitigar os riscos associados a essa ameaça crescente.

Além disso, Wang et al. (2023) apontam que a popularização de sistemas VoIP e a facilidade de manipulação de identificadores de chamadas aumentaram a sofisticação e o alcance dessas fraudes. Essas ameaças evidenciam a importância de mecanismos como o STIR/SHAKEN, que buscam autenticar a origem das chamadas e mitigar tais vulnerabilidades.

2.3 Infraestrutura de Chaves Públicas (PKI)

A Infraestrutura de Chaves Públicas (*Public Key Infrastructure* - PKI) é um conjunto de políticas, procedimentos, hardware e software utilizados para criar, gerenciar e revogar certificados digitais. Esses certificados vinculam chaves públicas a identidades específicas, permitindo a autenticação confiável e a comunicação segura entre partes.

No contexto do STIR/SHAKEN, a PKI desempenha um papel fundamental, emitindo certificados digitais que autentiquem as chamadas telefônicas. Esses certificados garantem que o número apresentado ao receptor seja legítimo e não tenha sido manipulado durante a transmissão.

Conforme descrito por Chien (2021), o modelo tradicional de PKI apresenta desafios significativos, como custos elevados de renovação e a necessidade de infraestrutura robusta para sua manutenção. O autor propõe o uso de certificados dinâmicos, que permitem a troca de chaves públicas sem necessidade de renovação frequente, reduzindo custos e aumentando a eficiência. Esses avanços são especialmente importantes para a aplicação do STIR/SHAKEN em mercados emergentes, onde os recursos podem ser limitados.

Entretanto, a dependência da PKI também apresenta limitações. Redes legadas não suportam a autenticação baseada em PKI, o que deixa esses sistemas vulneráveis a ataques

de falsificação. Esses desafios destacam a necessidade de explorar alternativas tecnológicas que possam complementar o modelo atual e garantir a segurança das comunicações.

3 Fundamentação Teórica

3.1 VoIP e SIP: Benefícios e Desafios

A tecnologia de Voz sobre IP (VoIP) permite a realização de chamadas telefônicas utilizando redes de internet, substituindo as linhas telefônicas tradicionais. Essa abordagem oferece vantagens econômicas e operacionais, como redução de custos e maior flexibilidade nas comunicações. O Protocolo de Iniciação de Sessão (SIP) é amplamente utilizado para gerenciar essas chamadas, sendo responsável pelo estabelecimento, manutenção e término de sessões de comunicação.

Embora o VoIP represente uma revolução nas telecomunicações, ele também trouxe novos desafios de segurança. A facilidade de manipulação de cabeçalhos SIP, por exemplo, permite que golpistas realizem *Caller ID Spoofing*, mascarando a origem das chamadas. Wang et al. (2023) destacam que o VoIP potencializou a disseminação de *robocalls* e outros golpes relacionados, devido à sua vulnerabilidade a ataques de falsificação.

Além disso, o SIP é suscetível a diversos tipos de ataques, como interceptação de chamadas, manipulação de mensagens e *spoofing*. Para mitigar esses problemas, foram desenvolvidas soluções como o STIR/SHAKEN, que adicionam autenticação digital aos cabeçalhos SIP. Isso garante que as chamadas sejam originadas por fontes legítimas, aumentando a confiança dos usuários.

Koilada (2019) aponta que, apesar de seus benefícios, a integração do STIR/SHAKEN em sistemas VoIP enfrenta desafios técnicos e regulatórios. Entre eles, destacam-se os custos associados à implementação e as dificuldades de interoperabilidade entre diferentes operadoras. Esses obstáculos ressaltam a importância de esforços coordenados entre reguladores, operadoras e pesquisadores para aprimorar a segurança nas comunicações.

3.2 O Papel do SS7 nas Telecomunicações

O *Signaling System No. 7* (SS7) é um conjunto de protocolos de sinalização utilizado globalmente para o gerenciamento de chamadas em redes de telefonia fixa e móvel. O SS7 permite a comunicação entre centrais telefônicas, possibilitando funções como encaminhamento de chamadas, portabilidade numérica, mensagens SMS e autenticação de usuários. Esse protocolo foi originalmente desenvolvido para operar em redes de telefonia controladas diretamente por operadoras, onde todos os elementos da infraestrutura eram considerados confiáveis. Nesse ambiente fechado, a necessidade de mecanismos avançados de segurança era mínima. No entanto, com a interconexão dessas redes a sistemas externos e a evolução das telecomunicações, o SS7 tornou-se vulnerável a interceptações e falsificação de chamadas

quando exposto a redes não confiáveis.

No contexto da segurança, o SS7 não possui suporte nativo para criptografia ou autenticação digital robusta, tornando-se um alvo para ataques e interceptação de chamadas. Como resultado, redes baseadas em SS7 não são compatíveis com o protocolo STIR/SHAKEN, que exige infraestrutura baseada em IP e suporte para criptografia de chave pública. Essa limitação reforça a necessidade de atualizações tecnológicas ou da adoção de soluções complementares, como o *Caller ID Verification* (CIV), que busca oferecer uma alternativa para redes legadas (Wang et al., 2023).

Dessa forma, apesar de sua ampla utilização, o SS7 apresenta desafios significativos para a implementação de mecanismos modernos de autenticação de chamadas, exigindo adaptações e estratégias híbridas para garantir a segurança das telecomunicações.

3.3 Arquitetura Zero-Trust

A arquitetura *Zero-Trust* é um modelo de segurança cibernética baseado no princípio de que nenhuma entidade, seja interna ou externa a uma rede, deve ser automaticamente confiável. Diferente das abordagens tradicionais, que pressupõem a confiabilidade de usuários e dispositivos dentro de um perímetro de rede definido, a *Zero-Trust* adota uma política de verificação contínua, exigindo autenticação rigorosa e monitoramento constante para conceder acesso a recursos e sistemas.

O conceito de *Zero-Trust* foi formalizado pelo *National Institute of Standards and Technology* (NIST), que define os princípios fundamentais dessa abordagem. Entre as diretrizes principais, destacam-se:

- **Verificação explícita**: todos os acessos devem ser autenticados e autorizados com base em múltiplos critérios, como identidade do usuário, localização e integridade do dispositivo.
- **Menor privilégio possível**: os usuários e dispositivos devem receber apenas os acessos estritamente necessários para a execução de suas funções.
- **Suposição de violação**: a segurança da rede deve ser projetada considerando que ataques podem ocorrer a qualquer momento, exigindo monitoramento contínuo e respostas rápidas a ameaças.

No contexto das telecomunicações, a adoção da arquitetura *Zero-Trust* se mostra relevante na mitigação de ataques como a falsificação do identificador de chamadas e outras ameaças associadas à manipulação de protocolos de sinalização. A integração dessa abordagem ao SHAKEN permite um controle mais rigoroso sobre a autenticação de chamadas, reforçando a confiabilidade e segurança das redes de comunicação.

3.4 Protocolo STIR

O *Secure Telephone Identity Revisited* (STIR) é um padrão desenvolvido pelo *Internet Engineering Task Force* (IETF) para combater a falsificação de identificadores de chamadas em redes VoIP. Definido em uma série de documentos técnicos conhecidos como *Request for Comments* (RFCs), o STIR estabelece um mecanismo de autenticação digital para verificar se o número de chamada exibido ao destinatário corresponde, de fato, ao originador legítimo da ligação.

O funcionamento do STIR é estruturado com base em quatro RFCs principais:

- **RFC 8224**: define a estrutura do protocolo e o processo de assinatura digital das chamadas;
- **RFC 8225**: especifica o formato dos certificados utilizados na autenticação das chamadas;
- **RFC 8226**: estabelece os métodos de gerenciamento e validação das assinaturas digitais;
- **RFC 8588**: expande o protocolo STIR, introduzindo identificadores adicionais para melhorar a interoperabilidade entre operadoras e sistemas de telefonia.

O STIR é baseado no protocolo SIP, utilizado para o estabelecimento, manutenção e encerramento de chamadas VoIP. No entanto, o SIP, por si só, não possui um mecanismo nativo de autenticação da identidade do chamador. O STIR resolve essa limitação adicionando assinaturas digitais às chamadas, permitindo a verificação da legitimidade do número apresentado. Esse processo ocorre em três etapas principais:

- A operadora de origem da chamada assina digitalmente o número do *Caller ID* com um certificado emitido por uma autoridade certificadora reconhecida;
- A assinatura digital é transmitida junto com a chamada até a operadora de destino;
- A operadora de destino verifica a assinatura digital para garantir a autenticidade do número apresentado.

Embora o STIR seja eficiente na autenticação de chamadas, ele apenas valida a origem da ligação, sem definir como chamadas não autenticadas devem ser tratadas. Isso significa que o protocolo, por si só, não determina se chamadas suspeitas devem ser bloqueadas, sinalizadas ou permitidas.

Conforme descrito por McEachern e Burger (2019), o STIR é eficiente na proteção de redes baseadas em IP, como SIP. No entanto, sua eficácia é limitada em redes legadas, como SS7, que não possuem suporte nativo para autenticação digital. Essa limitação reforça a necessidade de soluções complementares para garantir a integridade das chamadas em diferentes tipos de infraestrutura de telecomunicações.

3.5 Protocolo SHAKEN

O *Signature-based Handling of Asserted Information Using ToKENs* (SHAKEN) é um *framework* desenvolvido pela *Alliance for Telecommunications Industry Solutions* (ATIS) e pelo SIP Forum para definir a implementação prática do STIR em redes comerciais de telecomunicações. Enquanto o STIR autentica chamadas adicionando assinaturas digitais, o SHAKEN estabelece as diretrizes que as operadoras devem seguir para classificar e tratar chamadas autenticadas e não autenticadas.

Para isso, o SHAKEN introduz um sistema de atestação em três níveis:

- **Nível A (Totalmente autenticada):** o chamador e o número exibido foram verificados e são legítimos.
- **Nível B (Parcialmente autenticada):** a operadora de origem foi verificada, mas o número pode não estar associado a um chamador legítimo.
- **Nível C (Não autenticada):** a identidade do chamador não pôde ser verificada.

Além da categorização das chamadas, o SHAKEN define como chamadas não verificadas devem ser tratadas, permitindo que operadoras apliquem medidas como bloqueio, alertas de chamada suspeita ou encaminhamento sem alterações.

Dessa forma, enquanto o STIR autentica chamadas por meio de assinaturas digitais, o SHAKEN estabelece as regras para o uso dessas informações, garantindo que operadoras possam implementar políticas eficazes para proteger os usuários contra fraudes telefônicas. Juntos, esses dois componentes formam o sistema STIR/SHAKEN, já adotado em diversos países, incluindo os Estados Unidos e o Brasil, para combater fraudes telefônicas.

3.6 Funcionamento do STIR/SHAKEN

O protocolo STIR/SHAKEN utiliza certificados digitais baseados em técnicas de criptografia de chave pública para garantir que o número de chamada de uma ligação seja autêntico e não tenha sido falsificado. Nesse processo, o provedor de serviços telefônicos da parte originadora obtém um certificado digital de uma autoridade certificadora confiável, reconhecida por outros provedores de serviços telefônicos. Durante a chamada, a assinatura digital gerada é transmitida junto com a chamada. O provedor de serviços da parte destinatária verifica essa assinatura para confirmar a autenticidade do número de chamada. Caso a verificação seja bem-sucedida, a chamada é aceita; caso contrário, ela pode ser bloqueada. Este processo garante maior segurança e confiabilidade na comunicação TRANSNEXUS (2024).

Como ilustrado na Figura 1, o funcionamento do protocolo STIR/SHAKEN envolve múltiplas etapas, desde a autenticação da chamada até sua verificação pelo provedor de destino.

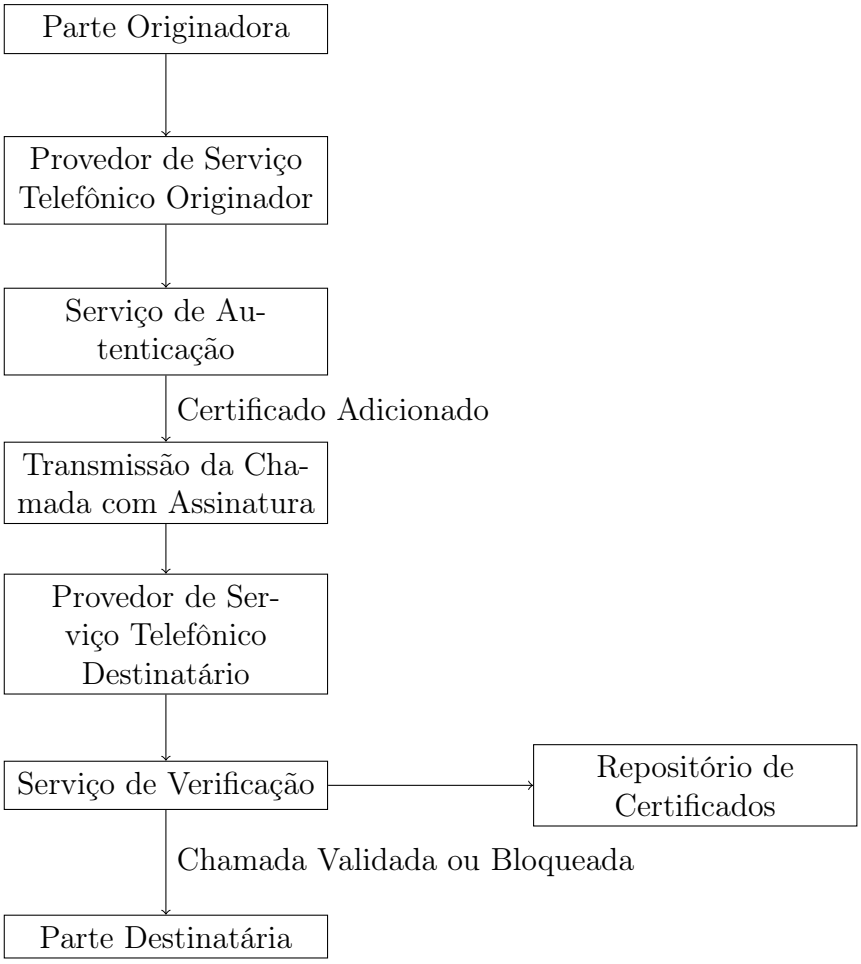

Figura 1: *Fluxograma Detalhado do Funcionamento do STIR/SHAKEN.*

3.7 Desafios e Limitações do STIR/SHAKEN

Apesar de sua eficácia comprovada, o STIR/SHAKEN enfrenta diversos desafios e limitações, incluindo:

- **Cobertura limitada:** o protocolo não protege redes legadas, como SS7, que ainda são amplamente utilizadas em muitos países;
- **Escalabilidade:** a implementação de uma PKI global é complexa e onerosa;
- **Interoperabilidade:** a integração entre operadoras de diferentes países é dificultada pela falta de padronização internacional.

Wang et al. (2023) sugerem que soluções alternativas, como o *Caller ID Verification* (CIV), podem complementar o STIR/SHAKEN, especialmente em redes não-IP. Essas abordagens destacam a necessidade de esforços colaborativos entre operadoras, reguladores e pesquisadores para superar as limitações atuais.

3.8 Impacto Global e Perspectivas Futuras

O impacto do STIR/SHAKEN tem sido significativo em países que implementaram o protocolo, como os Estados Unidos. Koilada (2019) aponta que a regulamentação TRACED Act foi fundamental para reduzir *robocalls* e aumentar a confiança nas telecomunicações. No entanto, desafios técnicos e regulatórios continuam a limitar sua adoção em escala global.

Perspectivas futuras incluem a integração do STIR/SHAKEN com tecnologias emergentes, como arquiteturas *Zero-Trust*, e o desenvolvimento de soluções complementares para redes legadas. Essas iniciativas são essenciais para garantir a segurança das comunicações em um cenário de ameaças crescentes.

4 Metodologia

A metodologia adotada neste trabalho fundamenta-se na Revisão Sistemática da Literatura (RSL), com o objetivo de identificar e analisar publicações relevantes sobre o protocolo STIR/SHAKEN como mecanismo de combate à falsificação do identificador de chamadas. A abordagem utilizada visa sintetizar as principais evidências e lacunas no campo, aplicando um método rigoroso para garantir a qualidade das publicações selecionadas.

Para assegurar transparência e reprodutibilidade no processo de seleção dos artigos, foram seguidas as diretrizes da metodologia *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA). O PRISMA consiste em um conjunto de diretrizes amplamente adotado em revisões sistemáticas, com a finalidade de aprimorar a qualidade e a confiabilidade dos estudos ao estruturar as etapas de busca, triagem, elegibilidade e inclusão dos artigos científicos.

A metodologia PRISMA segue um fluxo estruturado de quatro etapas principais:

- **Identificação:** coleta de publicações em bases de dados confiáveis.
- **Triagem:** remoção de artigos duplicados e leitura inicial dos títulos e resumos.
- **Elegibilidade:** avaliação detalhada dos estudos completos conforme critérios pré-definidos.
- **Inclusão:** seleção final dos artigos mais relevantes para a pesquisa.

4.1 Representação Gráfica do Processo

A Figura 2 apresenta um fluxograma do processo de busca e seleção, ilustrando as etapas-chave desde a definição das strings de busca até a seleção final dos artigos analisados.

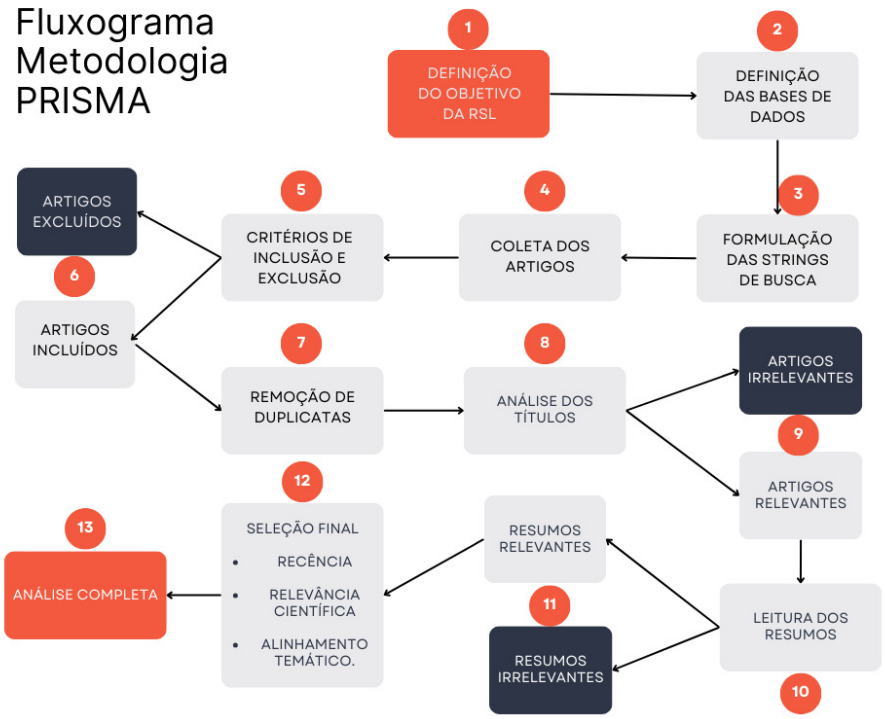

Figura 2: *Fluxograma do processo de busca e seleção dos artigos.*

4.2 Critérios de Inclusão e Exclusão

Os critérios de inclusão utilizados na revisão foram:

- Artigos publicados nos últimos cinco anos em periódicos indexados;
- Publicações que abordem diretamente o protocolo STIR/SHAKEN como solução contra *Caller ID Spoofing*;
- Estudos com metodologia clara e resultados aplicáveis ao contexto do trabalho.

Os critérios de exclusão foram:

- Estudos duplicados entre as bases pesquisadas;
- Artigos que mencionam o tema de forma superficial ou que não apresentem dados concretos sobre STIR/SHAKEN;
- Publicações indisponíveis para leitura integral.

4.3 Processo de Busca e Seleção

A busca foi realizada nas bases de dados Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), *Institute of Electrical and Electronics Engineers Xplore Digital Library* (IEEE Xplore) e *Association for Computing Machinery* (ACM), utilizando as seguintes strings:

- **String 1:** (STIR) **and** (SHAKEN);
- **String 2:** (Ataque de falsificação) **or** *(Caller ID Spoofing)* **and** (STIR/SHAKEN);
- **String 3:** (Segurança VoIP) **or** *(VoIP Security)* **and** (STIR/SHAKEN).

As etapas para a seleção dos artigos incluíram:

- Identificação de artigos relevantes nas bases mencionadas;
- Remoção de duplicatas;
- Leitura dos títulos e resumos para uma triagem inicial;
- Exclusão de artigos indisponíveis ou não relacionados ao tema;
- Análise detalhada dos artigos completos selecionados.

4.4 Organização e Análise dos Dados

Os resultados da busca inicial apresentaram uma quantidade significativa de artigos, totalizando 393 artigos, como mostrado na Tabela 1. Após a aplicação dos critérios de exclusão, cinco artigos científicos foram selecionados para compor a análise deste trabalho, representando as contribuições mais relevantes sobre o tema.

Tabela 1: *Resultados da Busca nas Bases de Dados.*

STRING DE BUSCA	**CAPES**	**IEEE Xplore**	**ACM**
(STIR) and (SHAKEN)	14	20	272
(Ataque de falsificação or *Caller ID Spoofing*) and (STIR/SHAKEN)	3	2	58
(VOIP Security or Segurança VOIP) and (STIR/SHAKEN)	1	2	21
TOTAL:	**18**	**24**	**351**

4.5 Comentários e Análise

Entre os 393 artigos identificados inicialmente, apenas cinco atenderam aos critérios de inclusão e exclusão, evidenciando uma escassez significativa de estudos científicos aprofundados sobre STIR/SHAKEN. Essa redução se deu, principalmente, pela:

- Exclusão de artigos duplicados entre as bases de dados;
- Identificação de estudos que não abordavam o tema com profundidade técnica;
- Remoção de publicações indisponíveis para análise integral.

Além disso, observou-se que, embora a base ACM apresente um volume muito maior de publicações, a maioria dos estudos não era diretamente relevante ao objetivo deste trabalho. Por outro lado, as bases CAPES e IEEE Xplore apresentaram resultados mais direcionados e tecnicamente relevantes. A discrepância observada na Figura 3 deve-se a uma inconsistência na plataforma da ACM, que resultou na indexação de artigos não relacionados ao tema pesquisado. Durante o processo de busca, verificou-se que a ACM retornou publicações em que as strings de busca utilizadas correspondiam parcial ou incidentalmente a termos contidos em títulos, resumos ou palavras-chave de artigos sem relação com o protocolo STIR/SHAKEN. Esse comportamento não foi identificado nas demais bases consultadas, sugerindo uma limitação nos algoritmos de correspondência da ACM. Dessa forma, os artigos dessa base exigiram um processo de filtragem mais criterioso para garantir a relevância dos estudos incluídos na revisão.

Dessa forma, os cinco artigos selecionados representam as contribuições mais robustas e detalhadas sobre o tema, sendo complementados por fontes secundárias, como relatórios técnicos e páginas de organizações relevantes para o campo.

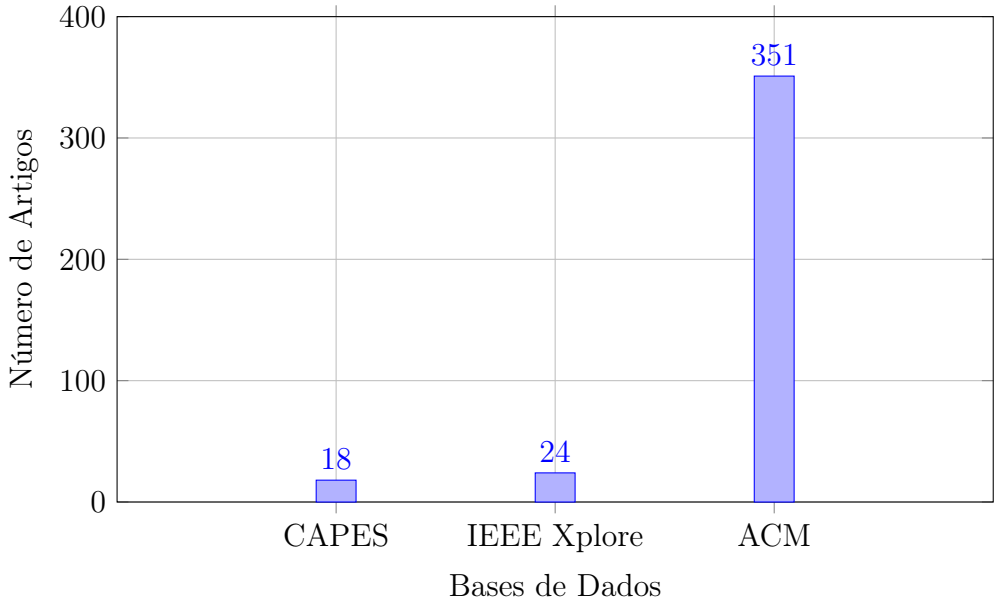

Figura 3: *Distribuição de Artigos nas Bases de Dados.*

5 Resultados e Discussão

Nesta seção, é apresentada uma análise detalhada dos cinco artigos selecionados na revisão sistemática da literatura. Cada artigo é discutido separadamente, com o objetivo de destacar suas contribuições específicas, além de identificar as principais lacunas e desafios no contexto do protocolo STIR/SHAKEN.

5.1 Artigo 1: Spoofing Against Spoofing

O artigo de Wang et al. (2023) propõe uma abordagem inovadora para combater a falsificação do identificador de chamadas, introduzindo o método *Caller ID Verification* (CIV) como alternativa ao STIR/SHAKEN. Este método elimina a dependência da PKI e utiliza um processo de autenticação baseado na interação entre o chamador e o receptor, garantindo maior segurança na verificação da identidade da chamada. Entre os principais achados, destacam-se:

- A capacidade do CIV de autenticar chamadas em redes IP e não-IP, como SS7;
- A implementação prática em VoIP, redes celulares e telefones fixos;
- A proposta de integrar o CIV em *clouds* de telecomunicações como serviço, oferecendo maior escalabilidade.

Wang et al. (2023) também identificam que o CIV apresenta custos reduzidos em comparação ao STIR/SHAKEN, tornando-o uma solução promissora para mercados emergentes.

5.2 Artigo 2: Strategic Spam Call Control and Fraud Management

Koilada (2019) discute a adoção do STIR/SHAKEN nos Estados Unidos, destacando o impacto da regulamentação TRACED Act na redução de fraudes telefônicas. Este estudo apresenta:

- A eficácia do protocolo na autenticação de chamadas e na redução de *robocalls*;
- As barreiras enfrentadas pelas operadoras, como custos de implementação e integração com redes legadas;
- A importância de estratégias complementares para mitigar fraudes, incluindo medidas educacionais para consumidores.

Embora o STIR/SHAKEN seja eficaz em chamadas locais, o autor aponta limitações significativas em chamadas internacionais devido à falta de adesão global.

5.3 Artigo 3: How to Shut Down Robocallers

McEachern e Burger (2019) oferecem uma visão prática do impacto do STIR/SHAKEN, enfatizando sua capacidade de fechar brechas exploradas por golpistas. O estudo destaca:

- O aumento significativo no volume de *robocalls*, totalizando 85 bilhões em 2018;
- A eficácia do protocolo em chamadas locais, mas sua incapacidade de proteger redes não-IP;

- A necessidade de regulamentações internacionais para ampliar sua aplicação.

Os autores também reforçam a importância de ferramentas complementares, como bloqueadores de chamadas, para aumentar a eficácia do STIR/SHAKEN.

5.4 Artigo 4: Dynamic Public Key Certificates

Chien (2021) explora o conceito de certificados dinâmicos de chave pública como alternativa ao modelo tradicional de PKI. Este estudo apresenta:

- A definição formal de certificados dinâmicos, permitindo a troca de chaves sem a necessidade de renovação frequente;
- A aplicação em redes de telecomunicações, reduzindo custos e melhorando a eficiência;
- O potencial uso em sistemas VoIP e SS7, oferecendo maior flexibilidade e segurança.

A proposta de Chien visa superar os desafios econômicos e técnicos associados à implementação do STIR/SHAKEN em larga escala.

5.5 Artigo 5: Towards Zero-Trust VoIP Architecture

Fox et al. (2023) propõem uma arquitetura *Zero-Trust* para VoIP, integrando o STIR/SHAKEN em um ambiente de teste. Este estudo foca em:

- A implementação prática de uma arquitetura segura para VoIP;
- O uso de modelos *Zero-Trust* para mitigar ataques baseados em falsificação de chamadas;
- Lições aprendidas na interoperabilidade entre operadoras e protocolos de segurança.

O estudo conclui que o STIR/SHAKEN pode ser adaptado para trabalhar em conjunto com modelos *Zero-Trust*, aumentando significativamente a segurança das telecomunicações.

6 Discussão Geral

A análise dos artigos selecionados e as informações levantadas na fundamentação teórica demonstram que o STIR/SHAKEN é uma solução promissora no combate à falsificação do identificador de chamadas e fraudes telefônicas. No entanto, sua implementação em larga escala enfrenta desafios técnicos, regulatórios e econômicos. Nesta seção, é discutido o impacto global do protocolo, com ênfase nas aplicações práticas no Brasil e nas perspectivas futuras.

6.1 Implementação do STIR/SHAKEN no Brasil

A Agência Nacional de Telecomunicações (Anatel) desempenha um papel regulador essencial na supervisão das telecomunicações no Brasil, buscando aprimorar a segurança e reduzir fraudes telefônicas. Como parte dessas iniciativas, a Anatel havia previsto para janeiro de 2024 o início da implementação do protocolo STIR/SHAKEN, denominado no Brasil como **Origem Verificada**. Embora os primeiros testes tenham sido iniciados em 2024, a implementação obrigatória foi postergada para 2025, permitindo que operadoras e demais agentes do setor realizem ajustes técnicos necessários antes de sua efetiva aplicação. Até o momento, a adesão ao sistema é voluntária, e ainda não há definição oficial sobre a obrigatoriedade do protocolo.

A implementação técnica do sistema está a cargo da ABR Telecom, responsável por operar a solução centralizada de autenticação das chamadas entre operadoras. Esse modelo permite que as prestadoras de telecomunicações adotem um padrão único de verificação, assegurando maior segurança e confiabilidade nas chamadas telefônicas (TELESÍNTESE, 2024a).

A adoção do STIR/SHAKEN no Brasil acompanha uma tendência global, sendo influenciada por regulamentações internacionais, como a TRACED Act nos Estados Unidos, que tornou obrigatória a autenticação de chamadas por meio desse protocolo (Koilada, 2019). No entanto, sua aplicação no Brasil apresenta desafios específicos, entre os quais destacam-se:

- **Interoperabilidade entre operadoras**: a adesão ao protocolo requer que todas as operadoras adotem um padrão unificado, garantindo que chamadas autenticadas sejam verificadas corretamente em qualquer rede.
- **Compatibilidade com dispositivos**: apenas dispositivos modernos, conectados às redes 4G e 5G, poderão exibir informações verificadas, como o nome da empresa, logotipo e motivo da chamada.
- **Adoção e regulamentação**: apesar do avanço da tecnologia, a Anatel ainda não definiu uma data oficial para a obrigatoriedade do protocolo, e sua adoção depende do engajamento das operadoras e da viabilidade técnica e econômica da solução.

Desde o início de 2024, a Anatel já realizou testes do Origem Verificada em mais de 30 milhões de chamadas, abrangendo operadoras, bancos e seguradoras. O lançamento oficial ocorreu no segundo semestre de 2024, com a adesão inicial de 33 operadoras. Atualmente, o volume de chamadas autenticadas contratadas já alcança 2,2 bilhões por mês, evidenciando a rápida adoção da tecnologia. No entanto, a participação no sistema continua sendo opcional, e há discussões em andamento sobre a possibilidade de tornar sua adoção obrigatória nos próximos anos (TELESÍNTESE, 2024b).

Com a progressiva desativação das redes 3G e legadas, como o SS7, o impacto dessas limitações tende a ser reduzido. A modernização da infraestrutura de telecomunicações facilitará

a adoção do Origem Verificada como um padrão de segurança essencial, contribuindo para restaurar a confiança dos consumidores nas chamadas telefônicas e reduzir significativamente fraudes e ligações indesejadas.

6.2 Impacto Global e Lições de Outras Implementações

O impacto global do STIR/SHAKEN pode ser observado em países que já implementaram a tecnologia, como os Estados Unidos e o Canadá. Nos Estados Unidos, a adoção do protocolo foi impulsionada pela TRACED Act, uma legislação aprovada em 2019 que obrigou operadoras a implementarem mecanismos de autenticação de chamadas, sob pena de sanções regulatórias (Koilada, 2019). Estudos indicam que, desde a implementação, houve uma redução significativa no volume de *robocalls* e golpes telefônicos, especialmente aqueles baseados em falsificação de números.

Entretanto, a experiência norte-americana revela desafios importantes que devem ser considerados na adoção do protocolo em outros países, incluindo o Brasil. Entre esses desafios, destacam-se:

- **Falta de adesão global**: embora eficaz dentro dos Estados Unidos e Canadá, o STIR/SHAKEN ainda não possui adoção ampla em escala internacional. Isso significa que chamadas recebidas de países que não adotaram a tecnologia continuam vulneráveis a fraudes, reduzindo a eficácia da autenticação.

- **Desafios econômicos para operadoras menores**: a implementação do protocolo requer investimentos em infraestrutura de autenticação, incluindo a adoção da PKI. Para grandes operadoras, esse custo pode ser absorvido mais facilmente, mas para pequenas prestadoras de serviços, pode representar uma barreira significativa.

- **Integração com redes legadas**: embora a tendência global seja a desativação de redes SS7 e 3G, muitos países ainda operam infraestruturas híbridas. A necessidade de soluções compatíveis para chamadas que transitam entre redes legadas e redes IP se mantém como um desafio técnico.

- **Evasão por parte de golpistas**: mesmo com a implementação do STIR/SHAKEN, fraudadores continuam explorando brechas no sistema, como o uso de chamadas originadas fora de redes autenticadas ou serviços de roteamento alternativos. Isso reforça a necessidade de uma abordagem combinada, incluindo regulamentação rígida e mecanismos complementares, como análise comportamental e monitoramento de tráfego.

Esses desafios evidenciam a importância de adaptações locais e estratégias colaborativas entre reguladores, operadoras e a indústria de telecomunicações para maximizar o impacto do protocolo. No Brasil, a experiência de países como os Estados Unidos oferece um referencial para ajustes regulatórios e para a estruturação de mecanismos que garantam a viabilidade da

adoção do Origem Verificada, considerando as particularidades do mercado nacional. Além disso, iniciativas como a possível obrigatoriedade da tecnologia para todas as operadoras podem garantir maior eficácia na proteção contra fraudes telefônicas no país.

6.3 Perspectivas Futuras

O avanço do STIR/SHAKEN dependerá de sua integração com tecnologias emergentes e da adoção de novas estratégias para ampliar sua eficiência. Uma das tendências mais promissoras é a incorporação de arquiteturas *Zero-Trust*, que adotam o princípio de não confiar automaticamente em nenhuma comunicação, exigindo verificações contínuas. Fox et al. (2023) destacam que essa abordagem pode aumentar a resiliência do protocolo contra ataques cibernéticos, ampliando sua aplicabilidade em redes VoIP e reforçando a segurança nas telecomunicações.

Outra alternativa abordada é o *Caller ID Verification* (CIV), proposto por Wang et al. (2023), que oferece uma solução viável para redes legadas. Diferente do STIR/SHAKEN, o CIV não depende de infraestrutura de PKI, utilizando um método baseado em desafios e respostas para autenticar chamadas. Esse modelo apresenta potencial para ser adotado em mercados emergentes e em regiões onde a transição para redes IP ainda é limitada.

No Brasil, espera-se que a implementação do STIR/SHAKEN, aliado a regulamentações eficazes e à modernização das redes, reduza significativamente fraudes telefônicas e chamadas abusivas. No entanto, para garantir uma adoção eficiente, será essencial a cooperação entre operadoras, reguladores e pesquisadores, a fim de superar as barreiras existentes e tornar a tecnologia acessível ao setor de telecomunicações.

7 Conclusão

Este trabalho analisou a implementação do STIR/SHAKEN, denominado Origem Verificada no Brasil, como uma solução eficaz para mitigar fraudes telefônicas e falsificação do identificador de chamadas. Sua adoção foi avaliada em diferentes contextos, identificando benefícios e desafios técnicos, econômicos e regulatórios que impactam sua implementação.

Os resultados demonstram que o protocolo é eficiente na autenticação de chamadas e na redução de *robocalls*, mas sua adoção ainda enfrenta obstáculos, especialmente devido à necessidade de interoperabilidade entre operadoras e aos custos de implementação para prestadoras menores. Além disso, a adesão global limitada compromete sua eficácia em chamadas internacionais, evidenciando a importância de regulamentações mais robustas e investimentos contínuos.

No Brasil, a iniciativa liderada pela Anatel e implementada pela ABR Telecom tem avançado gradualmente, representando um passo importante para fortalecer a segurança nas telecomunicações. Com a desativação progressiva das redes 3G e legadas SS7, a implementação do STIR/SHAKEN torna-se ainda mais relevante, pois sua integração com redes

IP eliminará barreiras técnicas que antes limitavam sua aplicação.

A evolução do setor exige o desenvolvimento de soluções complementares, como o *Caller ID Verification* (CIV) e abordagens baseadas em *Zero-Trust*, que podem ampliar a proteção contra fraudes em diferentes cenários. A cooperação contínua entre operadoras, reguladores e empresas de tecnologia é essencial para garantir a consolidação do protocolo.

Com a modernização da infraestrutura e uma regulamentação adequada, o Origem Verificada apresenta potencial para se tornar um marco na segurança das telecomunicações, contribuindo para a restauração da confiança dos usuários e para a redução significativa de fraudes e chamadas indesejadas.

8 Referências Bibliográficas

CHIEN, H. Y. *Dynamic public key certificates with forward secrecy.* 8. ed. Switzerland: MDPI AG, 2021. ISSN 2079-9292.

FOX, M. et al. Towards zero-trust voip architecture: A testbed implementation, approach, and lessons learned. In: *2023 IEEE Future Networks World Forum (FNWF).* [S.l.: s.n.], 2023. p. 1–9.

KOILADA, D. V. S. R. K. Strategic spam call control and fraud management: Transforming global communications. *IEEE Engineering Management Review*, New York, v. 47, p. 65–71, jul. 2019. ISSN 1937-4178.

MCEACHERN, J.; BURGER, E. How to shut down robocallers: The STIR/SHAKEN protocol will stop scammers from exploiting a caller ID loophole. [S.l.]: *IEEE*, 2019. p. 46–52.

TELESÍNTESE. 33 operadoras já integram o programa de chamadas de Origem Verificada, ou STIR/SHAKEN. 2024a. Disponível em: <https://www.telesintese.com.br/33-operadoras-ja-integram-o-programa-de-chamadas-de-origem-verificada-ou-stir-shaken/>. Acesso em: 24 fev. 2025.

TELESÍNTESE. Origem Verificada: chamadas contratadas chegam a 2,2 bi por mês. 2024b. Disponível em: <https://www.telesintese.com.br/origem-verificada-chamadas-contratadas-chegam-a-22-bi-por-mes/>. Acesso em: 24 fev. 2025.

TRANSNEXUS. Understanding STIR/SHAKEN Whitepaper. 2024. Disponível em: <https://transnexus.com/whitepapers/understanding-stir-shaken/>. Acesso em: 24 fev. 2025.

WANG, S. et al. Spoofing against spoofing: Toward caller id verification in heterogeneous telecommunication systems. *ACM Transactions on Privacy and Security*, New York, v. 27, n. 1, p. 1–25, 2023. ISSN 2471-2566.

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

Documento Digitalizado Ostensivo (Público)

TCC

Assunto:	TCC
Assinado por:	Annderson Weshleen
Tipo do Documento:	Termo
Situação:	Finalizado
Nível de Acesso:	Ostensivo (Público)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Annderson Weshleen Confessor de Sousa Alves**, **DISCENTE (202211210019) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE**, em 14/03/2025 20:02:21.

Este documento foi armazenado no SUAP em 14/03/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1420076
Código de Autenticação: 11a8127571