How safe is VoIP? A survey of existing security infrastructure in VoIP

Lokesh Gautam[1], Keshav Mohan[2], Aryan Chaudhary[3], Ansh Jindal[4]

[1,2,3,4] Department of Electronics and Communications, Delhi Technological University

March 2024

Abstract

As the adoption of Voice over Internet Protocol (VoIP) continues to surge, it becomes imperative to assess the security posture of this burgeoning communication medium and comprehend the array of security threats it presents. The literature survey endeavors to furnish a comprehensive analysis of prevailing VoIP infrastructures, meticulously scrutinizing their security vulnerabilities. Its overarching objective is to delineate potential avenues for fortifying the security landscape of VoIP communication channels. Through systematic inquiry, this study seeks to elucidate the intricate nuances of existing VoIP architectures, thereby facilitating an informed discourse on the requisite enhancements to bolster security measures within this domain.

1 Introduction

VoIP, or Voice over Internet Protocol, is a communication technology that has revolutionized the way we make phone calls and the way businesses operate. Voice over internet protocol (or VoIP) is a technology that enables voice calls to be transmitted over the internet using internet data packets rather than traditional phone lines. VoIP has many benefits and is now widely used in many industries.

1.1 What is VoIP?

Instead of using dedicated phone lines, voice over Internet Protocol (VoIP) converts an analogue voice signal into digital data packets (think of them as emails or videos). These packets are then sent over the internet, where they reach the recipient via an internet connection and VoIP service provider (VoIP service provider). With VoIP, you can do things like:

- Video calls are audio and video conferencing for face to face communication.
- Instant messaging is text chat and other communications features integrated into a VoIP service. Voice calls are calls made and received over a computer, mobile device, or a dedicated voice over Internet Protocol (VoIP) phone.

1.2 Factors Driving VoIP Adoption

There are several Factors that are contributing to the increase in adoption of Voice of Internet Protocol (VoIP), Such as :

- Cost-effective: VoIP calls tend to be cheaper than traditional landlines or mobile calls, particularly for long- distance communications. Businesses can drastically reduce their communication costs by transitioning to VoIP.Flexibility and scalability: Unlike traditional phone systems, VoIP services offer greater flexibility and scalability. Businesses can add or remove users, and adjust their plans accordingly. This makes VoIP an ideal choice for remote work setups, as well as for growing businesses.
- Advanced features: VoIP platforms provide more than just basic voice calls. VoIP platforms offer voice transcription, call forwarding and video conferencing capabilities, as well as integration with other business apps.
- Improved quality: Thanks to advances in internet technology, modern VoIP call quality is comparable, if not better, than traditional phone lines. Even with international calls, modern VoIP systems offer crisp, clear audio.

- Mobile integration: With the proliferation of smartphones and mobile applications, users can make and receive calls on the go. This eliminates the need to be tethered to a desk phone.

1.3 VoIP Architecture and Communication protocols

Voice over Internet Protocol (VoIP) architecture is the framework and protocols by which voice communications are transmitted over the internet. VoIP works by converting an analogue voice signal into digital data packets. These packets are then sent over IP networks. There are several important components and communication protocols involved in VoIP.

1.3.1 Endpoint

An endpoint is a device that receives or receives a VoIP call. It is also referred to as a user device or a terminal. An endpoint can be a computer, a smartphone, an IP phone, or a traditional phone with an analog telephone adapter (ATA) that converts an analog signal to a digital signal.

1.3.2 VoIP Server

VoIP servers act as central hubs in VoIP architecture, managing call setup, termination, and routing. They handle tasks such as call signaling, media processing, and user authentication. VoIP servers can include various components such as SIP (Session Initiation Protocol) servers, proxy servers, media gateways, and session border controllers (SBCs).

1.3.3 Protocols

- SIP: SIP stands for Session Initiation Protocol. It's one of the main protocols used to set up, modify, and end a VoIP session. SIP sets up communication sessions among endpoints, sets up calls, and provides features like call forwarding, conference calls, presence information, etc.
- RTP: also known as Real-Time Transport Protocol (RTP), is used to transfer data packets (audiovisual and video) between two or more endpoints during a Voice over Internet Protocol (VoIP) call. RTP is used in combination with Real-Time Control Protocol (RTCP) to provide feedback on the transmission quality and to help synchronize multimedia streams.
- H.323: H.323 is a protocol suite used for voice over Internet Protocol (VoIP) communication, although it is not as widely used as SIP. It includes various call signaling protocols, media control protocols, and data transport protocols. It is commonly used in enterprise environments and in older VoIP systems.

1.3.4 Codecs

Codecs (Coder-Decoder) are algorithms used to compress and decompress audio signals for transmission over the network. They determine the quality and bandwidth requirements of VoIP calls. Common codecs include G.711 (PCM), G.729, and Opus, each offering different trade-offs between audio quality and bandwidth consumption.

1.3.5 Network infrastructure

Voice over Internet Protocol (VoIP) communications use Internet Protocol (IP) networks, such as the internet, as well as local area networks (LANs) used by businesses to send and receive data. QoS (quality of service) mechanisms, such as traffic priority and bandwidth management, are often used to improve performance and reduce latency and packet loss.

1.4 Security concerns associated with VoIP(Voice over Internet Protocol) com- pared to traditional PSTN (Public Switched Telephone Network)

There are many benefits to VoIP over PSTN, but there are also some security risks associated with VoIP that are not present in PSTN. Here are the key differences between VoIP and PSTN:

1.4.1 Public Switched Telephone Network (PSTN)

- In order to intercept traditional phone calls, it is necessary to physically access the phone line. This makes it harder for unauthorized people to listen in on the call.
- Less sophisticated technology, PSTN uses legacy, less sophisticated technology, which may make it less susceptible to some types of attacks than VoIP.

1.4.2 Voice over Internet Protocol (VoIP)

- The security of voice over internet protocol (VoIP) calls depends heavily on internet security and the security of your service provider's infrastructure. If either of these are weak, VoIP calls can be intercepted.
- Voice over Internet Protocol (VoIP) systems have a wider "attack surface" than voice over PSTN (voice over internet protocol). This means that there are more entry points for attackers to take advantage of, such as insecure networks, software bugs, and user logins.
- Increased risk of attacks, Some of the most common security threats related to VoIP include:
  - Call Interception, Call Spoofing, Denial of Service (DoS) Attacks, Malware and Viruses
  - Call Interception, Hackers can intercept calls and eavesdrop on conversations. Call Spoofing is when malicious actors pretend to be legitimate callers. This can lead to fraud and identity theft.
  - Call spoofing (Call Spoofing) is when a malicious actor pretends to be a legitimate caller.
  - Denial of Service Attacks (DoS), These are attacks where a VoIP system is overloaded with traffic, making it unavailable to legitimate users.
  - Malware and viruses,Security vulnerabilities in VoIP systems allow malware and viruses to gain access to sensitive information.

PSTN is Not Immune, Traditional phone lines are generally more vulnerable to physical interception, but most reliable VoIP providers have various security measures in place to protect calls, including encryption and firewalls, as well as user authentication. To sum up, VoIP has its pros and cons, and PSTN has its cons. For VoIP, you need to choose a good provider, have strong security protocols in place, and stay on top of ever-changing cyber threats.

1.5 The purpose of the literature review

The primary objective of conducting a comprehensive literature review is to delve into the intricacies of Voice over Internet Protocol (VoIP) and its prevailing framework while scrutinizing the accompanying security proto- cols implemented amidst its burgeoning utilization. The overarching goal is to identify avenues for augmenting these security measures without detracting from the service's quality. By meticulously examining existing literature, this study aims to pinpoint research lacunae pertaining to the fortification of VoIP systems and the establishment of a robust infrastructure ensuring their security. Through this thorough survey, insights can be gleaned to bridge these identified gaps, thereby fostering a more resilient and safeguarded environment for Voice over Internet Protocol operations.

2 Literature Review

In the extensive expanse of scholarly literature, a multitude of studies have been devoted to the comparative analysis of diverse VoIP channels, the intricate examination of security parameters inherent in existing VoIP networks, the exploration of methodologies for enhancing security within VoIP channels through the application of established encryption techniques, and the dynamic evolution and restructuring of VoIP architecture. Within the purview of this comprehensive literature review, a thorough and systematic analysis has been conducted across these multifaceted domains of research. The primary objective underlying this rigorous examination is to discern and elucidate the persistent deficiencies and challenges that continue to characterize modern-day VoIP systems. Through a nuanced and discerning investigation, the overarching aim is to delineate pragmatic and efficacious strategies aimed at mitigating these identified challenges and shortcomings. Such efforts are poised to contribute significantly to the ongoing refinement and fortification of contemporary VoIP infrastructures, thereby fostering enhanced reliability, security, and functionality within the realm of voice communication over internet protocol networks.

2.1 Security threats and vulnerabilities in existing VoIP systems

Security threats and vulnerabilities in existing VoIP systems pose significant risks to communication integrity and confidentiality. Common threats include interception of voice data, eavesdropping, unauthorized access to VoIP servers, and denial-of-service (DoS) attacks targeting VoIP infrastructure. Malicious actors may exploit vulnerabilities in VoIP protocols and implementations, such as SIP (Session Initiation Protocol) or RTP (Real- Time Transport Protocol), to intercept or manipulate calls, leading to information leakage or service disruption. Additionally, inadequate authentication mechanisms and weak encryption practices can leave VoIP systems susceptible to unauthorized access and data breaches. Moreover, emerging threats such as voice phishing

(vishing) and voice spamming further exacerbate security concerns in VoIP environments. To mitigate these risks, robust security measures, including encryption, access controls, intrusion detection systems, and regular security audits, are essential for safeguarding VoIP systems against evolving threats.

2.1.1 Security Threats in Collaborative Cyber Defense Efforts

- Operating under the assumption of a threat model wherein two peers aim to exchange information to establish collaborative cyber defense mechanisms.
- Identified threats include: Malicious control of network infrastructure, enabling the capture, dropping, or modification of communications. Potential attacks leveraging limited computational power and/or storage resources.
- Adversaries possessing capabilities such as deep-packet inspection, albeit restricted to applying them at 'full' wire speed for short observation windows.

2.1.2 Issues with Authentication Mechanisms

- The original authentication mechanism for SIP was HTTP digest-based, which was not strong enough to provide the required security.
- Various authentication mechanisms such as hashing, nonce-based authentication, password, smartcard, and ECC were introduced, but they were found to be vulnerable to various types of attacks.
- Several proposed authentication and key establishment schemes were found to have limitations and vulnerabilities, leading to the need for more robust solutions.

2.1.3 Caller ID spoofing attacks

- This form of attack involves the deliberate manipulation of caller identification information to misrepresent the identity of the caller. Perpetrators exploit vulnerabilities within VoIP protocols to falsify caller information, enabling them to impersonate legitimate entities or obscure their true identities.
- Caller ID spoofing not only undermines the integrity of communication channels but also facilitates various malicious activities, including phishing scams, social engineering attacks, and fraudulent transactions.
- Given its potential for exploitation and its implications for trust and security in VoIP environments, comprehensive research and mitigation strategies are imperative to address the challenges posed by Caller ID spoofing attacks.

2.1.4 Man in the Middle attacks

- These attacks involve an adversary intercepting communication between two parties, potentially altering or eavesdropping on the exchange without the knowledge of the communicating entities.
- In the context of VoIP, MitM attacks can lead to various security breaches, including call interception, unauthorized access to sensitive information, and even the injection of malicious content into the communication stream.
- Understanding and mitigating the risks posed by MitM attacks is crucial for maintaining the confidentiality, integrity, and authenticity of VoIP communications.

2.1.5 MAC address spoofing

- MAC address spoofing in VoIP entails the deliberate alteration of the Media Access Control (MAC) address associated with VoIP devices.
- This manipulation serves to obscure the true identity of the device and potentially evade network security measures. Through this practice, malicious actors can attempt to gain unauthorized access to VoIP networks, intercept communications, or launch various forms of attacks.
- Understanding the nuances and implications of MAC address spoofing is crucial for devising effective security strategies within VoIP environments, as it represents a significant threat to the integrity and confidentiality of voice communication over IP networks.

2.2 Existing security standards and best practices for VoIP deployments and their Efficiencies

Numerous contributions have been made in advancing the VoIP infrastructure as well as increasing the security of connections over VoIP and research regarding the same such as Chebyshev chaotic map-based efficient authen- tication scheme for secure access of VoIP services through SIP[7] , Covert Communication over VoIP Streaming Media with Dynamic Key Distribution and Authentication[10] , Optimizing Packet Scheduling and Path Selection for Anonymous Voice Calls[11], VoIP traffic in VPN tunnel via Flow Spatio-Temporal Features[11], VoIP network covert channels to enhance privacy and information sharing[13], Security Enhancement of SIP Protocol in VoIP communication[14]. Some of the advancements and work done as well as the existing VoIP architecture are:

2.2.1 Security Solutions with Privacy-Enhancing Technologies (PET) in Collaborative Cyber Defense

- Use of SIP (Session Initiation Protocol) for call management, media stream initialization, and voice data transfer. Exploration of VAD (Voice Activity Detection) optimization in User Agents (UAs) to halt transmission during speech pauses, leading to bandwidth conservation. Discussion on challenges associated with implementing efficient VAD strategies without compromising conversation quality through additional distortions or delays.
- Addressing the necessity for injection/extraction of secrets and creation of fake silence packets adhering to recognizable templates for covert communication. Emphasis on preserving features of the entire VoIP conversation while transmitting secret information through a covert channel.
- Dynamic subdivision of information into chunks to fit into Protocol Data Units (PDUs) generated by the RTP layer. Spoofing certain fields and adjusting values in RTP packets to prevent disruption of the VoIP conversation.
- Particularly focusing on privacy-enhancing technologies (PET) within the context of collaborative cyber defense. Emphasizing on the necessity of advanced techniques to enforce privacy, aiming to mitigate the repercussions of counterattacks and thwart the contamination of data exchanged among Law Enforce- ment Agencies (LEAs) or within distributed security frameworks, framework designed for implementing a steganographic communication service, which is accessible via a generic virtual network interface.
- This service can be utilized for tunneling other protocols, enhancing privacy measures. The frame- work facilitates full-duplex communications and assesses the ramifications of embedding data within silence/talkspurt patterns, analyzing factors such as delay and resource availability.

2.2.2 Packet Scheduling and Path Selection for Anonymous Voice Calls

David Schatz, Michael Rossberg, and Guenter Schaefer in their paper[1] suggests 2 ways to enhance the security of communication over Voice over Internet Protocol

- Onion Routing: The paper suggests using onion routing, similar to the approach implemented by Tor, to provide anonymous VoIP. This involves splitting application data into uniform-sized packets, encrypting them in multiple layers, and forwarding them across relays. By setting up circuits beforehand, onion- encryption of voice packets only requires symmetric ciphers, minimizing processing delay.
- Yodel Protocol: The Yodel protocol is proposed as a method to provide strong relationship anonymity for VoIP. It involves synchronizing the start and end time of calls, grouping voice packets in communication rounds, and allowing for batch processing. This helps in defeating watermarking attacks that drop packets and ensures strong relationship anonymity.

Efficiencies of these methods are evaluated in terms of Quality of Service (QoS) and Efficiency. The paper discusses that by minimizing latency, the theoretical limits of the approach can be evaluated, and the lower bounds for end-to-end latency are expected to be below 400 ms. Additionally, probabilistic path selection modeled by the proposed methods results in mixes handling a total number of circuits proportional to their capacity, leading to low processing/forwarding bottlenecks and efficient network usage.

2.2.3 Secure communication over VPN tunnels

- Implementation of encryption protocols such as SSL/TLS, IPSec, and L2TP to ensure secure communi- cation over VPN tunnels.

- Utilization of encryption to obfuscate the content of VoIP communication, enabling evasion of firewalls and Network Address Translation (NAT) constraints. Guaranteeing the security of sensitive communication over potentially compromised Internet infrastructure through encryption.
- The effectiveness of VPNs in providing secure communication for remote users is acknowledged, as they create a secure tunnel between the user's device and the Internet, preventing traffic from being spoofed, sniffed, or censored.
- The identification of VPN-tunneled traffic presents a significant challenge due to packet-level encryption. The implementation of encryption protocols like SSL/TLS, IPSec, and L2TP at the application, network, or data link layers adds complexity to VPN traffic analysis.

2.2.4 Donar, Anonymous VoIP over Tor

In their publication, titled "Donar: Anonymous VoIP over Tor,"[8] the authors delineate a novel approach to the integration of VoIP technology with the Tor network, introducing a methodology termed "Donar."

- DONAR enables anonymous VoIP with good quality-of-experience (QoE) over Tor by addressing the challenges of meeting VoIP networking requirements within the Tor network.
- It utilizes active performance monitoring, dynamic link selection, adaptive traffic scheduling, and redun- dancy at no extra bandwidth cost. DONAR spreads VoIP traffic over several links, enabling high QoE with latency remaining under 360 ms for 99% of VoIP packets during most calls.

3 Key Finding and Analysis

Through this comprehensive literature review, we have gained insight into the operational mechanisms of Voice over Internet Protocol (VoIP), including its architectural frameworks and operational dynamics. The review has underscored the increasing adoption of VoIP technology and the imperative for establishing secure and robust connections within its framework. Furthermore, our examination has elucidated the myriad security threats confronting VoIP systems, alongside recent innovations aimed at bolstering their architectural integrity to mitigate such risks. Despite notable advancements, our analysis has also identified persistent research gaps that warrant attention to ensure the secure deployment of VoIP systems in practice.

3.1 The most notable security solutions and emerging research trends

Voice over Internet Protocol (VoIP) has emerged as a prominent communication medium, offering cost-effective and versatile voice communication over internet networks. However, with its increasing adoption comes the critical imperative to ensure the security and integrity of VoIP communication channels. This literature review aims to comprehensively analyze the evolving landscape of VoIP security, highlighting notable advancements, emerging trends, and pivotal contributions in enhancing the security of VoIP deployments.

3.1.1 Overview of Emerging Trends and Contributions

- A plethora of recent research endeavors has focused on augmenting the security of VoIP services through innovative approaches and technologies. Notable additions to the VoIP ecosystem include authentication schemes such as the Chebyshev chaotic map-based efficient authentication scheme for secure access of VoIP services through SIP. Moreover, solutions like Donar: Anonymous VoIP over Tor have garnered attention for their efficacy in safeguarding user anonymity and mitigating security threats inherent in VoIP communications.
- Additionally, advancements in covert communication techniques, such as VoIP network covert channels, and optimization strategies for packet scheduling and path selection in anonymous voice calls, underscore the diverse approaches to bolstering VoIP security. Furthermore, initiatives like Covert Communication over VoIP Streaming Media with Dynamic Key Distribution and Authentication represent innovative endeavors towards enhancing the confidentiality and integrity of VoIP communication channels.

3.1.2 Trend Towards Encryption and Alternative Architectures

- A prevailing trend in the realm of VoIP security pertains to the inclination towards enhancing encryption protocols and exploring alternative deployment architectures. Many recent developments emphasize the utilization of robust encryption mechanisms to fortify the confidentiality of VoIP communications. How- ever, concerns regarding the degradation of service quality and latency spikes associated with enhanced encryption techniques underscore the need for a balanced approach in security implementation.

- Furthermore, there is a notable shift towards deploying VoIP over existing architectures such as Virtual Private Networks (VPNs) or Onion Routing (TOR). The rationale behind this trend lies in the ability of these architectures to provide secure communication channels without significantly compromising quality of service or introducing latency spikes. By leveraging VPNs or TOR for VoIP deployment, organizations can mitigate security risks associated with conventional VoIP infrastructure, such as MAC address spoofing and man-in-the-middle attacks.

3.1.3 Donar: A Pivotal Contribution to VoIP Security

- Among the noteworthy contributions to enhancing VoIP security, Donar stands out as a pivotal innova- tion. By leveraging the existing architecture of TOR, Donar facilitates the deployment of VoIP over a secure and anonymized network, thereby mitigating a myriad of security threats inherent in traditional VoIP infrastructure. Notably, Donar addresses vulnerabilities such as MAC address spoofing, man-in-the- middle attacks, and authentication issues by ensuring anonymous selection of relay nodes and obfuscating data packet paths. This approach eliminates the potential for interception and tampering of VoIP communications, enhancing overall security and privacy.

In conclusion, the evolving landscape of VoIP security is characterized by a diverse array of advancements, trends, and contributions aimed at fortifying the confidentiality, integrity, and availability of VoIP communi- cation channels. From innovative authentication schemes to covert communication techniques and alternative deployment architectures, the realm of VoIP security continues to evolve to meet the evolving threat landscape. Notably, solutions like Donar exemplify the potential of leveraging existing infrastructure to enhance VoIP security without compromising service quality. Moving forward, further research and development efforts will be pivotal in addressing remaining challenges and ensuring the continued security of VoIP deployments in an increasingly interconnected world.

3.2 Continued research necessary to address crucial security challenges

- Authentication Mechanisms: Developing robust authentication mechanisms that can effectively verify the identities of users and devices within VoIP networks is essential. Current authentication methods may be susceptible to various attacks, including spoofing and impersonation, highlighting the need for enhanced authentication protocols.
- Encryption Techniques: While encryption plays a crucial role in safeguarding VoIP communications, there is a need for ongoing research to optimize encryption techniques. Balancing the trade-off between security and performance is critical to ensure that encryption does not degrade the quality of service or introduce latency spikes.
- Covert Communication Detection: Detecting covert communication channels within VoIP networks re- mains a significant challenge. Further research is needed to develop advanced techniques for identifying and mitigating covert communication channels, which could be exploited by malicious actors for surreptitious information exchange.
- Anonymity and Privacy: Preserving user anonymity and privacy in VoIP communications is paramount. Future research should focus on enhancing anonymity protocols and privacy-preserving mechanisms to mitigate the risk of unauthorized surveillance and data breaches.
- Network Infrastructure Security: Strengthening the security of underlying network infrastructure, includ- ing routers, switches, and gateways, is essential for protecting VoIP communications against external threats. Research efforts should explore innovative approaches to mitigate vulnerabilities and safeguard network elements from exploitation.

By addressing these critical security challenges through rigorous research and development efforts, it is possible to enhance the security posture of VoIP deployments and ensure the integrity, confidentiality, and availability of voice communication over IP networks.

4 Conclusion

With the escalating adoption and demand for Voice over Internet Protocol (VoIP) technology, it becomes paramount to cultivate a comprehensive understanding of contemporary communication modalities facilitated by VoIP, along with the attendant security vulnerabilities. The impetus behind conducting this literature review is to meticulously scrutinize and assess the advancements aimed at fortifying VoIP deployments' security landscape. Through this scholarly inquiry, a nuanced comprehension emerges, elucidating potential strategies and contributions directed towards enhancing the security posture of VoIP implementations.

The literature review underscores the fundamental imperative of ensuring the security and integrity of VoIP communication channels amidst their widespread adoption. By delving into existing research and contributions, discernible trends and emergent solutions pertinent to VoIP security surface. A salient observation gleaned from this review is the proposition of leveraging infrastructures based on onion routing or deploying VoIP over existing onion routing frameworks as viable avenues towards bolstering security.

The allure of onion routing lies in its capacity to provide anonymity and secure connections without com- promising the quality of service or incurring latency spikes. This approach aligns with the overarching objective of fortifying VoIP deployments' security landscape, offering a promising avenue towards addressing prevalent security risks. By harnessing the inherent capabilities of onion routing, VoIP communications can be shielded from potential eavesdropping, interception, and tampering, thereby engendering a more resilient and secure communication milieu.

Furthermore, deploying VoIP over existing onion routing infrastructures presents a pragmatic solution to augmenting security without necessitating extensive overhauls or disruptions to existing VoIP deployments. Leveraging the robust anonymity and security features inherent in onion routing frameworks, VoIP communi- cations can traverse networks clandestinely, mitigating the risk of malicious interception or tampering.

The appeal of these approaches lies in their ability to proffer comprehensive security without compromising the efficiency or reliability of VoIP communication channels. By circumventing traditional security vulnera- bilities associated with conventional VoIP architectures, onion routing-based solutions offer a paradigm shift towards safeguarding sensitive voice communications in an increasingly interconnected and digitally reliant landscape.

In essence, this literature review underscores the imperative of fortifying VoIP deployments' security posture in tandem with their escalating adoption and utilization. Through a judicious analysis of existing research and contributions, the proposition of leveraging onion routing infrastructures emerges as a promising strategy to address prevailing security risks. By embracing these innovative approaches, stakeholders can engender a more secure and resilient VoIP ecosystem, safeguarding sensitive communication channels against malicious exploits and ensuring the continued viability and trustworthiness of VoIP technology in contemporary communication paradigms.

5 Future Work

Despite the deployment of the Donar architecture over the Tor network, challenges persist due to the limited capacity of Tor, which accommodates only approximately 7000 relay nodes. This constraint poses a significant obstacle to deploying a substantial portion of modern VoIP traffic over this infrastructure. Consequently, there is a pressing need to explore avenues for addressing this limitation and expanding the scalability of secure VoIP deployments.

Future research endeavors should not only focus on augmenting the existing Tor infrastructure but also on exploring alternative approaches, such as developing or deploying independent infrastructures on dedicated servers. By diversifying the scope of research to encompass both enhancements to Tor and the creation of independent infrastructures, opportunities arise to surmount the limitations posed by the current reliance on Tor for secure VoIP communications.

Amendments to the Tor infrastructure may involve optimizing network resources, increasing relay node capacity, and enhancing scalability to accommodate the growing demand for secure VoIP services. Simultaneously, efforts to develop independent infrastructures can explore novel architectures and protocols tailored specifically for VoIP communication, thereby circumventing the constraints imposed by Tor's limited capacity.

By pursuing a dual-pronged approach that encompasses both enhancing Tor and exploring independent infrastructures, the scope for future research expands significantly. This comprehensive strategy offers potential solutions to the scalability challenges inherent in secure VoIP deployments, paving the way for the realization of robust and resilient communication channels in the digital era.

6 References

[1] David Schatz, Michael Rossberg, and Guenter Schaefer. 2021. Optimizing Packet Scheduling and Path Selection for Anonymous Voice Calls. In The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3465481.3465768

[2] Levi Perigo, Rahil Gandotra, Dewang Gedia, Moiz Hussain, Praniti Gupta, Shirin Bano, Vineet Kulkarni. 2020. VOIP SECURITY: A PERFORMANCE AND COST-BENEFIT ANALYSIS. In IT in Industry, vol. 8, no.2, 2020

[3] Abir El Azzaoui, Min Yeong Choi, Chang Hoon Lee, and Jong Hyuk Park. 2022. Scalable Lightweight Blockchain-Based Authentication Mechanism for Secure VoIP Communication. In Human-centric Computing and Information Sciences (2022) 12:08 DOI: https://doi.org/10.22967/HCIS.2022.12.008

[4] Mashari Alatawi and Nitesh Saxena. 2023. SoK: An Analysis of End-to-End Encryption and Authentication Ceremonies in Secure Messaging Systems. In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), May 29-June 1, 2023, Guildford, United Kingdom. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3558482.3581773

[5] Nur Khairani Kamarudin, Nur Syafiqa Bismi, Nurul Hidayah Ahmad Zukri, Mohd Faris Mohd Fuzi4, Rashidah Ramle. 2020. Network Security Performance Analysis of Mobile Voice Over IP Application (mVoIP): Kakao Talk, WhatsApp, Telegram and Facebook Messenger. In Journal of Computing Research and Innovation (JCRINN) Vol. 5 No. 2 (2020) eISSN: 2600-8793 https://doi.org/10.24191/jcrinn.v5i2.136

[6] Quentin Dufour. High-throughput real-time onion networks to protect everyone's privacy. Networking and Internet Architecture [cs.NI]. Universit´e Rennes 1, 2021. English. NNT : 2021REN1S024. Tel-03356197

[7] Mahor, V.K., Padmavathy, R. and Chatterjee, S. (2022) 'Chebyshev chaotic map-based efficient authen- tication scheme for secure access of VoIP services through SIP', Int. J. Security and Networks, Vol. 17, No. 1, pp.39–47.

[8] Y´erom-David Bromberg, Quentin Dufour, Davide Frey, and Etienne Rivi`ere. 2022. "Donar: Anonymous VoIP over Tor". In19th USENIX Symposium on Networked Systems Design and Implementation. It was presented at the symposium held on April 4–6, 2022, in Renton, WA, USA. The open access to the proceedings is sponsored by USENIX.

[9] Faiz Ul Islam, Guangjie Liu, Jiangtao Zhai, and Weiwei Liu. 2021. "VoIP Traffic Detection in Tunneled and Anonymous Networks Using Deep Learning." In Volume 9, IEEE Explore, 2021.

[10] Jinghui Peng, Shanyu Tang, FBCS. 2020. Covert Communication over VoIP Streaming Media with Dynamic Key Distribution and Authentication. In IEEE Transactions on Industrial Electronics, DOI 10.1109/TIE.2020.2979567

[11] Faiz Ul Islam, Guangjie Liu, and Weiwei Liu. 2020. Identifying VoIP traffic in VPN tunnel via Flow Spatio-Temporal Features. In Mathematical Biosciences & Engineering · July 2020 DOI: 10.3934/mbe.2020260

[12] PETR KADLEC. 2021. Replication of attack on VoIP end-to-end encrypted messengers. In Bachelor's Thesis, for Faculty of Informatics, at Masaryk University.

[13] Jens Saenger, Wojciech Mazurczyk a, J¨org Keller, Luca Caviglione. 2020. VoIP network covert channels to enhance privacy and information sharing. In Future Generation Computer Systems 111 (2020) 96–106, https://doi.org/10.1016/j.future.2020.04.032

[14] Hussein Sudi lema, Fatuma Simba, Joseph Cosmas Mushi. 2023. Security Enhancement of SIP Protocol in VoIP Communication. In JICTS volume 1(2) Pages 71-92, DOI : https://doi.org/10.56279/jicts.vli2.32