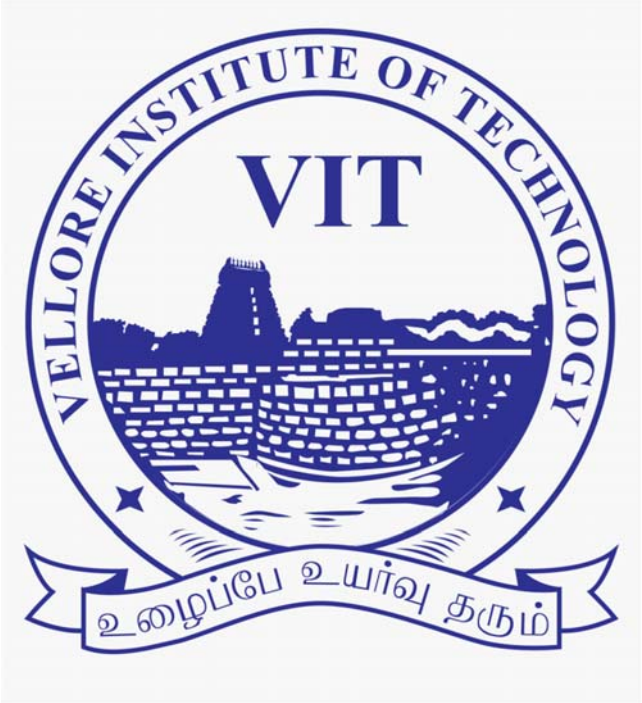
Voice over IP is a real-time interactive audio/video application



Vellore Institute of Technology, Vellore

Data Communication and Computer Networking

24MCA0258 – JANHAVI ZAMBRE

Abstract

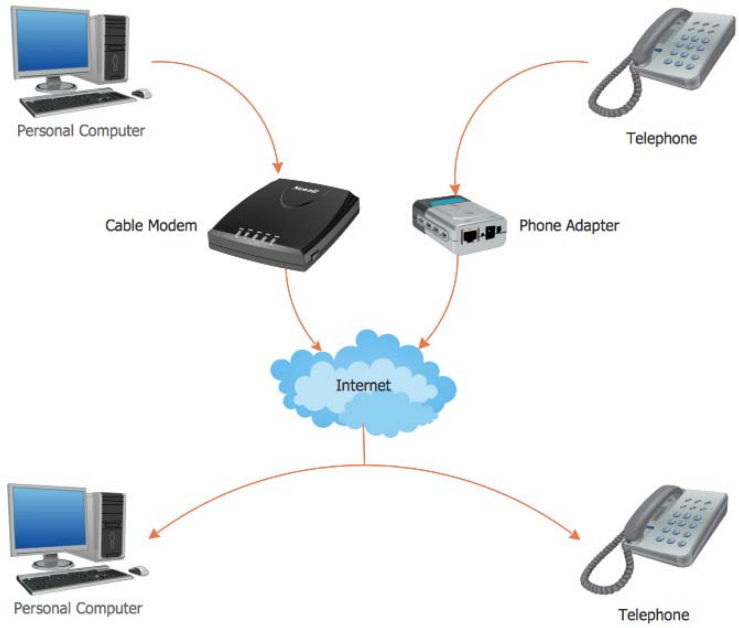
Voice-over-Internet Protocol (VoIP) technology has seen widespread adoption due to its ability to deliver communication services over the internet efficiently. The papers examined explore various aspects of VoIP, including forensics in encrypted network traffic, call admission control (CAC) in 5G and WiFi networks, WebRTC platforms, and general VoIP protocols and challenges. These studies propose frameworks and methodologies to tackle issues like encryption, real-time communications, and QoS optimization in VoIP. By employing experimental setups, they investigate call quality, encryption challenges, and system optimization using tools such as Wireshark and codec adjustments. Ultimately, these efforts contribute to improving VoIP security, efficiency, and reliability across different applications. We provide a comparative analysis of SOLSR protocol, SIP protocol, WEBRTC protocol, its QoS performance for VoIP in disaster-prone scenarios, and security concerns such as eavesdropping, denial of service (DoS) attacks, and spoofing. Based on the literature, the paper highlights emerging trends in VoIP, particularly with the growing use of 5G networks and cloud-based services. The paper concludes by recommending improvements in VoIP security protocols to enhance system resilience in high-risk environments.

Introduction

VoIP technology has transformed communication by leveraging the internet for voice and multimedia transmission. Traditional Public Switched Telephone Networks (PSTN) have given way to VoIP, which is cost-effective and scalable. Applications of VoIP range from real time audio and video personal communication to enterprise-level systems and disaster management solutions, where the ability to communicate in the absence of conventional infrastructure is critical. Key to VoIP's functionality are the protocols that ensure voice data is efficiently transmitted, compressed, and decoded. Among these, SIP (Session Initiation Protocol) and SOLSR (Secure Optimized Link State Routing) are pivotal for establishing and managing communication sessions (3) (2).

The SOLSR protocol, used primarily in disaster-prone areas, ensures secure communication over ad-hoc networks, like mobile ad-hoc networks (MANET), which are highly beneficial in emergency scenarios. Additionally, the study of compression algorithms (codecs) such as G.711 and G.729 has shown that VoIP can effectively reduce bandwidth usage while maintaining communication quality (5) (2).

Working of VoIP



Voice over Internet Protocol (VoIP) works by converting voice signals into digital data packets, which are transmitted over the internet instead of traditional phone lines. Here's a simplified breakdown of how it functions:

1. **Call Initiation:** When a user makes a call, the voice is captured by a microphone and converted into digital data.
2. **Packetization:** The digital voice data is broken down into small packets.
3. **Transmission:** These packets are sent over the internet to the recipient using routers and servers.
4. **Reassembly:** At the destination, the packets are reassembled into their original sequence.
5. **Conversion Back to Audio:** The digital data is then converted back into voice and played through the recipient's speaker.

This process allows real-time communication with flexibility, lower costs, and support for additional features like video and messaging.

Methodology

The study also reviews the security concerns associated with VoIP, focusing on vulnerabilities such as eavesdropping, spoofing, and denial of service attacks. Protocols like SIP and H.323 are compared for their efficiency in handling these security issues. This analysis also delves into the role of codecs in managing bandwidth and maintaining voice quality across different network configurations (5) (2).

The methodology for this review involves a comparative study of different VoIP protocols and their performance in terms of security, Quality of Service (QoS), and practical application in disaster scenarios. The SOLSR protocol is tested on a network of Raspberry Pi devices to simulate an ad-hoc network used in emergency communication (12). Parameters such as throughput, delay, jitter, and packet loss were evaluated using the Iperf software under various connectivity scenarios (3).

SIP (Session Initiation Protocol)

• **Usage:** Primarily designed for initiating, maintaining, and terminating real-time sessions such as VoIP.

• **Strengths:** Extensible, widely adopted for voice and video communications, supports mobility.

• **Weaknesses:** Susceptible to security threats, such as DoS attacks, and can struggle with NAT traversal.

SOLSR (Secure OLSR)

• **Usage:** A routing protocol in mobile ad-hoc networks (MANETs), used for secure link-state routing.

• **Strengths:** Optimized for dynamic network topologies, efficient in low-latency environments, includes security features.

• **Weaknesses:** Not designed for session management; can suffer from computational overhead due to security mechanisms.

Experimental Data Collection

To deepen the understanding of VoIP performance metrics, we also incorporated experimental data from practical VoIP deployments and testing environments, sourced from research papers and datasets. The performance of different VoIP configurations was evaluated using Session Initiation Protocol (SIP) and Web Real-Time Communication (WebRTC). Several parameters, including delay, jitter, and packet loss, were measured under varied network conditions to simulate real-world usage (1).

• **Experiment:** Jitter and Packet Loss Analysis

• Data was gathered from a study that conducted VoIP testing using Asterisk PBX server. Using G.711-ULaw voice codec, the researchers set up a test environment with 4 clients, measuring jitter and packet loss using tools like NISTNet and Wireshark (1). The network conditions were simulated by introducing packet delay variations and limiting bandwidth, and the effects on MOS scores were measured. The table below presents a summary of the results.

Parameter	Average Value	Impact on QoE
Jitter	18 ms	Noticeable delay, lower call quality
Packet Loss	1.5%	Minor distortion, reduced clarity
Mean Opinion Score	3.8	Moderate quality, acceptable for non-critical use (1)

Experiment: Real-Time Transport Protocol (RTP) Performance

In another study, researchers simulated a VoIP network using OPNET Modeler to measure the performance of RTP for video and audio communication (8). The testbed included RTP over UDP, with and without encryption. The focus was on packet delay, bandwidth usage, and the impact of encryption on real-time traffic. The findings indicated that enabling encryption increased packet delay by an average of 23 ms, which had a significant impact on call quality under high-traffic conditions.

VoIP Security Challenges

VoIP networks are vulnerable to various security threats due to their reliance on the internet. Common attacks include Denial of Service (DoS), eavesdropping, and packet manipulation (4). Moreover, the lack of encryption in many VoIP protocols, such as SIP and RTP, makes these systems particularly susceptible to intrusions.

• **Eavesdropping:** Attackers intercept VoIP communication by sniffing traffic (4).

• **Caller ID Spoofing:** Malicious users manipulate caller information to impersonate legitimate users (4).

• **DoS Attacks:** Attackers flood VoIP networks with traffic, overwhelming servers and degrading service quality (4).

Comparative Critical Analysis

Protocol Comparison: SIP vs. SOLSR

The SOLSR protocol, designed for disaster recovery and emergency management, is optimized for routing in ad-hoc networks where the infrastructure may be unstable or non-existent. This makes SOLSR particularly well-suited for VoIP communication, as it uses secure link-state routing that adapts dynamically to changing network conditions (3). On the other hand, SIP is more commonly used in enterprise environments and supports a wide range of multimedia communications beyond just voice. However, SIP has limitations when it comes to mobility and handling the dynamic network reconfigurations required in disaster scenarios (2).

QoS Evaluation

SOLSR excels in environments with high latency and jitter, making it ideal for handling voice traffic in critical applications where network conditions are unstable. It maintains consistent throughput and minimizes packet loss, which is crucial for ensuring voice quality (3). In contrast, SIP while widely used—tends to perform poorly under such challenging conditions, experiencing higher levels of jitter and delay that degrade communication quality (5).

Security Concerns

Both SOLSR and SIP are vulnerable to security threats such as eavesdropping and denial of service (DoS) attacks. However, SOLSR offers better protection against rogue nodes due to its inherent routing security, which is particularly important in emergency scenarios. SIP, by relying on centralized servers and being more susceptible to spoofing, is more vulnerable in insecure environments (5) (2).

Targeted Adversarial Voice over IP Network

The COVID-19 pandemic led to a surge in VoIP and video conferencing usage, yet little research has focused on adversarial attacks through these channels. This paper introduces TAINT—the first targeted adversarial attack on commercial speech recognition systems over VoIP. VoIP poses unique challenges like signal degradation and random noise, but these are addressed through reverse engineering and a noise-resilient gradient estimation method. The attack was tested on four major speech recognition platforms across five popular VoIP software, successfully bypassing detection in even the most difficult scenarios—such as a Zoom call or Google meet (10).

Alternative Methodologies

Machine Learning for Traffic Prediction: Instead of relying solely on pattern recognition in traffic analysis ([8†source]), machine learning models could predict user behaviour from encrypted traffic more accurately by learning from large datasets.

Hybrid CAC Models: The CO-CAC system ([9†source]) could be enhanced by incorporating machine learning for more adaptive, real-time predictions of network congestion, enabling more efficient codec adjustments and call handling in dynamic environments.

Conclusion

Paper elaborates handling encrypted traffic, optimizing call quality in hybrid networks, and integrating new technologies like WebRTC into traditional VoIP frameworks, along with SIP. Its ability to dynamically adapt to network changes and its performance in terms of QoS make it ideal for emergency communication systems. However, security remains a significant challenge, with vulnerabilities such as eavesdropping and DoS attacks needing more robust countermeasures.

Future research should focus on enhancing the security protocols for VoIP systems, particularly in high-risk environments. Improved encryption methods and authentication mechanisms could mitigate the risks posed by attackers and ensure the integrity and reliability of VoIP communications. These methodologies can be expanded through modern techniques like machine learning and blockchain, particularly in large-scale deployments.

References

1. Bramantyo Adhilaksono, Bambang Setiawan, "A Study of Voice-over-Internet Protocol Quality Metrics," Procedia Computer Science, 2021.

2. Vinod Kumar and Om Prakash Roy, "Security and Challenges in Voice over Internet Protocols: A Survey," IOP Conf. Ser.: Mater. Sci. Eng., 2021.

3. Aditya Wijayanto, Rifki Adhitama, and Auliya Burhanuddin, "SOLSR Protocol Performance Analysis for VoIP Application in Mesh Topology," IEEE International Conference on Communication, Networks and Satellite (Comnetsat), 2021

4. Dharmin Suthar, Parag H. Rughani, "A Comprehensive Study of VoIP Security," ICACCCN, 2020.

5. U. R. ALO and Nweke Henry Firday, "Voice over Internet Protocol (VOIP): Overview, Direction And Challenges," Journal of Information Engineering and Applications, Vol. 3, No. 4, 2013.

6. Vicente Mayor, Rafael Estepa and Antonio Estepa, "CO-CAC: A new approach to Call Admission Control for VoIP in 5G/WiFi UAV-based relay networks," Computer Communications, 2023.

7. Soliman Abd Elmonsef Sarhan et al., "A Framework for Digital Forensics of Encrypted Real-Time Network Traffic," Ain Shams Engineering Journal, 2023.

8. Om Prakash Roy, Vinod Kumar, "A Survey on Voice over Internet Protocol (VoIP) Reliability Research," IOP Conf. Ser.: Mater. Sci. Eng., 2021.

9. OUESSE Mohamed El-Amine, Mohamed SALL, Adrien BASSE, "A WebRTC - VoIP Communication Platform," 10th International Conference on IoT, Microwave Engineering, and Communications, 2021.

10. Han Liu, Zhiyuan Yu, Mingming Zha, XiaoFeng Wang, William Yeoh, Yevgeniy Vorobeychik and Ning Zhang, "When Evil Calls: Targeted Adversarial Voice over IP Network," Creative Commons Attribution International (CCS), 2022.