VELLORE INSTITUTE OF TECHNOLOGY, VELLORE

COURSE NAME → Data Communication and Networking.
(PMCA505L)

Name - Barsha Routh
Reg no - 24MCA0164

TITLE → Voice over IP is a real time interactive audio / video application.

ABSTRACT

Voice-Over-Internet-Protocol (VoIP) has become a key communication technology, offering cost-effective and scalable voice and multi-media services over the internet. This report explores various VoIP protocols, with an emphasis on forensic in encrypted traffic, call admission control (CAC) in 5G and Wi-fi networks, WebRTC platforms, and challenges of ensuring QoS (Quality of Service). Additionally, the report provides a comparative analysis of SOLSR, SIP, and WebRTC protocols, focusing on their performance in disaster-prone scenarios and vulnerabilities to attacks such As eavesdropping, DOS, spoofing. Emerging trends like 5G integration and cloud-based VoIP services are discussed, concluding with recommendations for enhancing VoIP security protocols to improve resilience in high-risk environments.

INTRODUCTION

VoIP technology has revolutionized communication by enabling the transmission of voice and multimedia over Internet, making traditional Public Switched Telephone Network (PSTN) increasingly obsolete. The flexibility and cost-efficiency of VoIP make it ideal for various applications, from personal communication to disaster management, where traditional infrastructure might be unavailable. Key Protocols such as SIP and SOLSR (Secure Optimized Link State Routing) play a pivotal role in ensuring efficient communication over VoIP networks. Additionally, a study of compression algorithm, such as G.711 and G.729 codecs, has shown how VoIP reduces bandwidth usage while maintaing quality.

BARSHA ROUTH, 24MCA0164

Working of VoIP

The basic functionality of VoIP involves the conversion of voice signals into digital data, which is then transmitted over the internet. The key steps are:

1. Call Initiation: The user's voice is captured by a microphone and converted into digital signals.
2. Packetization: The digital data is divided into small packets.
3. Transmission: These packets are transmitted over the internet via routers and servers.
4. Reassembly: At destination, the packets are reassembled into original order.
5. Conversion to Audio: The reassembled data is converted back into audio, enabling real-time communication.

This process supports real-time interactions and is more cost-effective than traditional telephony with added support for video & message.

METHODOLOGY

This report compares different VoIP protocols, focusing on their performance in terms of security, QOS and use in emergency scenarios. The study evaluates SOLSR in a network of Raspberry Pi devices to simulate an ad-hoc communication network for disaster management. Metrics such as throughput, delay, jitter, and packet-loss are measured using Iperf software. Additionally, SIP and WebRTC are tested under varying network conditions.

Key focus areas:

- SIP (Session Initiation Protocol): Widely used for real-time sessions, SIP is extensible and supports both voice and video communication but has vulnerabilities, particularly with NAT traversal and DOS attacks.

Date

- SOLSR (Secure OLSR): Designed for mobile ad-hoc networks (MANETs), SOLSR provides secure routing in dynamic topologies, ideal for disaster-prone areas.

EXPERIMENTAL DATA COLLECTION

To understand VoIP performance, experimental data was collected from real world deployments using Asterisk PBX servers, with the G.711 codec for voice transmission. The parameters measured include jitter, packet loss, the Mean Opinion Score (MOS), which assesses call quality. The experiment simulates network conditions with delayed packets and limited bandwidth to analyse the impact on voice quality.

Parameter	Average value	Impact on QOE
Jitter	18 ms	Noticable delay, lower Quality
Packet loss	1.5%	Minor distortion, reduced clarity
MOS	3.8	Moderate quality.

The results indicated that enabling encryption increased packet delay by 23 ms, significantly affecting real-time traffic.

VOIP SECURITY CHALLENGES

VoIP system face several security threats, including:

- Eavesdropping: Attackers intercept unencrypted VoIP traffic.
- Caller ID spoofing: Malicious actors manipulate caller IDs to impersonate legimate users.
- Denial of Service (DOS): Flooding VoIP servers with traffic can degrade service quality.

→ While SOLSR offers better protection against rogue nodes and is more secure for ad-hoc networks, SIP is more vulnerable to centralized server attacks & spoofing.

Comparative Analysis

- **SIP vs. SOLSR**: SIP is widely used for high-latency environments with minimal packet loss, making it ideal, but struggles with mobility and dynamic configurations. SOLSR optimised for MANETs, is more resilient in these environments but suffers from computational overhead due to its security features.
- **QoS Evaluation**: SOLSR is used to better suit for high-latency env. with minimal packet loss, making it ideal for voice traffic in emergency scenarios. SIP, while robust under normal conditions, experiences higher jitter and delay in unstable environments, affecting communication quality.

Suggested Alternate Methodology

1. **Machine learning for Traffic Prediction**: Instead of traditional traffic analysis, machine learning algo. can predic user behaviour more accurately by analyzing encrypted VoIP traffic
2. **Hybrid Call Admission Control (CAC) Models**: Introducing machine learning into CAC system, such as CO-CAC, can provide more adaptive and real-time predictions of network congestion. This would allow for more efficient codec adjustments and better call handling in dynamic, high-traffic environments.
3. **Blockchain for Secure VoIP**: Integrating blockchain technology into VoIP systems could enhance security by decentralizing control and providing tempes-proof logs for call sessions. This would mitigate risks like eavesdropping and DoS attacks, providing a robust framework.

CONCLUSION

This report highlights key advancements in VOIP technology, focusing on protocols like SIP and SOLSR and their application in real-time communication, particularly in disaster scenarios. SOLSR's adaptability & performance in challenging environments make it strong candidate for emergency communi-cation systems. However, security remains a significant concern, with vulnerability such as eavesdropping and Dos attacks requiring stronger countermeasures.

Future research should explore modern encryption techniques, blockchain based security models, and the role of machine learning in optimising VOIP performance. These improvements will be critical for ensuring the resilience and security of VOIP systems in high risk environments.

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. Dharmin Suthar, Parag H. Rughani, "A Comprehensive Study of VoIP Security." ICACCCN, 2020.
4. Dio Aditya Wijayanto, Ritti Adhitama and Auliya Burhanuddin, "SOLSR protocol performance Analysis for VoIP Application in Mesh Topology," IEEE International Conference on Communication, 2024.
5. V.R Alo and Nweke Henry Friday, "Voice over Internet Protocol (VOIP): Overview," Journal of Information Engineering And Application, 2013.