UNIVERSIDADE ESTADUAL DO MARANHÃO – UEMA
CENTRO DE CIÊNCIAS TECNOLÓGICAS – CTT
CURSO DE ENGENHARIA DA COMPUTAÇÃO

CHRISTIANN DÊNYS DA FONSECA VIEIRA

ANÁLISE DA SEGURANÇA DO AMBIENTE DE TELEFONIA VOIP DA UNIVERSIDADE ESTADUAL DO MARANHÃO

São Luís – MA
2019

CHRISTIANN DÊNYS DA FONSECA VIEIRA

ANÁLISE DA SEGURANÇA DO AMBIENTE DE TELEFONIA VOIP DA UNIVERSIDADE ESTADUAL DO MARANHÃO

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Curso de Engenharia da Computação, da Universidade Estadual do Maranhão, como pré-requisito para alcançar o título de Bacharel em Engenharia da Computação.

Orientador: Prof. Wesley Batista Dominices de Araujo

São Luís – MA

2019

CHRISTIANN DÊNYS DA FONSECA VIEIRA

ANÁLISE DA SEGURANÇA DO AMBIENTE DE TELEFONIA VOIP DA UNIVERSIDADE ESTADUAL DO MARANHÃO

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do Curso de Engenharia da Computação, da Universidade Estadual do Maranhão, como pré-requisito para alcançar o título de Bacharel em Engenharia da Computação.

Orientador: Prof. Wesley Batista Dominices de Araujo

Aprovada em / /

BANCA EXAMINADORA

_____

Prof. Wesley Batista Dominices de Araujo (Orientador)

Mestre em Engenharia de Computação
Universidade Estadual do Maranhão

_____

Prof. Luís Carlos Costa Fonseca

Doutor em Informática na Educação
Universidade Estadual do Maranhão

_____

Prof. Reinaldo de Jesus da Silva

Doutor em Informática na Educação
Universidade Estadual do Maranhão

AGRADECIMENTOS

Primeiramente, quero agradecer a Deus por permitir que tudo isso acontecesse, por ter me dado saúde e força para superar as dificuldades e chegar até aqui.

À Universidade Estadual do Maranhão por ter me dado a oportunidade de fazer este curso e aos professores por terem compartilhado comigo do seu conhecimento durante esses anos de estudos.

Ao meu orientador pela orientação, apoio, confiança e pelo empenho dedicado à elaboração desse trabalho.

Aos meus pais, Nubia Maria e Benedito Vieira, à minha irmã, Nubiane Vieira, e à minha noiva, Dayane Mendes, pelo amor, incentivo e apoio incondicional.

Aos meus amigos e companheiros de trabalho que fizeram parte da minha formação.

E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

Com o advento da internet surgiram novas formas de comunicação e uma dessas tecnologias é o VoIP – Voz sobre IP. O VoIP é uma tecnologia de baixo custo, onde é possível receber e realizar ligações em qualquer lugar que tenha conexão com a internet. O VoIP realiza a convergência de voz e de dados na mesma rede, por exemplo, a Internet. Com o crescimento dessa tecnologia crescem também as ameaças ao serviço oferecido por esta tecnologia. O objetivo deste trabalho é apresentar as ameaças e vulnerabilidades na tecnologia VoIP, bem como métodos de segurança contra esses problemas. Para demonstrar uma vulnerabilidade na aplicação VoIP da Universidade Estadual do Maranhão, realizaram-se dois testes de captura de voz, sendo um utilizando a rede cabeada e o outro a rede Wi-Fi. A captura e a análise dos dados foram realizadas com o *software Wireshark.* Como resultado provou-se que existe uma vulnerabilidade na aplicação no que diz respeito à confidencialidade do fluxo de voz e sugeriu-se métodos de segurança.

Palavras-chave: Segurança, VoIP, Wireshark, *Call Eavesdropping.*

ABSTRACT

With the advent of the Internet new forms of communication have emerged and one of these technologies is VoIP - Voice over IP. The VoIP is a low-cost technology where you can receive and make connections anywhere you have an internet connection. VoIP performs voice and data convergence on the same network, for example the Internet. With the growth of this technology, also grows the threats to the service offered by this technology. The purpose of this paper is to present the threats and vulnerabilities in VoIP technology as well as security methods against these problems. In order to demonstrate a vulnerability in the VoIP application of the Universidade Estadual Maranhão, two voice capture tests were performed, one using the wired network and the other the Wi-Fi network. The capture and analysis of data was carried out with the software Wireshark. As a result, it has been proven that there is a vulnerability in the application regarding the confidentiality of the voice stream and security methods have been suggested.

Keywords: Security, VoIP, Wireshark, Call Eavesdropping.

LISTA DE FIGURAS

LISTA DE SIGLAS

WAN – *Wide Area Network*
ATA – Adaptador para Telefone Analógico
PABX – *Private Automatic Branch eXchange*
TCP – *Transport Control Protocol*
UDP – *User Datagram Protocol*
IP – *Internet Protocol*
RTP – *Real-time Transport Protocol*
RTCP – *Real-time Transport Control Protocol*
CNAME – *Canonical Name*
RR – *Receiver Report*
SR – Sender Report
SDES – *Source Description*
MGCP – Media Gateway Control Protocol
ITU – *International Telecommunication Union*
IETF – *Internet Engineering Task Force*
SIP – *Session Initiation Protocol*
RFC – *Request for Comments*
UA – User Agents
URI – *Uniform Resource Identifier*
CPqD – Centro de Pesquisa e Desenvolvimento em Telecomunicações
S/MIME – *Secure/Multipurpose Internet Main Extensions*
IPSec – *Internet Protocol Security*
SRTP – *Secure Real-time Transport Protocol*
SRTCP – *Secure Real-time Transport Control Protocol*
MIKEY – *Multimedia Internet KEYing*
ZRTP – *Zimmermann Real-time Transport Protocol*
LAN – *Local Area Network*
VLAN – *Virtual Local Area Network*
DHCP – Dynamic Host Configuration Protocol
IDS – *Intrusion Detection System*
IPS – *Intrusion Prevention System*
DoS – *Deny of Service*
SPIT – *SPAM over Internet Telephony*
NTI – Núcleo de Tecnologia da Informação
UEMA – Universidade Estadual do Maranhão
TLS – *Transport Layer Security*
VoIP – *Voice over Internet Protocol*

SUMÁRIO

1. INTRODUÇÃO

Após a invenção do telefone o mundo não foi mais o mesmo, pois mudou a forma da comunicação à distância entre as pessoas, não era mais necessário enviar cartas e esperar dias pela resposta. Agora, por meio do telefone, era possível falar em tempo real com as pessoas, não importa onde estivessem, bastando possuírem um telefone.

Com o advento da internet e com a facilidade de acesso a ela começaram a surgir outras formas de comunicação que a utilizam como meio, trazendo mudanças radicais ao mundo das telecomunicações e uma dessas tecnologias é o VoIP – Voz sobre IP. Um dos maiores atrativos dessa tecnologia é o baixo custo, que pode até ser nulo, além da flexibilidade para realizar ligações.

Com VoIP é possível receber e realizar ligações em qualquer lugar que tenha conexão com a internet por meio de computadores ou telefones IP, isso dá ao VoIP uma mobilidade maior que a telefonia convencional. O VoIP realiza a convergência de voz e de dados na mesma rede, por exemplo a Internet. E como com a internet não há limites de distância, o custo das ligações pode ser bem reduzido, além de poder tornar inexistentes os custos de tarifas interurbanas e internacionais.

A tecnologia VoIP vem crescendo cada vez mais ao longo dos últimos anos, e junto com isso crescem também as ameaças ao serviço. O VoIP integra os serviços de voz em uma rede de dados que já é razoavelmente exposta a ameaças. Essa integração acaba trazendo para o VoIP os riscos de segurança que já existem na rede IP. Com a quantidade de dados que são transmitidos pela rede, passando por locais que muitas vezes não estão sob o domínio dos interessados, é necessária uma grande preocupação com a segurança, pois os dados estão suscetíveis às mais diversas ameaças no caminho entre remetente e destino.

A telefonia convencional envolve a transmissão por um meio físico baseada em comutação de circuitos e para ataques de espionagem, por exemplo, é necessário acesso presente às linhas físicas. Com VoIP não é necessária presença física para se ter acesso ao sistema de voz, pois agora a comunicação é baseada em comutação de pacotes pela rede IP e este é um sistema aberto onde um endereço IP pode se conectar a outro.

Em VoIP a voz é digitalizada e compactada em pacotes de voz, esses pacotes de voz são enviados pela rede IP e, se não houver mecanismos de segurança, um

atacante pode acessar a rede VoIP e interceptar esses pacotes podendo usar as informações para prejudicar o dono da informação, realizar fraudes, escutas telefônicas, assim como usar o acesso para atacar toda a rede.

Para garantir a segurança de um sistema VoIP existem protocolos e mecanismos para implementar segurança na aplicação, como criptografia e autenticação. O intuito desse trabalho é apresentar as ameaças existentes, os métodos de segurança e realizar uma tentativa de ataque no ambiente VoIP da Universidade Estadual do Maranhão, para analisar se existem mecanismos de defesa e quais as consequências caso não existam.

1.1. Objetivos

1.1.1. **Objetivo Geral**

Apresentar as ameaças e vulnerabilidades na tecnologia VoIP, bem como métodos de segurança contra esses problemas.

1.1.2. **Objetivos específicos**

- Estudar a tecnologia VoIP;
- Investigar as ameaças à tecnologia VoIP;
- Investigar as medidas de segurança para sistemas VoIP;
- Analisar a segurança de um sistema VoIP;
- Propor medidas de segurança para esse sistema e
- Demonstrar a viabilidade da implementação de segurança.

1.2. Estrutura do Trabalho

O Trabalho está dividido em cinco capítulos. No segundo capítulo serão apresentados conceitos importantes para o trabalho, como: Conceito de VoIP, funcionamento da tecnologia, protocolos utilizados para VoIP, segurança aos sistemas VoIP, bem como as ameaças ao serviço e os mecanismos de defesa. No terceiro capítulo será apresentada a metodologia desenvolvida, que consiste em uma tentativa de *eavesdropping* – escuta telefônica, a partir da captura de pacotes de voz de uma ligação VoIP realizada pelo serviço VoIP da Universidade Estadual do Maranhão. No quarto capítulo serão analisados os resultados do teste demonstrando se foi possível realizar a escuta telefônica, bem como apresentados métodos de segurança para corrigir o problema caso o ataque tenha sido bem-sucedido. O último

capítulo apresentará as conclusões, descrevendo se os objetivos desse trabalho foram alcançados e apresentando sugestões para trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão abordados alguns conceitos essenciais para esse trabalho, tais como: VoIP, Protocolos e Segurança.

2.1. VoIP

“Dentre as muitas tecnologias convergentes, capazes de transportar voz e dados pela internet, uma das que mais se destaca atualmente é a chamada Voz sobre IP ou simplesmente, VoIP” (ROSS, 2007, P. 8).

O VoIP (*Voice over Internet Protocol*) foi criado em meados de 1995 pela empresa Vocal Tec com o intuito inicial de realizar chamadas de longas distâncias e internacionais. O projeto consistia da digitalização da voz, comprimindo e a enviando pela rede, possuía uma qualidade baixa, com cortes e atrasos e só era possível realizar ligações entre dois computadores, sendo necessário o uso de um microfone e caixa de som, o nome dado ao *software* desenvolvido foi ***Internet Software Phone***.

No ano de 1998 a Vocal Tec começou a desenvolver novos modelos do VoIP para que pudessem ser utilizados com outros programas de computador, os chamados *SoftPhones*, e também permitindo chamadas entre VoIP e Telefones convencionais. (A história..., 2018).

Com o surgimento da tecnologia VoIP, um grande número de provedores de serviços de telecomunicações passou a integrar soluções de VoIP em seus sistemas e a fornecer serviços VoIP para seus clientes. Os fabricantes de equipamentos e usuários finais se beneficiaram muito com os avanços no desempenho, com a redução de custos e com o suporte a recursos oferecidos pela tecnologia VoIP. (PHITHAKKITNUKOON et. al., 2008).

Segundo Bordim (2010), o VoIP é uma tecnologia que utiliza técnicas para estabelecer chamadas a partir do empacotamento e transmissão de amostras de voz usando como meio a rede IP. A voz é digitalizada em bits para que possa trafegar pela rede e, utilizando o protocolo IP, ela é transmitida como pacotes de dados, sendo em uma rede privativa ou pública. (ROSS, 2007)

Ross (2007) diz que o VoIP é um conjunto de tecnologias que utiliza as redes IP públicas ou privadas para a comunicação por voz, servindo para substituir ou complementar a telefonia convencional, utilizando das redes de dados e dos protocolos das redes IP para a transmissão dos sinais de voz na forma de pacotes de dados em tempo real.

As primeiras utilizações coorporativas da tecnologia VoIP, eram realizadas por empresas que interligavam suas centrais telefônicas de filiais dispersas geograficamente e também por empresas de telefonia para ligações internacionais, pois barateava os custos de ligações a longa distância já que as chamadas trafegavam junto com outros tipos de informação na rede, não necessitando que as chamadas fossem enviadas isoladas pela rede de telefonia padrão.

De acordo com Liu e Hajhamad (2005 apud Armênio e Reis, 2010), foi somente com a evolução da tecnologia e o desenvolvimento de novas tecnologias VoIP, nos mercados de operadoras de telefonia e de soluções corporativas, no final da década de 1990, que a utilização da tecnologia VoIP de forma comercial se tornou possível.

Para que a transmissão da voz seja possível, o VoIP recebe a voz analógica e a transforma em pacote de dados, tornando possível enviar esses pacotes pela rede TCP/IP, ou seja, enviá-los por uma rede, por exemplo, pela internet. E quando os dados chegam ao destino, ocorre o processo inverso, transformando dos pacotes de dados novamente em sinal analógico e transmitido para uma caixa de som, por exemplo, onde a voz pode ser ouvida novamente. (ALECRIM, 2005).

A Figura 1 ilustra uma estrutura típica de rede VoIP:

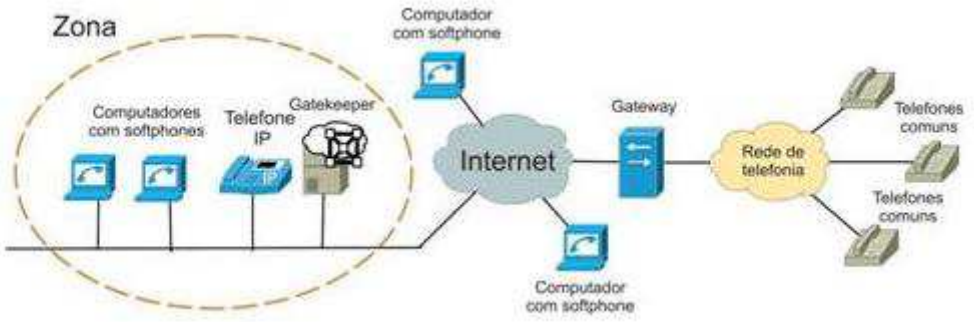

Figura 1: Estrutura típica de rede VoIP.
Fonte: Ribeiro, 2018.

Alguns equipamentos que possibilitam o processo da comunicação por VoIP são os seguintes (RIBEIRO, 2019):

- ***Gateway***: é um equipamento que conecta a rede IP à rede de telefonia convencional. Trabalha ao mesmo tempo com mídia e sinalização, ou seja, realiza o repasse de fluxo entre redes, e também trata as solicitações de chamadas telefônicas.

- ***Gatekeeper***: equipamento que controla o sistema VoIP, já que os equipamentos se registram nele para que seja admitida e gerenciada a largura de banda para a chamada telefônica.
- **Terminais**: equipamentos de comunicação, como telefones convencionais, telefones IP e também computadores com *softphones*.
- **Zona**: é o conjunto dos dispositivos controlados pelo *gatekeeper*, pode ser também uma rede LAN – *Local Area Network.*

As chamadas VoIP podem ser realizadas de diversas formas, por exemplo, entre dois computadores com *softphones* instalados e equipados com *headsets* ou caixas de som e microfone. Esse é o método mais simples de implementação e utilização. A Figura 2 ilustra esse cenário:

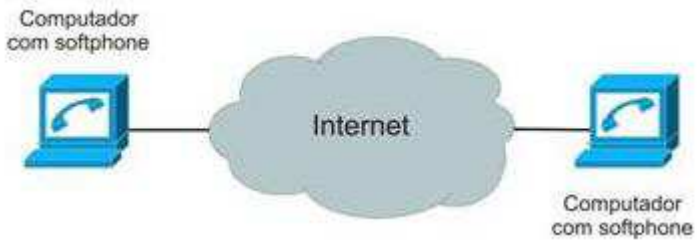

Figura 2: Ligação VoIP entre computadores.
Fonte: Ribeiro, 2018

Também podem ser realizadas chamadas entre computador e telefone convencional, utilizando de um aparelho chamado ATA – Adaptador para telefone Analógico – conectando o telefone à rede IP. O número discado é enviado à empresa contratada como provedora do serviço VoIP, e o *gateway* da provedora redireciona a chamada para o IP do número discado. A Figura 3 ilustra esse cenário:

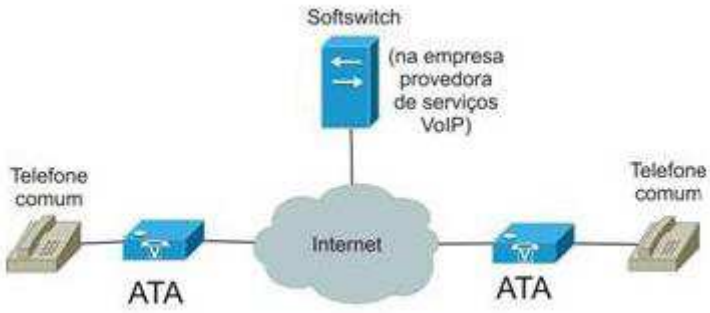

Figura 3: Ligação VoIP entre aparelhos convencionais com ATA.
Fonte: Ribeiro, 2018

Existem também os Telefones IP, que foram desenvolvidos justamente para utilização de VoIP, que possuem uma entrada RJ-45 para um cabo de rede. Basta estarem configurados e serem conectados à rede, que pode ser a internet ou mesmo a uma rede local (LAN). A Figura 4 ilustra esse cenário:

Figura 4: Ligação VoIP entre telefones IP.
Fonte: Ribeiro, 2018

Além disso, os *smartphones* também possuem aplicações de *softphone* para chamadas VoIP, como por exemplo o Zoiper.

Na telefonia convencional existe o conceito de PABX (*Private Automatic Branch eXchange*), que é um aparelho onde são ligadas as linhas telefônicas de uma empresa, por exemplo, e distribuídas para ramais telefônicos, possibilitando que todos os ramais possam realizar ligações externas, além de ligações internas gratuitas. Para uma rede VoIP existe o PABX IP, um novo conceito que mantém a topologia de um PABX centralizado, em *Data Centers*, e os ramais são entregues como ramais de VoIP e não mais como linhas convencionais. (ROSS, 2007).

O VoIP pode ser utilizado tanto na rede pública como na rede privada. Quando na rede pública, qualquer pessoa com acesso à internet pode realizar uma chamada VoIP. A rede privada geralmente é utilizada por empresas para interligarem seus setores para comunicação interna, podendo ser em redes locais (LAN) ou até mesmo em redes globais (WAN) em grandes empresas.

Para que o VoIP funcione de maneira adequada na rede pública é necessário que se tenha uma conexão de boa qualidade com a internet, pois se a qualidade de transmissão for péssima, pode haver perdas ou atrasos de pacotes, o que gera uma queda momentânea da voz durante a conversa. Para uma aplicação na rede privada isso é algo que ocorre com frequência em redes bastante congestionadas ou mal implementadas.

2.2. Protocolos

Durante uma comunicação VoIP ocorrem basicamente dois processos simultâneos (RIBEIRO, 2019):

- Sinalização e controle de chamadas: estabelecimento, acompanhamento e finalização.
- Processamento da informação a ser enviada e recebida: controle e transporte da mídia.

Para que esses processos sejam realizados de maneira adequada são implementados os protocolos de VoIP, onde cada um possui sua função nos processos descritos acima.

2.2.1. Protocolos de Transporte

A internet (TCP/IP) possuiu dois protocolos de transporte, sendo eles o TCP e o UDP. Tendo o VoIP sido construído totalmente em cima do modelo TCP/IP, a comunicação entre dispositivos VoIP pode utilizar como protocolo de transporte tanto o UDP quanto o TCP, porém é comumente utilizado o UDP para aplicações de tempo real. (BORDIM, 2010).

> Um protocolo da camada de transporte fornece comunicação lógica entre processos de aplicação que rodam em hospedeiros diferentes. Comunicação lógica nesse contexto significa que, do ponto de vista de uma aplicação, tudo se passa como se os hospedeiros que rodam os processos estivessem conectados diretamente. (KUROSE e ROSS, 2013, p. 135).

Segundo Tanenbaum (2003), o TCP (*Transmission Control Protocol* – Protocolo de Controle de Transmissão) é um protocolo orientado a conexões, confiável, permitindo a entrega de um fluxo de dados sem erros de um emissor, onde esse fluxo é fragmentado em mensagens discretas para serem transportados. No destino o TCP monta novamente esses dados.

Para Kurose e Ross (2013), o protocolo TCP é orientado para conexões, pois no início de uma comunicação os processos necessitam se apresentar, por meio de uma troca de dados preliminares, para estabelecerem os parâmetros para a transferência dos dados.

Outra função do TCP é o controle de fluxo, no qual o protocolo obriga os remetentes a limitarem a taxa de envio do tráfego para rede de acordo com o fluxo atual da rede. Se a rede estiver com muito congestionamento, a taxa de envio será reduzida, e se houver pouco congestionamento, a taxa de envio será aumentada. (KUROSE E ROSS, 2013).

Segundo Tanenbaum (2003), o UDP *(*User Datagram Protocol – *Protocolo de Datagrama do Usuário)* é um protocolo não orientado para conexão, pois ele não

necessita que seja realizada uma apresentação entre os processos remetente e destinatário para estabelecer uma conexão antes de enviar uma informação, isso torna a entrega dos pacotes mais rápida.

O UDP não possui controle de fluxo, ou seja, ele não limita a taxa de envio de informações na rede de acordo com a situação de congestionamento. Ele também não possui controles de erros, ou seja, não reenvia pacotes que tiveram erros ou não foram recebidos pelo destino. Ele também não mantém a sequência das mensagens da transmissão de dados. (BORDIM, 2010).

Uma das maiores utilizações do UDP são as aplicações de tempo real, em que a entrega rápida é mais importante do que entrega exata, como em transmissões de áudio ou vídeo pela internet. Como essas aplicações são sensíveis ao atraso, não faz sentido gastar tempo com a correção dos pacotes para não gerar atraso. E já que o VoIP é uma aplicação de tempo real, o UDP é o protocolo ideal. (RIBEIRO e MENDES, 2016)

Como o UDP não possui controle de sequência dos pacotes na transmissão de dados e os pacotes do VoIP disputam espaço com outras aplicações navegando na rede, esses pacotes podem ser perdidos, sofrerem atrasos ou chegarem fora de ordem no destino. Logo é necessário um tratamento adequado desses pacotes. É aí que entra o RTP (Realtime Transporte Protocol – Protocolo de Transporte de Tempo Real), um protocolo que enumera os pacotes para que possam ser reconstruídos na ordem correta quando chegarem ao receptor. (BORDIM, 2010).

O RTP é definido pela recomendação RFC (*Request for Comments*) 1889 do IETF (*Internet Engineering Task Force*), sendo o principal protocolo que é utilizado por terminais VoIP para o transporte dos pacotes de voz em tempo real pela rede IP. Para Alecrim (2005), o RTP basicamente tenta organizar os pacotes para que sejam recebidos na ordem que foram enviados, para que dessa forma, seja possível uma transmissão de dados em tempo real. Se um pacote não chegar ao destino, o RTP causa uma interpolação no espaço deixado pelo pacote, e caso um pacote chegue atrasado, ele é descartado.

Os pacotes enviados usando RTP recebem uma numeração em ordem crescente em relação ao pacote antecessor. É a partir dessa numeração que o destino descobre se está faltando algum pacote e a ordem dos pacotes. Se um pacote não for recebido no destino antes que o pacote de numeração seguinte chegue, o destino deverá fazer uma aproximação do valor por interpolação. (TANENBAUM, 2003).

Segundo Tanenbaum (2003, p. 403): “[...] o RTP não tem nenhum controle de fluxo, nenhum controle de erros, nenhuma confirmação e nenhum mecanismo para solicitar retransmissões”. O RTP não assegura a entrega dos dados no tempo certo, e nem fornece garantias de qualidade de serviço (QoS). Ele não impede que os pacotes sejam perdidos, nem confirma que os pacotes chegarão na ordem correta. (KUROSE E ROSS, 2013).

2.2.2. Protocolos de Controle

O protocolo RTCP (*RTP Control Protocol*) foi definido pela recomendação RFC 1889 do IETF, e o seu funcionamento consiste no envio periódico de pacotes de controle para os participantes da chamada VoIP. Assim, é possível realizar a transmissão dos dados em tempo real com um controle mínimo a partir dos pacotes UDP da rede IP. (BERNAL, 2008).

Para Tanenbaum (2003), o RTCP é um protocolo que tem a função de fornecer *feedback* sobre atraso, flutuação, largura de banda, congestionamento e outras propriedades de rede. Ele também é responsável pela sincronização dos fluxos, já que os fluxos podem usar *clocks* diferentes. O RTCP cuida também da interface do usuário, já que ele fornece uma forma de nomear as origens em uma chamada, em ASCII, por exemplo, e essa informação pode ser utilizada com o intuito de exibir na tela do destino o nome de quem está se comunicando.

Segundo Clemente (2006), o RTCP possui quatro funções para realizar o controle da transmissão:

- Gerar relatório sobre a qualidade de serviço da transmissão.
- Manter um identificador persistente em nível de transporte, conhecido como CNAME.
- Controlar a taxa de envio de relatórios RTCP enviados pelos participantes.
- Transmitir informação para controle de sessão.

De Acordo com Perkins (2003), o protocolo RTCP possui cinco tipos de pacotes:

- ***Receiver Report*** **(RR):** reporta a qualidade de recepção dos participantes que estão recebendo dados. Essas informações podem ajudar o remetente a adaptar a sua transmissão de acordo com *feedback*.

- ***Sender report* (SR):** reporta a qualidade de envio dos pacotes que estão sendo enviados pelos participantes. A partir dessas informações, a aplicação pode calcular a taxa média de dados de carga útil e a taxa média de pacotes durante um intervalo sem receber os dados.
- ***Source Description* (SDES):** possui informações sobre a fonte, como a identificação do participante e outros detalhes complementares como, por exemplo, número de telefone. As informações dos pacotes SDES são tipicamente usadas para mostrar na tela de destino informações sobre o remetente.
- ***Membership Control* (BYE):** indica quando um participante deixa a sessão.
- ***Application-Defined RTPC Packets* (APP):** um pacote para funções específicas de aplicações.

Apesar das informações retornadas pelo RTCP não informarem onde ocorrem determinados problemas, elas podem servir como ferramentas para localizar esses problemas. (RIBEIRO e MENDES, 2016).

Outro protocolo de controle é o MGCP (*Media Gateway Control Protocol* – Protocolo de Controle de Gateway de Mídia). Esse protocolo foi definido pela recomendação RFC 2705 do IETF. Ele serve para controlar as conexões nos *Gateways* dos sistemas VoIP usando um elemento de controle externo de chamadas, de modo centralizado, o Agente de Chamadas. O MGCP é basicamente um protocolo *Master/Slave* (Mestre/Escravo), agindo para que o *gateway* execute o comando enviado pelo Agente de Chamadas. (RIBEIRO e MENDES, 2016).

Segundo Bernal (2008), a partir de um conjunto de transações do tipo comando/resposta que criam, controlam e auditam as conexões nos *Gateways*, o MGCP implementa uma interface de controle. As mensagens dessas transações usam os pacotes UDP e são trocados entre os *Gateways* e *Gateways Controllers* para estabelecimento, acompanhamento e finalização das conexões.

O protocolo H.248 também é um protocolo de controle e foi criado em conjunto pela IETF e a ITU (*International Telecommunication Union*), é também chamado de MeGaCo e é definido pela recomendação H. 248.2 do ITU-T. Mondadori (2006), nos diz que esse protocolo separa fisicamente o plano de controle do plano de conexão. O plano de controle é responsável pela troca de sinalizações e mensagens entre as

redes e protocolos, ele converte as mensagens para comandos do H.248 e encaminha pela rede IP para o plano de conexão.

2.2.3. Protocolos de Sinalização

Os protocolos de sinalização são responsáveis pelos controles de ligação entre elementos de uma rede fazendo a negociação entre equipamentos para estabelecer uma comunicação. Em relação ao VoIP existem dois protocolos e sinalização: o H.232 e o SIP.

> Um protocolo de sinalização para VoIP deve especificar a codificação da voz, a configuração das chamadas, o transporte de dados, o modo de autenticação, segurança, métodos utilizados na comunicação, cabeçalho, endereçamento, sintaxe da mensagem. (VAZ e DINAU, 2006).

Em 1996, a ITU Emitiu a recomendação H.323 que foi nomeada de “Sistemas e equipamentos de telefonia visual para redes locais que oferecem uma qualidade de serviço não garantida”. Tendo como principal contribuição o desenvolvimento de um conjunto de protocolos de sinalização que permitem controlar o estabelecimento, a manutenção e a liberação de conexões multimídia em redes de pacotes. (MORENO, SOTO E LARRABEITI, 2001).

Tanenbaum (2003) diz que o H.323 não é exatamente um protocolo específico, mas que ele faz referência a um conjunto de protocolos de sinalização para codificação de voz, configuração de chamadas, sinalização, transporte de dados entre outras áreas, ao invés de especificar cada uma delas.

O H.323 fornece um padrão para transmissão de dados, áudio e vídeo através da rede IP. Produtos e aplicações multimídia que seguem as regras desse padrão, mesmo sendo de fabricantes distintas, podem operar entre si. (CARDOSO, 2004).

Alguns dos benefícios do H.323 listados por Cardoso (2004) são os seguintes:

- Estabelece padrões para compressão e descompressão de dados de áudio e vídeo, para que os equipamentos de diferentes fabricantes operem entre si.
- Estabelece métodos para que os clientes no destino informem suas potencialidades ao remetente, para que não haja preocupação com compatibilidade no destino.
- É projetado para funcionar no topo das arquiteturas de rede, sendo independente da rede.

- Fornece suporte a multiponto, permitindo conferências de três ou mais pontos sem a necessidade de uma unidade de controle especializada.
- Fornece gerência de largura de banda, para que o tráfego de multimídia não obstrua a rede, dando ao gerente de rede uma ferramenta para limitar o número de conexões H.323 ou a largura de banda às aplicações H.323.
- É flexível, destinatários com potencialidades diferentes podem fazer parte da mesma conferência.

O H.323 é um padrão amplamente utilizado em sistemas de vídeo conferencia e comunicação multimídia no geral. Como a maioria das implementações de rede utilizam protocolos de transporte baseados em pacote, com o H.323 é possível utilizar das aplicações multimídia sem a necessidade de alteração da infraestrutura de rede.

Tanenbaum (2003) cita alguns dos protocolos do H.323 e suas funções. Para Codificação e Decodificação de voz, os sistemas H.323 devem ter suporte a recomendação G.711, porém são permitidos outros protocolos também. Para negociar qual algoritmo de compactação será usado pelos terminais, é utilizado o protocolo H.245. Esse protocolo também é responsável por negociar outros aspectos da conexão, como a taxa de bits, por exemplo.

Outro protocolo necessário é a recomendação ITU Q.931, que estabelece e encerra conexões, além de fornecer tons de discagem, sons de chamadas e outros aspectos encontrados na telefonia padrão. O Protocolo H.225 é usado para que os terminais se comuniquem com o *gatekeeper*, quando presente, e o canal utilizado nessa comunicação é chamado de canal RAS. Este canal permite a entrada e saída da zona por parte dos terminais, solicitação e devolução da largura de banda, além de atualizações de status e outras coisas. O Protocolo utilizado para a transmissão de dados é o RTP, sendo esse gerenciado pelo RTCP.

A Figura 5 demonstra os canais lógicos entre o chamador e o chamado durante uma chamada.

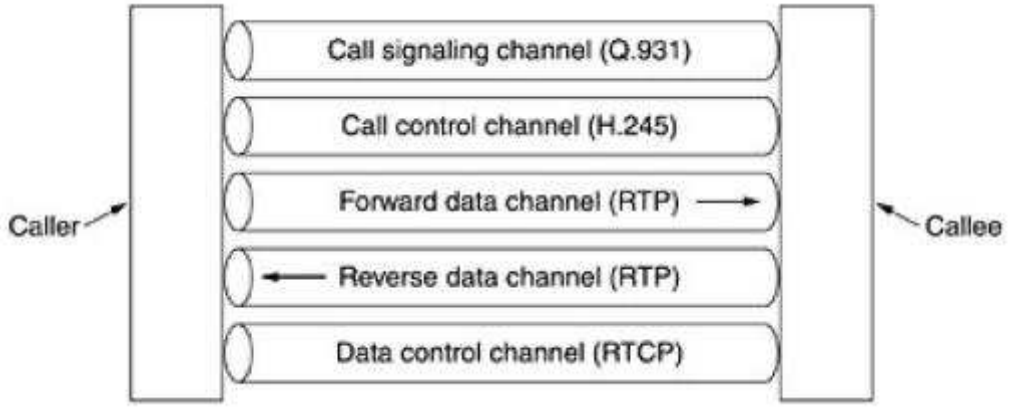

Figura 5: Canais lógicos
Fonte: Tanenbaum, 2003.

O protocolo SIP (*Session Initiation Protocol* – Protocolo de Iniciação de Sessão) teve sua primeira versão lançada em 1996 pela IETF e em 1999 foi proposto como um padrão publicado na RFC 2543. A versão v2 do SIP foi lançada em 2002 na RFC 3261. (BORDIM, 2010). Diferente do H.323 que é um conjunto de protocolos, o SIP é apenas um módulo, que foi projetado para interoperar com as aplicações da internet existentes. Com ele podem ser estabelecidas sessões telefônicas comuns, com apenas duas partes, ou sessões de conferência onde várias partes podem participar, ouvindo e falando, além de sessões de multidifusão, onde existem um transmissor e vários receptores. (TANENBAUM, 2003).

De acordo com a RFC 3261 (Rosenberg et. al., 2002), o SIP é um protocolo de controle da camada de aplicação do modelo TCP/IP, que pode estabelecer, modificar e terminar conexões multimídia, como por exemplo, ligações telefônicas pela internet. Permite também convidar outros usuários para uma sessão já existente, para realizar uma conferência, por exemplo.

Kurose e Ross (2013) descreve como função SIP o seguinte:

- Prover mecanismos para estabelecer chamadas entre dois dispositivos pela rede IP. Permitir o remetente avisar ao destino que deseja iniciar uma chamada. Permitir aos dois decidirem a codificação de mídia a ser usada. Permitir encerrar a chamada.
- Permitir que o remetente possa determinar o endereço IP do destino, para a realização da conexão.

- Gerenciar as chamadas, podendo adicionar novos fluxos de mídia, mudar a codificação, sem interromper a conexão, além de transferir as chamadas e até segurar chamadas.

O SIP é um protocolo baseado no modelo Cliente/Servidor, onde um cliente SIP envia uma mensagem de requisição ao servidor e este responde com uma mensagem de resposta. Os terminais SIP podem realizar chamadas diretamente sem a necessidade de elementos intermediários, assim como o H.323. (MORENO, SOTO E LARRABEITI, 2001).

O SIP não é um sistema de comunicação integrada, ele é um componente que pode ser usado com outros protocolos para construir uma arquitetura de multimídia como, por exemplo, o RTP/RTCP que é utilizado para o transporte de dados. Ele cuida apenas da configuração, do gerenciamento e encerramento das sessões, ele é um protocolo de sessão. Pode funcionar tanto sobre o TCP como do UDP.

De acordo com a RFC 3261 (Rosenberg et. al., 2002), os quatro principais componentes da arquitetura SIP são:

- ***User Agents (UA):*** é o elemento que interage com o usuário, sendo ele cliente (UAC) ou servidor (UAS). Tem a capacidade de enviar e receber requisições.
- ***Proxy Servers:*** funciona como um servidor intermediário do SIP, atuando como cliente e servidor, recebendo e passando adiante as requisições até chegarem ao destino. São usados para traduzir nomes e números de identificação dos UA para o endereço IP dos mesmos.
- ***Redirect Server:*** é um tipo de servidor SIP que não reencaminha os pedidos, mas responde a solicitação do UA fornecendo o endereço de outro servidor proxy mais próximo da localização do destino, ao qual o UA deve reencaminhar a requisição original.
- ***Registar Server:*** é um servidor que armazena registros dos usuários para fornecer a localização.

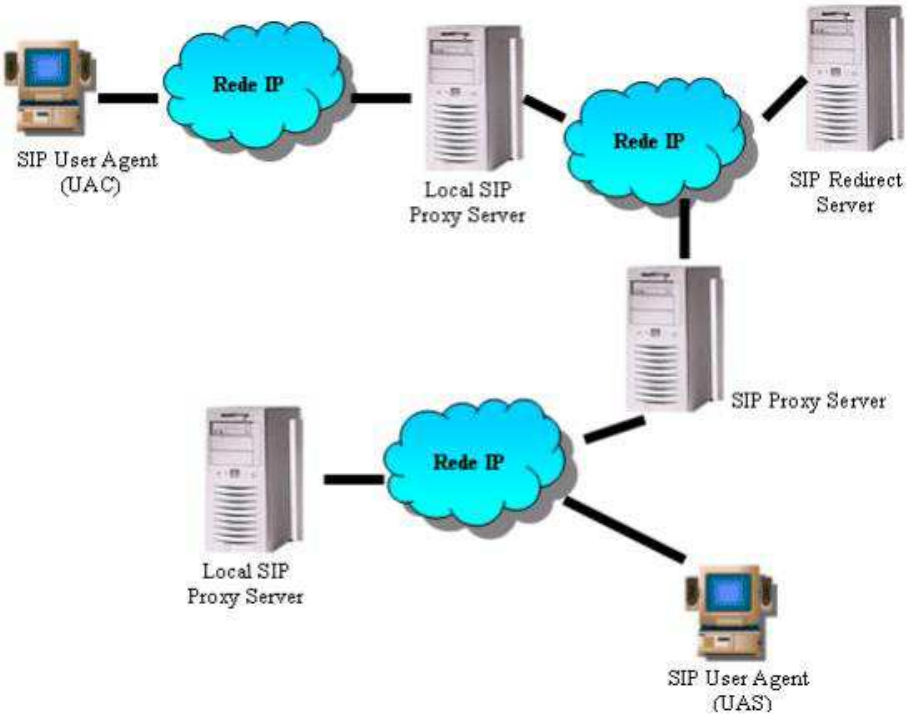

Figura 6: Arquitetura SIP.
Fonte: Registro [2004?].

O protocolo SIP é baseado em texto e se assemelha ao HTTP, tendo sido desenvolvido como intuito de estabelecer, mudar e encerrar chamadas entre um ou mais usuários na rede IP, sendo totalmente independente do conteúdo de mídia da sessão. Assim como no HTTP, suas operações se resumem apenas a métodos de requisições e respostas. Segundo Vaz e Dinau (2006), o SIP possui seis métodos de requisição que utiliza no cabeçalho de suas mensagens, sendo eles: *INVITE, ACK, CANCEL, OPTIONS, REGISTER E BYE*.

O *INVITE* é um método que indica ao usuário que ele está sendo convidado a participar de uma sessão. Ele é enviado quando o remetente solicita o estabelecimento de uma sessão e pode conter uma descrição da sessão (SDP – Protocolo de Descrição de Sessão). Se o usuário aceita participar de uma sessão, ele responde com um 200 (Aceitação). Quando o remetente recebe o código de aceitação, o Método *ACK* confirma o recebimento da mensagem 200 e o início da sessão. A Figura 7 demonstra esse processo para o início de uma sessão.

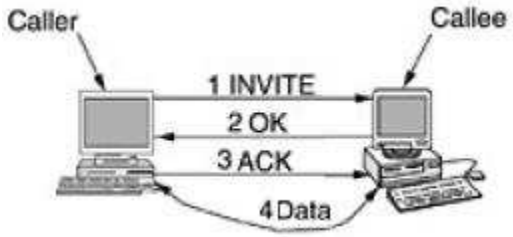

Figura 7: Início de sessão SIP.
Fonte: Adaptado de Tanenbaum (2003).

Quanto aos outros métodos, o *OPTIONS* é usado para consultar os recursos suportados pelo servidor e pelo usuário. O *REGISTER* registra o endereço de um usuário em um servidor SIP, para fornecer serviços de localização. O *CANCEL* é utilizado quando um usuário cancela uma requisição que não foi respondida. O método *BYE* é usado para liberar os recursos de uma sessão e pode ser utilizado por qualquer um dos participantes quando desejarem encerrar a sessão. Assim que o outro lado confirmar com a mensagem 200, a sessão é encerrada. (TANENBAUM, 2003).

O Protocolo SIP usa para endereçamento o SIP URI (*Uniform Resource Identifier*), que é um formato similar ao do e-mail, podendo ter o formato “usuario@dominio”, “usuario@host” e “usuario@IP”, além de possuir um modelo para indicar número de telefone da rede pública acessível por um *gateway*, o “numerodetelefone@gateway”. (YOCHIOKA, 2003).

Uma característica dos endereços SIP é que eles podem ser inseridos em páginas Web, da mesma maneira como são colocados endereços de e-mail como atalho para enviar e-mail. Assim se o usuário clicar no link com o URI, por exemplo sip:nome@dominio, e possuir um cliente SIP instalado em seu computador ou *smartphone*, a chamada já será iniciada com esse destino.

No SIP a autenticação pode ser entre um UA e um servidor e também entre dois UA. Um servidor pode solicitar uma autenticação a um UA para permitir que este utilize os serviços. Já dois UAs necessitam de autenticação para a confidencialidade, garantindo que estão se comunicando com a pessoa certa. A autenticação pode ser de duas formas: HTTP Digest e Criptografia e Troca de certificados. Porém o HTTP Digest não garante segurança e para isso deve ser utilizado o TLS ou S/MIME. (VAZ e DINAU, 2006).

Com o uso do HTTP Digest, o servidor *proxy* que recebe uma solicitação de autenticação, de um usuário não autenticado, responde com a resposta 407 *Proxy*

Server Authentication Required com o desafio. Após o envio do ACK, o solicitante reenvia o *INVITE* com um cabeçalho *Proxy-Authorization*. Normalmente o UA e os servidores Redirect e Registrar respondem a um INVITE que não possui um *Proxy-Authorization* com a mensagem 401 *Unauthorized*. Geralmente as credenciais de um UA são nome de usuário e senha, ambos criptografados. (VAZ e DINAU, 2006).

2.2.4. Codec (Codificado/Decodificador)

Os Codecs são os responsáveis pela codificação e decodificação dos dados analógicos de voz em dados digitais, para que assim seja possível a transmissão pela rede IP. Além disso, eles são os responsáveis pela compressão dos sinais de voz e, de acordo com o nível de compressão, é possível atingir um equilíbrio entre qualidade de voz e largura de banda para o sistema VoIP.

Como exemplos de Codecs de áudio, temos protocolo G.711, que possui uma qualidade muito boa, porém possui uma taxa de transmissão muito alta. Temos ainda o G.729 que possui uma qualidade não tão boa como o G.711, porém ainda é considerada boa, e uma baixa taxa de transmissão, assim este traz um equilíbrio entre a qualidade e a eficiência da largura de banda. (RIBEIRO, 2019).

2.3. Segurança em VoIP

O pesquisador Emilio Nakamura, do CPqD, falou em uma entrevista ao IPNews que o sistema de Voz sobre IP é seguro, mas que deve ser bem implementado para que não haja perigo de fraudes por parte de invasores. Segundo Nakamura (2010): “Se pensarmos em termos de segurança, os perigos de ataques por VoIP são maiores do que por telefone convencional, pois a voz sobre IP está conectada à rede, ou seja, qualquer dano na rede pode afetar a linha de telefonia por internet”.

Segundo Cabral (2010), o VoIP possui os mesmos riscos e vulnerabilidades presentes da rede IP, além de possuir riscos e vulnerabilidades específicos. Dito isso, um serviço VoIP não deve ser tratado como uma simples aplicação em uma rede IP, pois ele necessita de uma atenção especial, sendo ele um serviço complexo e de tempo real. Outro fato importante, é que cada elemento da infraestrutura de um serviço VoIP está acessível na rede e pode ser atacado ou usado para realizar ataques em toda rede.

> Se um atacante tiver êxito no seu ataque, pode passar a ter a acesso a servidores VoIP, provocar instabilidade do serviço, roubo de identidade,

> escutas telefônicas, redirecionamento de chamadas e sequestro de sessão. (CABRAL, 2010, p. 8)

Na telefonia convencional a intercepção de chamadas era feita no meio físico, colocando escutas. Já com VoIP, onde a voz é colocada em pacotes e enviada pela rede, pode ser mais acessível e fácil de interpretar por parte de invasores. Porém com a convergência de dados e voz em redes IP, torna-se possível utilizar de funcionalidades que não existiam na telefonia convencional, como a criptografia de dados de voz. (PASSITO et. al. 2004).

2.3.1. Mecanismos de defesa nos protocolos de sinalização

Segundo Passito et. al. (2004), uma das abordagens de segurança para VoIP é a adição de mecanismos de segurança nos protocolos de sinalização. Para o protocolo H.323 existe a recomendação H.235, que diz respeito a algoritmos de criptografia e autenticação a serem utilizados na comunicação de *gateways*, *gatekeepers* e terminais. Para o SIP existem soluções a serem implantadas nas mensagens de controle e no canal de mídia entre os *proxies* e os UA's.

A recomendação H.235 é uma estrutura de segurança para fornecer autenticação, confidencialidade e integridade, juntamente com os principais protocolos de troca para suportar comunicações para sistemas baseados em H.323. O H.235 recomenda mensagens, procedimentos, estruturas e algoritmos para segurança de sinalização, controle e comunicação de mídia em sistemas H.323. Ele fornece segurança de ponta-a-ponta além de suportar segurança *multicast* e *unicast*. Contudo ele requer um maior nível de complexidade de implementação para comunicações pela Internet, se comparado ao SIP. (PHITHAKKITNUKOON et. al., 2008).

O *Secure/Multipurpose Internet Main Extensions* (S/MIME) é definido pela RCF 3851 e pode fornecer para protocolos como o SMTP e o SIP: autenticação, confidencialidade de dados usando criptografia porto-a-ponto, integridade das mensagens e não-repúdio de origem usando assinaturas digitais. (RFC 3851, RAMSDELL, 2004).

Segundo Phithakkitnukoon et. al. (2008), o S/MIME também fornece confidencialidade de dados no SDP além de integridade das informações na parte SDP de uma mensagem SIP. Phithakkitnukoon et. al. (2008) também diz que a

implementação do S/MIME requer mais esforço devido sua complexidade e seus requisitos de infraestrutura.

O *Internet Protocol Security* (IPSec), de acordo com a RFC 6071 (Franquel e Krishnan, 2011), é uma suíte de protocolos que fornece segurança para as comunicações de internet na camada IP. Ele também pode ser usado para segurança de ponta-a-ponta. Outros protocolos da Internet também podem utilizar o IPSec para proteger parte do tráfego ou até mesmo todo o tráfego deles.

O IPSec fornece proteção a aplicações que usam para transporte o UDP ou TCP, e provem a confidencialidade, integridade e autenticação para sinalização e fluxos de mídia através da criação de túneis seguros entre dois pontos. Esses túneis seguros podem suportar TCP, UDP, RTP e SIP. (PHITHAKKITNUKOON et. al., 2008).

2.3.2. Mecanismos de defesa nos protocolos de transporte

A RFC 3711 (Baugher et. al., 2004) define o *Secure Real-time Transport Protocol* (SRTP) como um perfil do RTP, que pode fornecer confidencialidade, autenticação de mensagens e proteção de resposta para o trafego com RTP. Ele fornece também um framework para encriptação de fluxos RTP.

Numa comunicação com SRTP, antes mesmo de ser enviado qualquer fluxo de mídia existe uma negociação de chaves criptográficas entre as partes envolvidas na conexão. Assim garantindo a criptografia da carga útil dos pacotes transmitidos no tráfego RTP. (RIBEIRO, 2019).

Apesar do SRTP fornecer segurança para conteúdos de mídia, com confidencialidade, integridade e autenticação, ele não fornece a integridade da mensagem e autenticação ponto-a-ponto se o fluxo de mídia for de uma rede IP para uma rede de telefonia convencional. (PHITHAKKITNUKOON et. al., 2008).

Também defino pela RFC 3711 (Baugher et. al., 2004), o *Secure Real-time Transport Control Protocol* fornece os mesmos serviços de segurança para o RTCP, como o SRTP fornece para o RTP. Para que um pacote RTCP forme um pacote SRTCP equivalente, 3 novos campos são obrigatórios no cabeçalho RTCP: Um índice SRTCP, um sinalizador de criptografia e uma *tag* de autenticação.

2.3.3. Mecanismos de defesa para gerenciamento de chaves

O gerenciamento de chaves é essencial para proteção de aplicações multimídia pela internet, como o VoIP. Protocolos de segurança precisam de uma solução de gerenciamento de chaves para troca de chaves e parâmetros de segurança.

O *Multimedia Internet KEYing* (MIKEY) é um protocolo de gerenciamento de chaves para aplicações de real-time que é definida pela RFC 3830 (Arkko et. al. 2004), e tem seu uso para dar suporte ao SRTP. Segundo Phithakkitnukoon et. al. (2008), o MIKEY suporta negociação de chaves criptográficas e parâmetros de segurança para um ou mais protocolos de segurança. É Independente de um protocolo de comunicação específico, como SIP ou H.323.

O ZRTP é definido pela RFC 6189 (Zimmermann, Johnston e Callas, 2011) como um protocolo criptográfico de acordo de chaves para negociar as chaves de criptografia entre dois pontos para estabelecer uma sessão SRTP para aplicações de VOIP. Ele utiliza o algoritmo Diffie-Hellman para troca de chaves seguras, fornece confidencialidade, proteção contra os ataques do tipo Homem-no-Meio, e autenticação (caso o protocolo de sinalização forneça proteção de integridade ponto-a-ponto).

2.3.4. Técnicas de segurança para implantação VoIP

Existem várias alternativas para proteger uma infraestrutura VoIP dos diferentes ataques que um serviço em rede pode estar exposto, mas é necessário analisar cuidadosamente os custos e impactos que essas alternativas têm antes de aplicá-las. São apresentadas algumas dessas técnicas a seguir:

- **Separação do trafego de voz e dados:** separar os tráfegos de voz e dados em redes diferentes é uma alternativa para melhorar a segurança, pois pode prevenir ataques a partir de computadores na rede, impedindo que atacantes tenham uma entrada fácil a rede VoIP.

De acordo com Cabral (2010), com os dois tráfegos separados, pode-se utilizar ferramentas de segurança para cada um deles, já que nem toda ferramenta de segurança para uma rede de dados consegue proteger totalmente uma rede VoIP. A separação em redes diferentes ainda facilita a definição de regras de acesso, o que simplifica a configuração e o controle.

A separação da rede física pode se tornar muito caro, por isso essa separação é na maioria das vezes realizada usando a tecnologia de VLANs – *Virtual Area Network* (802.1q). Em uma rede que implementa VLANs os *switches* apenas permitem o roteamento entre dispositivos na mesma VLAN. Assim pode-se conectar Telefones IP na VLAN para VoIP e os outros dispositivos na VLAN para dados. (BUTCHER et. al., 2007).

Olchik (2006) comenta que essa técnica se torna um pouco complicada quando se trata do uso de *softphones* instalados em computadores, pois assim irão dividir a mesma rede, podendo deixar a rede VoIP exposta a ataques realizados sobre o computador do usuário. Já no caso de Telefones IP que possuem uma porta LAN extra para conexão de dados para um computador, esses devem implementar VLANs, para que o computador conectado seja colocado na VLAN de dados e não na de VoIP. (BUTCHER et. al., 2007).

- **Firewall**: a implementação de firewall visa bloquear o tráfego de fora da rede de acordo com regras e políticas de acesso, partindo da técnica de filtragem dos pacotes, onde são analisadas as informações contidas nos pacotes de voz, para identificar a legitimidade dos mesmos. Ele permite o controle de acesso ao segmento de redes de voz, filtrando todo tráfego enviado a rede de voz que não seja de utilidade do serviço de VoIP.
- **IP estático associado ao MAC *Address***: realizar o controle de acesso através da associação de um IP estático ao dispositivo por meio do seu MAC *Address* é uma forma de garantir que somente dispositivos autorizados tenham permissão para operar na rede. Assim, um dispositivo conectado na rede, passa por uma autenticação, só recebendo as configurações caso o seu Mac esteja na lista de controle de acesso.
- **DHCP separado para Voz e Dados**: junto com a separação dos tráfegos de Voz e Dados, ter servidores DHCP separados para cada segmento de rede garante que se um atacante realizar um ataque no servidor de configuração de uma rede de dados não afete a rede VoIP, e da mesma maneira, se o servidor DHCP da rede VoIP for atacado, que o funcionamento da rede de dados não seja afetado.

- **IDS e IPS**: O *Intrusion Detection System* (IDS) e o *Intrusion Prevention System* (IPS) são sistemas com a função de detectar pacotes maliciosos que venham a passar pelo *firewall*. A função do IDS é encontrar indícios de anomalias e situações suspeitas no funcionamento da rede e gerar alarmes e eventos ao administrador da rede. O IPS é diferente do IDS, pois ele é capaz de tratar os alertas e prevenir ataques através de ações especificas, como ações de bloqueio. (OLCHIK, 2006).
- Outras orientações: a estrutura VoIP deve ser mantida sempre bem atualizada, principalmente no que diz respeito aos softwares utilizados. Deve-se também utilizar equipamentos e softwares que sejam confiáveis, para que a segurança da rede não seja comprometida. É necessário ficar sempre atento às novas ameaças que podem afetar o VoIP e aos novos mecanismos de proteção. Os administradores de rede devem utilizar de ferramentas de monitoramento adequadas, para que possam identificar qualquer anomalia que venha a comprometer a segurança da rede, pois falhas na segurança da rede afetarão o VoIP.

2.3.5. Ameaças sobre VoIP

Ataques a redes VoIP são motivados por diversos fatores, desde acesso grátis a telefonia, ligações de longa distância grátis, personificação para cometer fraude, escutas telefônicas e interrupção do serviço. Nessa sessão serão descritas algumas ameaças ao serviço VoIP e algumas soluções propostas para segurança contra elas:

- **DoS (*Deny of Service*):** ataques do tipo negação de serviço (DoS) atacam a disponibilidade dos serviços, gerando perdas de receita, de produtividade, além de aumento nos custos devido a manutenções não previstas devido a degradação do serviço. Esses ataques podem ser direcionados a qualquer elemento da rede para interromper o funcionamento do sistema ou dos recursos de rede. (PHITHAKKITNUKOON et. al., 2008).

A partir de ataques DoS um atacante pode impedir o funcionamento normal do serviço VoIP, o que pode incluir a impossibilidade de realizar e receber chamadas. O ataque pode ser direcionado a todo o serviço, impossibilitando todas as chamadas,

ou ainda pode ser um ataque seletivo, impedindo as chamadas de determinados endereços. (BUTCHER et. al., 2007).

Algumas medidas são recomendadas contra os ataques de DoS em sistemas SIP de VoIP, dentre elas (PHITHAKKITNUKOON et. al., 2008):

- Monitoramento e filtro: manter uma lista de usuários suspeitos e bloqueá-los de estabelecer sessões.
- Autenticação: verificar a identidade dos usuários antes de encaminhas as mensagens do mesmo.
- *Stateless Proxy*: são servidores *proxy* que apenas encaminham as mensagens que recebem. Esses podem ser usados para executar outras verificações de segurança, como autenticação de usuários e filtragem de fontes de *spam*.

- ***Eavesdropping*** (Escuta Telefônica): é a tentativa de coletar informações sensíveis por meio do monitoramento da conversa de uma vítima com o intuito de coletar informações ou mesmo preparar um ataque. O atacante monitora a sinalização ou o conteúdo de mídia que são trocados entre os participantes de uma sessão.

Através de escutas telefônicas um atacante pode escutar e interpretar o tráfego na rede e conseguir obter nomes de usuários, senhas e a partir disso ter controle do plano de telefonia. Esse é um tipo de ataque que não altera os dados de usuários, porém afeta a confidencialidade das informações, pois essas ficam comprometidas. (CABRAL, 2010).

Algumas medidas para soluções contra os ataques de *eavesdropping* são: (PHITHAKKITNUKOON et. al., 2008)

- Utilizar hardwares confiáveis;
- Garantir que apenas pessoal autorizado tenha acesso ao cabeamento da rede;
- Implementar segurança de endereço MAC baseada em portas. Somente dispositivo com determinado MAC *Address* pode acessar determinada porta LAN.
- Verificar regularmente a rede em busca de dispositivos que estejam em execução no modo promíscuo.

- Usar os protocolos SRTP e SRTCP para segurança no transporte de pacotes.

- **Alteração do fluxo de voz:** esse é um ataque de substituição ou um ataque homem-no-meio. Conseguindo acesso ao fluxo de mídia RTP entre dois usuários em uma chamada, o atacante pode ouvir a comunicação entre dois usuários e até alterar a comunicação. A partir de gravações realizadas de sessões antigas, o atacante pode substituir partes da comunicação para que o destinatário receba uma mensagem diferente da enviada. Essa é uma ameaça que afeta a confidencialidade e a integridade do serviço VoIP. (BUTCHER et. al., 2007).

No Homem-no-meio o atacante intercepta uma sessão ativa e se apropria dela após autenticação, podendo se passar por outra pessoa para tentativas de fraude. Esse método é chamado também de sequestro de chamada dentro do universo VoIP. (RIBEIRO, 2019).

- **Manipulação de dados**: um *database* de registro de dados de chamadas contém informações sobre o número de chamadas que foram realizadas pelos usuários e para quem foram as chamadas, a hora, a duração e outras informações sobre a chamada. Com o acesso a uma base de registro de dados um atacante pode analisar padrões de chamadas e ter acesso a informações confidenciais.

Se um atacante consegue acesso de escrita ao *database*, ele pode manipular ou deletar os registros de chamadas. Esse método pode ser usado para fugir de pagamentos pelo serviço, ou para esconder atividades criminais mais sérias. O criminoso pode alterar, por exemplo, os números de telefones usados na chamada, escondendo suas atividades. (BUTCHER et. al., 2007).

- **SIP *Registration Hijack*** (Sequestro de registro SIP): cada usuário na rede SIP VoIP possui uma identificação própria no seu dispositivo, e com essa identificação o dispositivo se registra com um SIP *proxy*/registrar para que as chamadas possam ser redirecionadas para ele. O Sequestro de Registro acontece quando um atacante clona essa identificação para se registrar e substituir o registro legítimo do dono da identificação.

Com uma identificação clonada o dispositivo do atacante se registra no serviço VoIP como o dispositivo da vítima, assim toda ligação para o usuário clonado será redirecionada para o atacante, podendo esse se passar pela vítima. As ligações feitas pelo dispositivo do atacante também serão sinalizadas como feitas pelo dispositivo da vítima. (BUTCHER et. al., 2007).

- **SPIT** (*SPAM over Internet Telephony*): o SPAM é como ficou conhecido no âmbito do e-mail a habilidade de enviar múltiplas mensagens com pouco ou nenhum custo, para várias pessoas para oferecer produtos ou serviços, e até mesmo para realizar golpes. Com VoIP surgiu o *SPAM over Internet Telephony* (SPIT), principalmente por parte dos sistemas de telemarketing.

Atacantes podem criar servidores com listas de números telefônicos VoIP para serem usados para enviar mensagens em alto volume para a caixa de correio de voz da vítima. Esse é um problema até mais sério com VoIP do que com o e-mail, pois são necessários mecanismos de defesa de tempo real.

- ***Toll Fraud*** (Chamadas sem tarifação): o atacante leva o sistema a acreditar que o seu dispositivo é um dispositivo legítimo e tem acesso a realizar chamadas gratuitas, que não sejam tarifadas ou que sejam tarifadas para outros usuários. Essa é uma ameaça das mais críticas, pois a demora para descobrir o ataque pode causar enormes prejuízos financeiros.
- **SIP *Flooding*** (Inundação SIP): Esse ataque consiste no envio de inúmeras mensagens *INVITE* do SIP para iniciar conexões para os servidores SIP, desta forma há um acúmulo de solicitações de forma a degradar o serviço, pois o sistema não conseguirá mais atender às novas solicitações devido à falta de recursos, deixando ele inutilizável ou com a qualidade comprometida. (CABRAL, 2010).
- **SIP *Redirect:*** O SIP *Redirect* é um servidor que redireciona chamadas para um número, retornando para o remetente para onde a requisição deve ser enviada. Com isso é possível com um único número, conseguir ligar para um usuário onde quer que ele esteja. Porém se um atacante conseguir acesso ao servidor de redirecionamento, ele pode redirecionar

todas as chamadas realizadas a um determinado número para o seu próprio e receber as ligações no lugar da vítima.

O atacante pode ainda escolher desativar a rede, simplesmente redirecionando todas as ligações realizadas para um número que não existe. Se todas as chamadas forem redirecionadas a um número não existente, o sistema não será capaz de entregar as chamadas. (BUTCHER et. al., 2007).

- ***SIP Message Modification*** (Modificação de Mensagem SIP): as mensagens SIP não possuem um mecanismo próprio de integridade, por isso, a partir de um ataque do tipo homem-no-meio um atacante pode interceptar e modificar mensagens SIP, alterando alguns ou todos os parâmetros da mensagem. A partir disso, por exemplo, um atacante pode fazer com que a chamada de um usuário seja enviada para outro, sem o usuário perceber. O atacante pode redirecionar as chamadas para ele para tentativas de fraude.
- ***SIP Sinalling Loop*** (Repetição de Sinalização SIP): é um ataque onde um usuário é registrado em domínios diferentes, e quando o servidor SIP *proxy* recebe mensagens *INVITE* por meio desse ataque, as mensagens serão duplicadas nesses domínios, afetando o desempenho do sistema SIP. (RIBEIRO, 2019).
- ***VoIP Packet Replay Attack*** (Ataque de Resposta de Pacotes VoIP): o atacante captura os pacotes no fluxo VoIP e reenvia os mesmos fora da sequência, o que gera atraso e degradação da qualidade das chamadas.
- ***QoS Modification Attack*** (Ataque de Modificação de QoS): para que o QoS (Qualidade de Serviço) funcione, os pacotes de tempo real possuem marcadores para demonstrar que precisam de prioridade no tráfego de rede. Atacantes podem interceptar e modificar esses marcadores nos pacotes de tempo real para anular o mecanismo de QoS.
- ***VoIP Packet Injection*** (Injeção de Pacotes VoIP): consiste na injeção de pacotes VoIP falsificados nas chamadas ativas, como falas, ruídos e lacunas.
- ***Faked Call Teardown Message*** (Fraude de Mensagem de Término de Chamada) / *SIP Cancel/Bye Attack:* o objetivo desse ataque é encerrar

sessões SIP prematuramente, a partir do envio de mensagens *Bye/Cancel* aos dispositivos em chamada. Se um atacante enviar muitas mensagens dessa a um usuário, este ficara impossibilitado de enviar ou receber chamadas. O alvo do atacante pode ser também um gateway de sinalização, enviando mensagens *Bye/Cancel* o tempo todo, acarretando na negação de serviço aos usuários. (RIBEIRO, 2019).

3. METODOLOGIA

Após a exposição dos conceitos e técnicas de ataques a uma aplicação VoIP, realizou-se uma tentativa de *call eavesdropping* (escuta telefônica) na rede VoIP da Universidade Estadual do Maranhão – UEMA, sendo essa a aplicação VoIP utilizada nos telefones IP da Universidade e também nos terminais móveis (*smartphones*) dos técnicos do Núcleo de Tecnologia da Informação – NTI. O experimento foi realizado com o consentimento do chefe da Divisão de Redes e Datacenter – DRD do NTI. O experimento se dará por meio de dois testes. O primeiro teste fará a captura dos pacotes de voz pela rede Wi-Fi, e o segundo teste fará a captura dos pacotes por meio da rede cabeada. O diagrama das etapas da metodologia está descrito na Figura 8 abaixo:

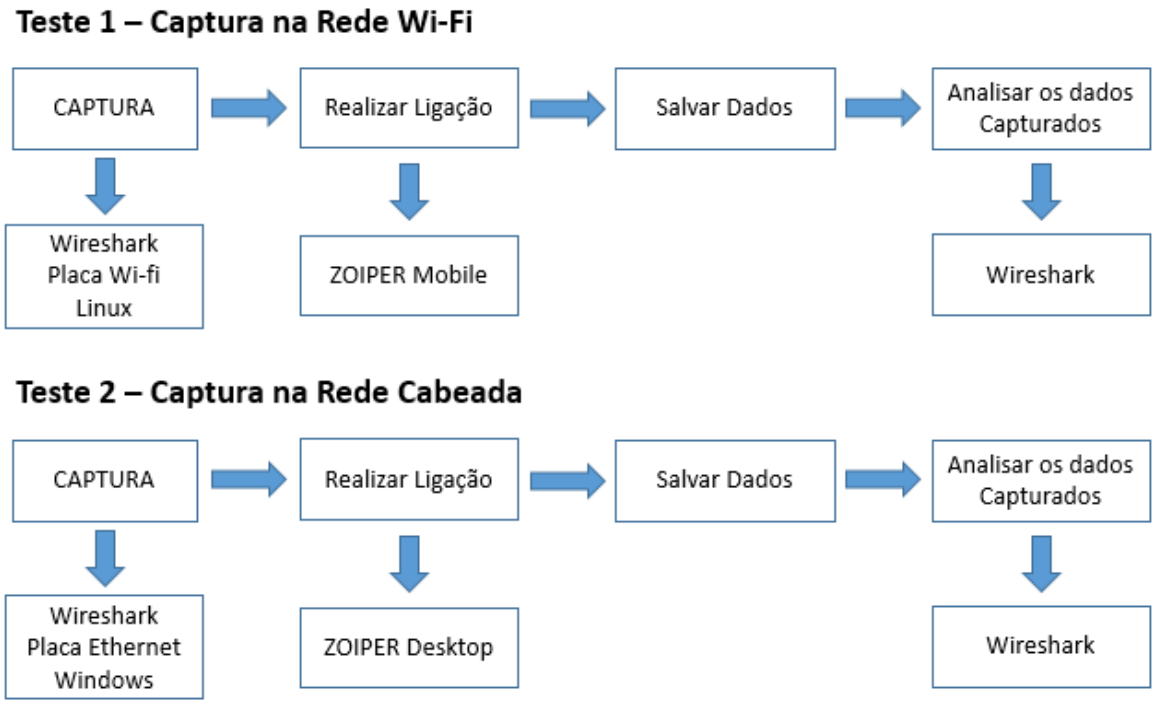

Figura 8: Diagrama de blocos da metodologia proposta.
Fonte: Autor, 2019.

3.1. Método de Captura

Para a captura de pacotes de rede existem vários *softwares*, tanto pagos quanto gratuitos. Como exemplos de *softwares* gratuitos temos: *Wireshark, Microsoft Network Monitor, Capsa Packet Sniffer, NetworkMiner e Sniffpass*. Para este trabalho o *software* utilizado para a captura dos pacotes foi o *Wireshark*, pois é um analisador de pacotes amplamente utilizado no mundo e seu desenvolvimento é dado por contribuições voluntárias de especialistas de redes ao redor do mundo. O projeto do

Wireshark foi iniciado em 1998 por Gerald Combs. Ele está disponível para os Sistemas Operacionais (SO) Windows, Linux, MacOS e outros.

É um *software* de fácil instalação e sua utilização para capturas de pacotes é de fácil inicialização, porém para a análise dos dados o usuário já necessita de um pouco mais de conhecimento. Para iniciar uma captura é necessário apenas escolher qual interface de rede utilizar na tela inicial do programa (Figura 9).

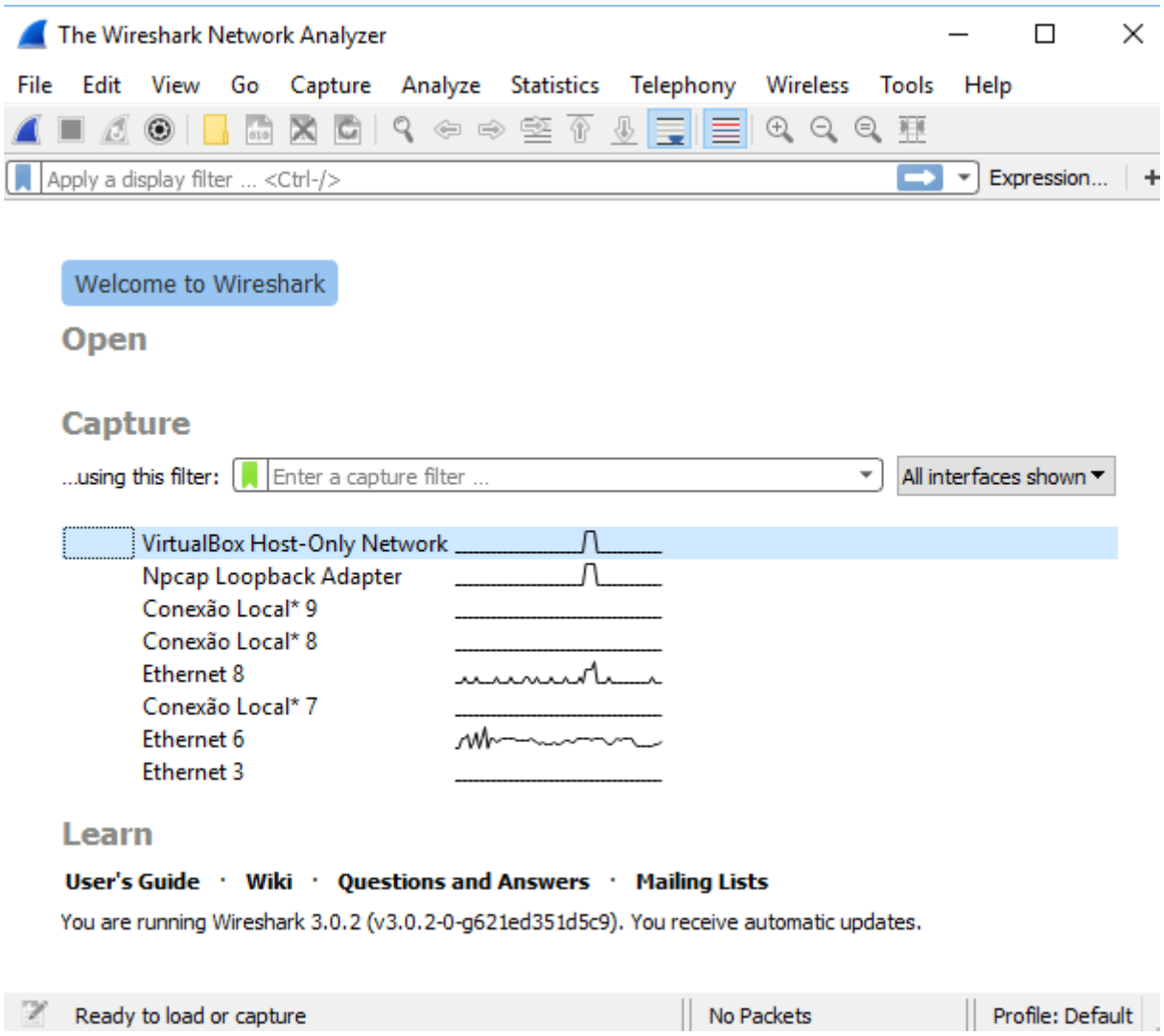

Figura 9: Wireshark.
Fonte: Autor, 2019.

O *Wireshark* irá colocar a interface de rede em modo promíscuo, nesse modo a interface capturará qualquer pacote que receba, mesmo não sendo endereçada a ela. Uma interface de rede que não esteja em modo promíscuo normalmente descarta os pacotes que não são destinados a ela.

Em especial para a captura pela rede Wi-Fi será necessário ativar o modo Monitor no Wireshark para a interface de rede Wi-Fi. Para que seja possível ativar

esse modo no Wireshark, a interface Wi-Fi deverá permitir ser colocada em modo Monitor e o Sistema Operacional deverá permitir tal ação. Para o teste com a rede Wi-Fi foi utilizado uma placa Wi-Fi USB e o sistema operacional Linux, pois este facilita o procedimento.

3.2. Experimento

O experimento foi composto de dois testes, sendo um a tentativa de captura dos pacotes de voz pela rede Wi-Fi e o segundo pela rede cabeada. Os testes serão descritos a seguir.

3.2.1. Captura de Pacotes de rede pela rede Wi-Fi

Todo o teste pela rede Wi-Fi foi realizado no sistema operacional Linux. Para o primeiro passo deste teste foi necessário a configuração da interface de rede Wi-Fi USB para o modo Monitor. Para realizar tal ação foram seguidos os seguintes passos:

- Abriu-se o terminal de comandos do Linux;
- Como demonstrado na Figura 10, inseriu-se o comando *iwconfig* para verificar se a interface Wi-Fi estava em funcionamento e para verificar o nome da interface, nesse caso: *wlx0036765543b1*;

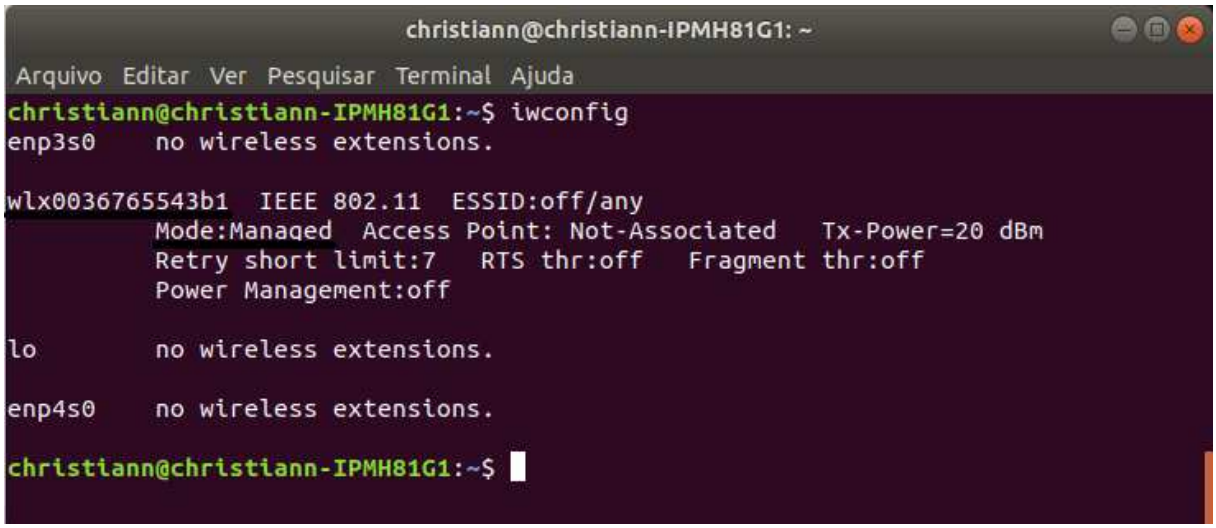

Figura 10: Comando iwconfig.
Fonte: Autor, 2019.

Os passos complementares estão mostrados na Figura 11, a seguir:

- Desativou-se a interface com o comando: *ifconfig wlx0036765543b1 down*;
- Alterou-se o modo da interface para Monitor com o comando: *iwconfig wlx0036765543b1 mode monitor*;

- Ativou-se novamente a interface: *ifconfig wlx0036765543b1 up*.
- E por fim inseriu-se novamente o comando *iwconfig* para verificar o modo de operação da interface *wlx0036765543b1*.

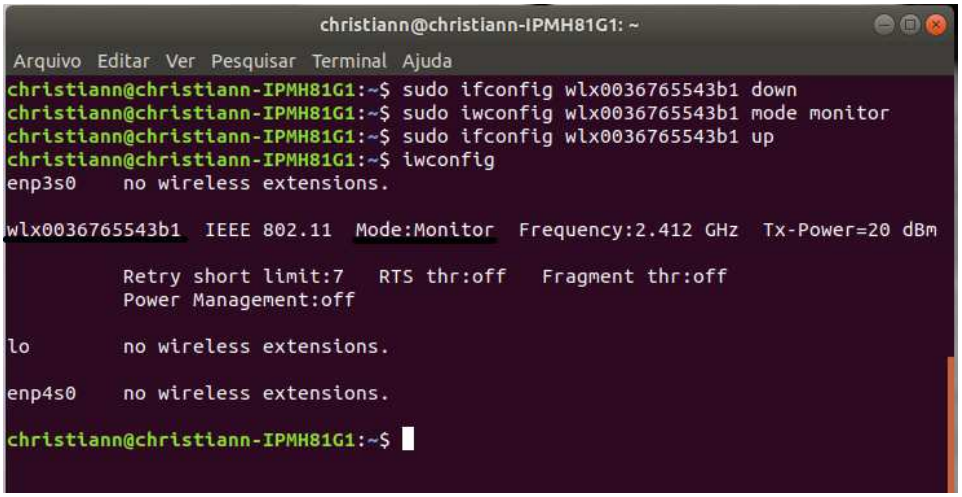

Figura 11: Passos complementares.
Fonte: Autor, 2019.

Após realizada essa configuração já é possível ativar o modo monitor no *Wireshark* e iniciar a captura de pacotes. A Figura 12, a seguir, mostra a ativação do modo Monitor (*Monitor Mode*) e *Promiscuous* no Wireshark para a interface de rede *wlx0036765543b1.*

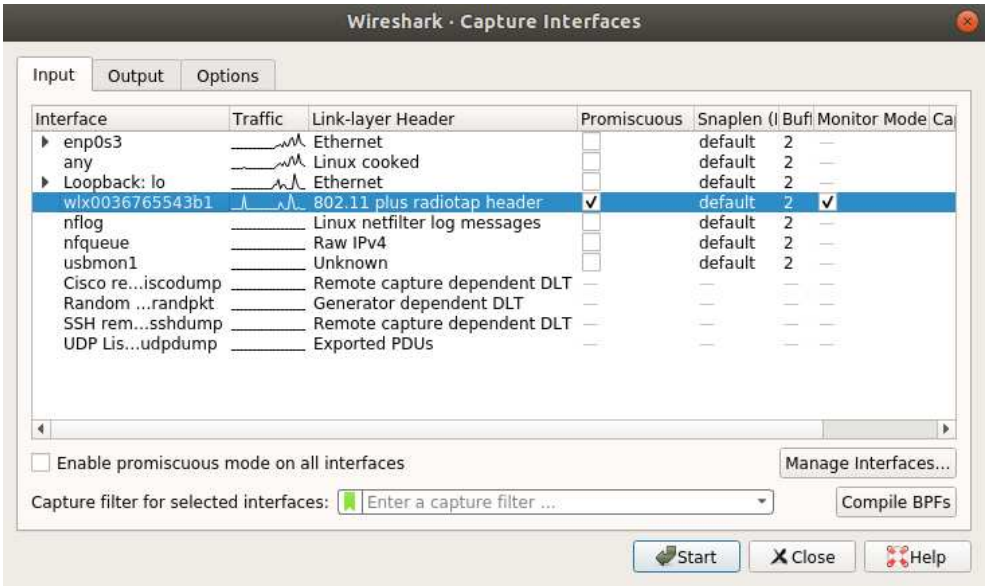

Figura 12: Modos Monitor e Promiscuous na interface Wi-Fi.
Fonte: Autor, 2019.

Após a captura iniciada, realizou-se uma ligação VoIP a partir do aplicativo *mobile* Zoiper no *smartphone,* utilizando a rede Wi-Fi, para o telefone IP instalado no *Helpdesk* do NTI. Após o término da ligação encerrou-se a captura dos pacotes e os dados obtidos foram salvos para posterior análise no arquivo *capturaWifi.pcapng*.

3.2.2. Captura de Pacotes de rede pela rede cabeada

O teste de captura dos pacotes pela rede cabeada foi realizado no sistema operacional *Windows*. Para o teste foi instalado um cliente VoIP (Zoiper) no computador usado para os testes e configurada uma conta VoIP, no caso a conta do próprio autor. A Figura 13, a seguir, mostra o Zoiper configurado.

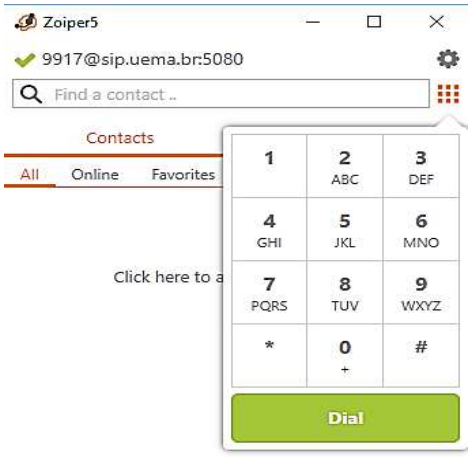

Figura 13: Zoiper configurado.
Fonte: Autor, 2019.

Após a configuração da aplicação VoIP, foi iniciado o Wireshark, selecionado a interface de rede ethernet (Conexão Local) para a captura de pacotes, e colocado em modo *Promiscuous*, conforme Figura 14.

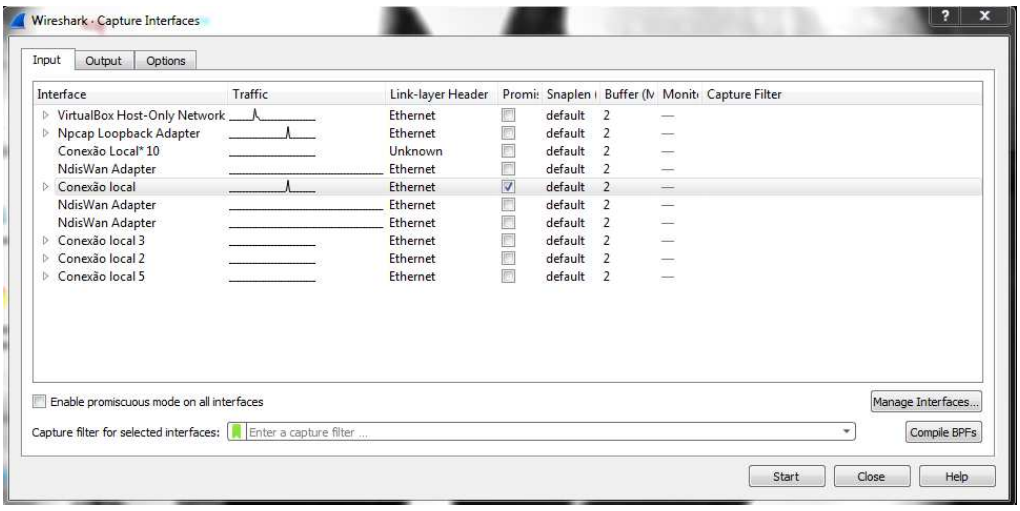

Figura 14: Modo Promiscuous na interface ethernet.
Fonte: Autor, 2019.

Assim que a captura foi iniciada, realizou-se uma ligação a partir cliente VoIP no computador para o telefone IP do *Helpdesk* do NTI. Após o término da ligação

encerrou-se a captura dos pacotes e os resultados foram salvos no arquivo *capturaCabeada.pcapng* para posterior análise.

4. RESULTADOS E DISCUSSÕES

Após a realização dos testes descritos no capítulo anterior, os dois arquivos gerados foram abertos usando o *Wireshark* para análise dos pacotes capturados, com o intuito de encontrar os pacotes RTP por onde a voz foi transmitida durante as ligações.

4.1. Análise da captura pela rede Wi-Fi

Para análise do arquivo da captura por Wi-Fi, o arquivo *capturaWifi.pcapng* foi aberto com o Wireshark e foi usado no campo de filtros o nome ***rtp***, o resultado pode ser visto na Figura 15.

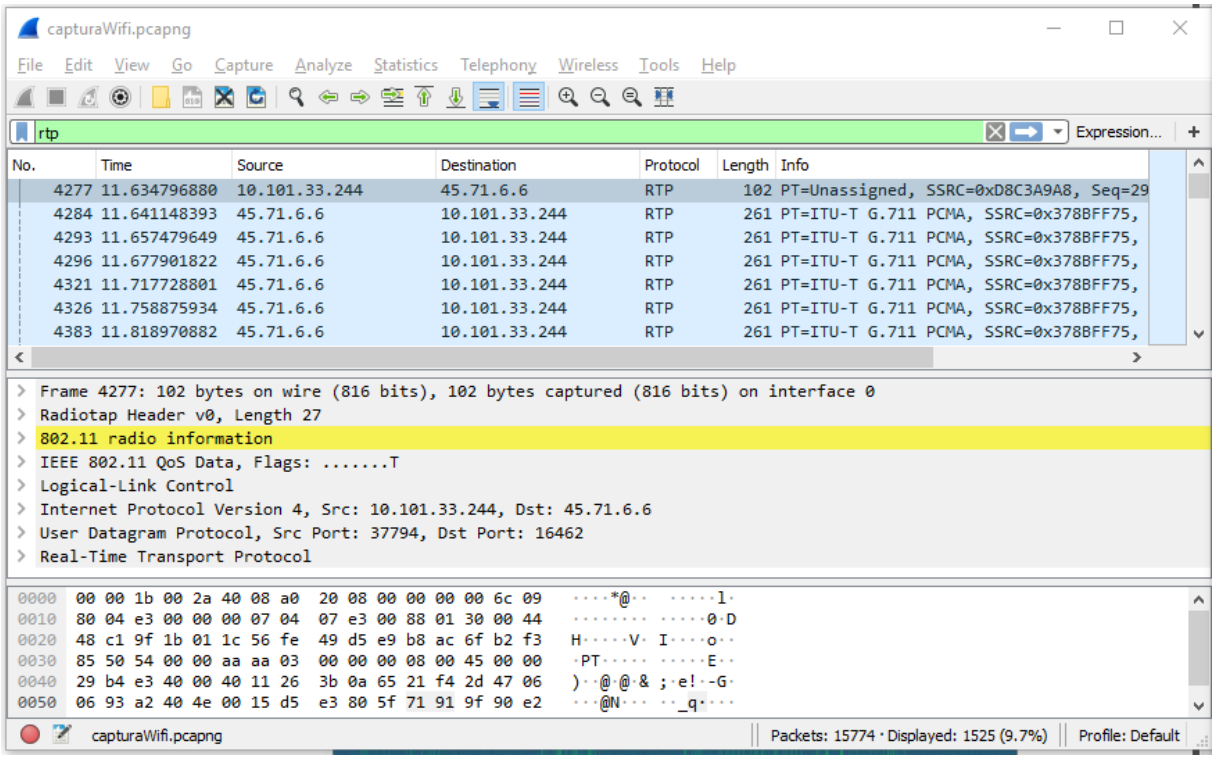

Figura 15: Filtro rtp na captura por Wi-Fi.
Fonte: Autor, 2019.

Como pode ser visto, os pacotes RTP foram capturados, o intuito agora é tentar ouvir a voz transmitida nesses pacotes. Para isso acessou-se o menu *Telephony* e clicando na função *VoIP Calls* o *Wireshark* listará a conversa VoIP capturada, exibindo os ramais remetente e destino, o protocolo usado para sinalização e a duração da chamada, entre outras informações conforme a Figura 16, a seguir.

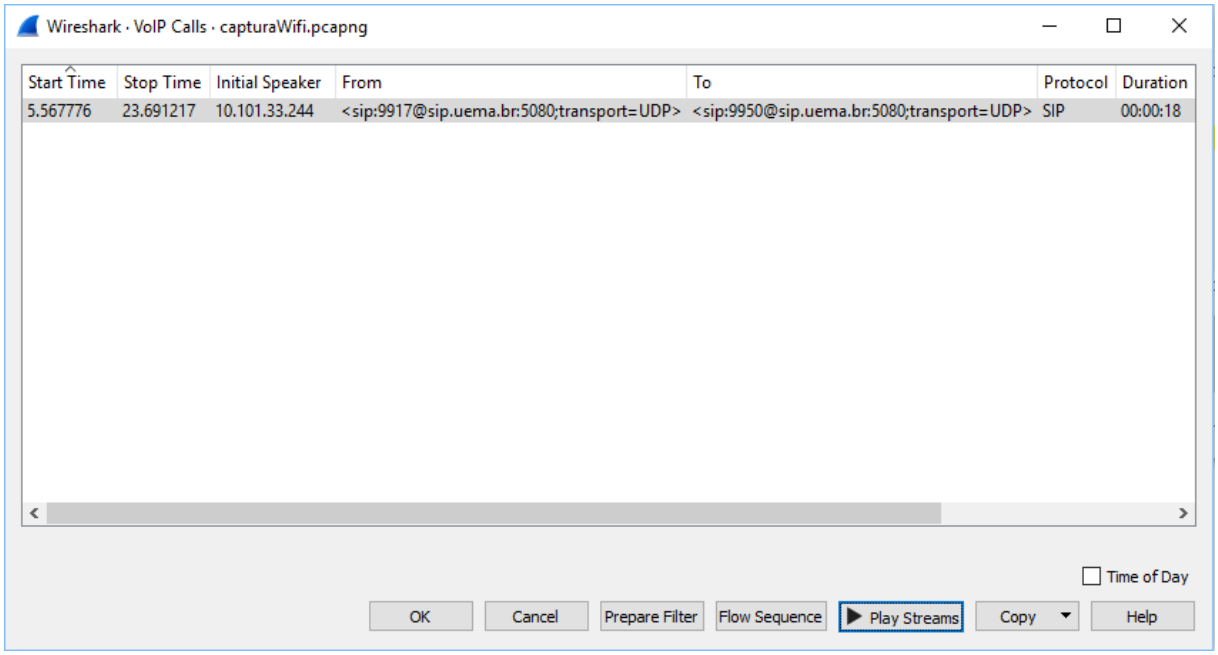

Figura 16: Conversa VoIP capturada por Wi-Fi.
Fonte: Autor, 2019.

Selecionando a opção *Play Streams* é aberto o *RTP Player* do *Wireshark*, e pode ser verificado na Figura 17 que o áudio foi capturado e pode ser ouvido. Porém ao executar o áudio, foi constatado que a qualidade do áudio não está boa e está praticamente incompreensível, com cortes e falas claramente fora de sequência.

Figura 17: Espectrograma da conversa capturada por Wi-Fi.
Fonte: Autor, 2019.

Verificando outra ferramenta do Wireshark, o *RTP Streams*, verificou-se que o motivo da péssima qualidade é devido a uma grande perda dos pacotes durante a captura Wi-Fi, além dos muitos pacotes com o número de sequência incorreto como pode ser visto na Figura 18.

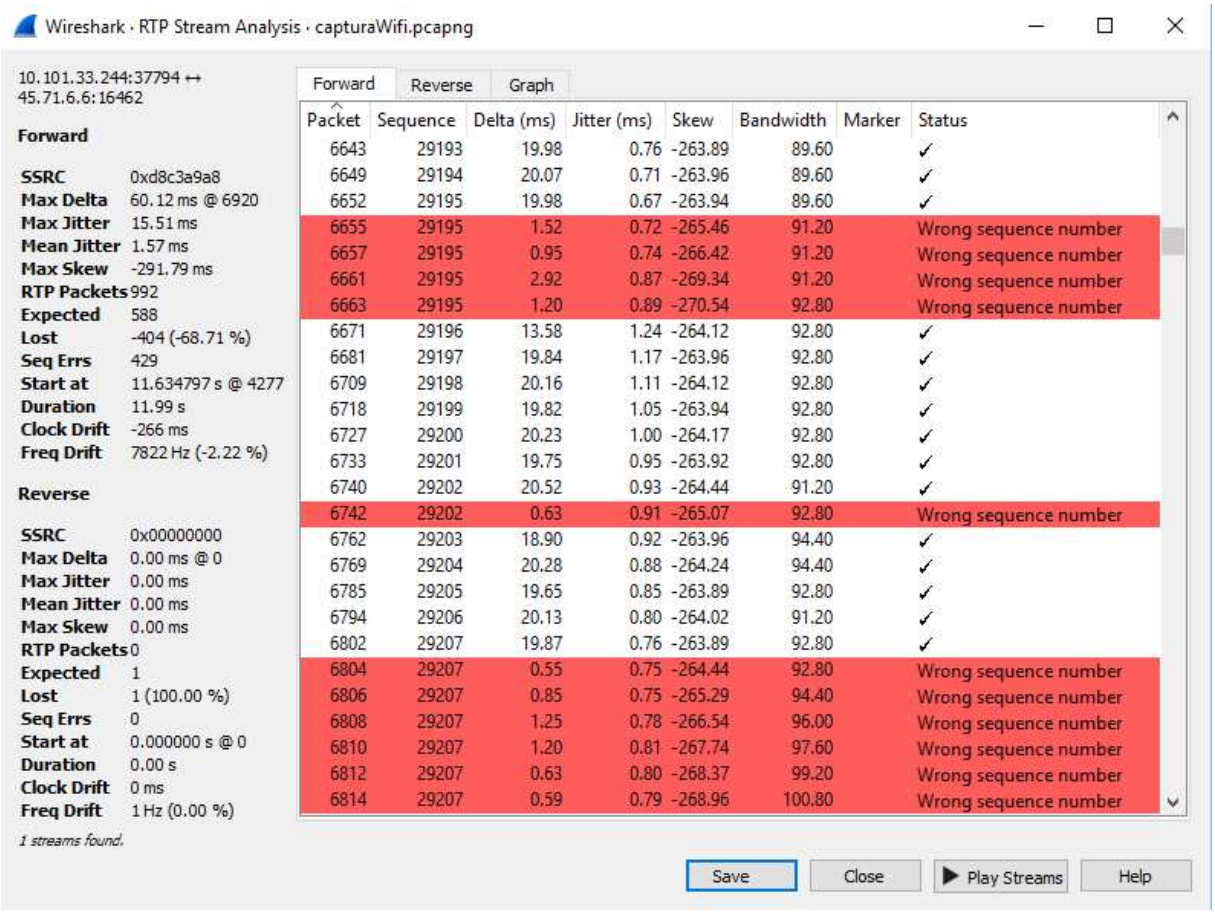

Figura 18: Análise do fluxo RTP capturado por Wi-Fi.
Fonte: Autor, 2019.

Essas dificuldades encontradas provavelmente estão atreladas à qualidade do equipamento utilizado para captura, por ser uma placa Wi-Fi USB de baixo custo, e por não ter uma placa Wi-Fi mais robusta não foi possível tentar realizar uma captura mais precisa dos pacotes RTP. Porém ainda assim foi possível realizar a captura dos pacotes e realizar a escuta telefônica, mostrando que os pacotes RTP não estão protegidos e estão suscetíveis a um ataque *eavesdropping*.

Apesar da perda de pacotes, é possível ouvir o áudio, sem os pacotes fora de ordem, ao utilizar a função do wireshark de exportar os fluxos de áudio, assim ele faz o tratamento desse fluxo, excluindo os pacotes fora de ordem. Após isso é só unir os fluxos com qualquer editor de áudio e a conversa pode ser ouvida e compreendida.

Um ponto a se destacar sobre o Wi-Fi é o fato da rede UEMA, que é a rede Wi-Fi utilizada por toda a comunidade da Universidade, ser uma rede aberta, sem segurança de senha, onde o *login* só é realizado após a conexão com a rede, por meio de um *Captive Portal*. Por ser uma rede aberta, o seu tráfego não é criptografado, sendo assim possível capturar todos os pacotes, o que passa a ser uma brecha de segurança fácil de ser utilizada por pessoas mal-intencionadas, já que elas não precisam nem estar logadas na rede para realizar as capturas dos pacotes. É necessário simplesmente se manter em uma área com cobertura dessa rede Wi-Fi e começar a capturar os pacotes.

4.2. Análise da captura pela rede cabeada

Para análise do arquivo da captura pela rede cabeada, abriu-se o arquivo *capturaCabeada.pcapng* com o *Wireshark* e usou-se a palavra ***rtp*** no campo de filtros, o resultado pode ser visto na Figura 19.

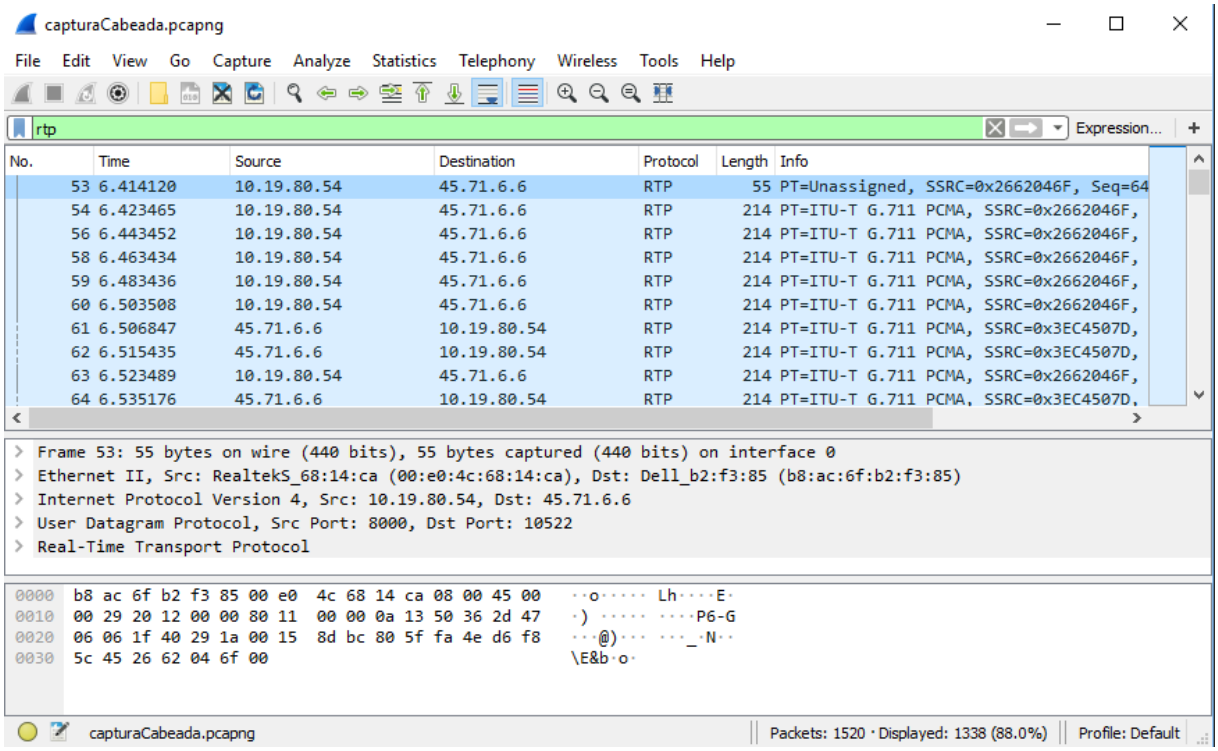

Figura 19: Filtro rtp na captura cabeada.
Fonte: Autor, 2019.

Após ser verificado que os pacotes RTP foram capturados, acessou-se novamente a função *VoIP Calls* e teve-se acesso a conversa transmitida pelos pacotes RTP. Ao clicar no *Play Streams* foi verificado que, diferente da captura por

Wi-Fi, o espectrograma do áudio estava mais estável (Figura 20), e ao ouvir se pode compreender inteiramente o conteúdo da conversa.

Figura 20: Espectrograma da conversa capturada na rede cabeada.
Fonte: Autor, 2019.

Por questões de comparação com a captura por Wi-Fi, acessando a função *RTP Streams*, pode ser visto na Figura 21 que a captura foi um sucesso, não havendo perdas de pacotes e nem pacotes fora de sequência. Assim mais uma vez provou-se que o fluxo RTP do sistema VoIP testado não está protegido, podendo sofrer um ataque *eavesdropping*.

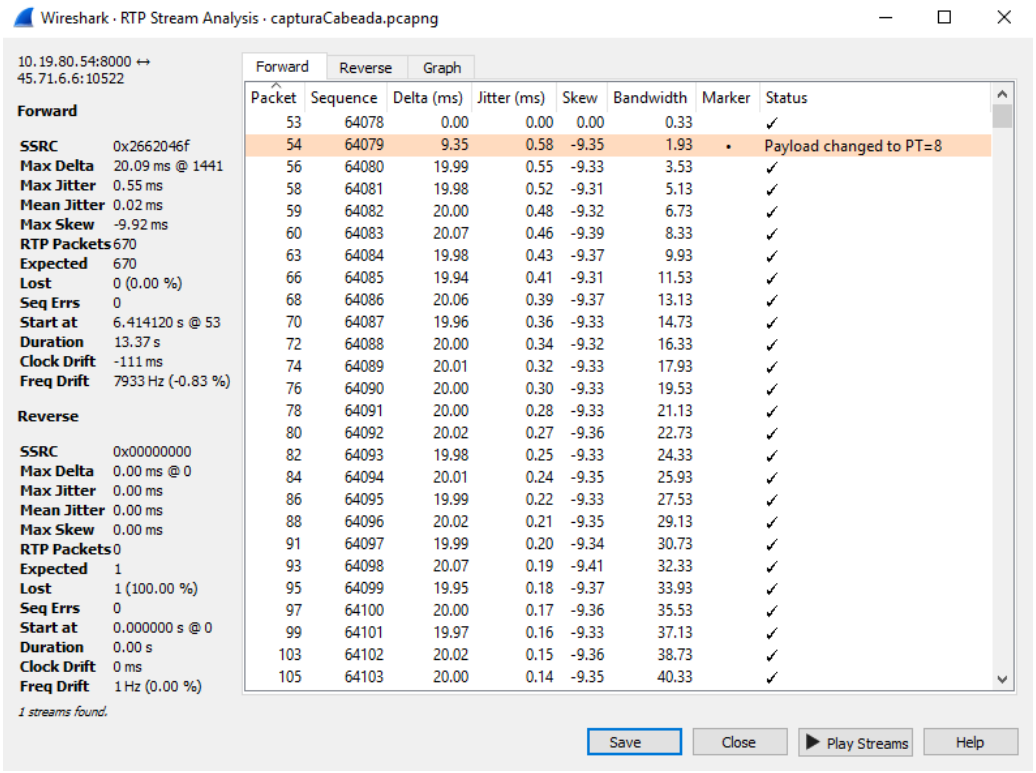

Figura 21: Análise do fluxo RTP capturado pela rede cabeada.
Fonte: Autor, 2019.

4.3. Implementação de segurança

Como foi mostrado anteriormente no item 2.3.5, existem alguns métodos para implantação de segurança para proteger o sistema de um ataque *eavesdropping*, como por exemplo, manter os *switches* da rede restrito onde apenas pessoal autorizado tenha acesso, pois se um atacante tiver acesso ao *switch*, a captura de pacotes se torna mais fácil.

Outro método importante é verificar regularmente a rede à procura de dispositivos em execução no modo promíscuo, pois como foi visto anteriormente, o *Wireshark* coloca a interface de internet em modo promíscuo para capturar os pacotes que não são destinados a essa interface. Ao encontrar um dispositivo nesse modo o administrador da rede pode encerrar sua conexão.

Para conexões Wi-Fi é importante manter a rede com segurança de senha, pois assim o tráfego será criptografado e, mesmo que o atacante tenha acesso a senha, ele não conseguirá realizar a capturar dos pacotes, tornando a tentativa de *eavesdropping* uma tarefa mais difícil para o atacante que pretende usar a rede Wi-Fi como meio.

Outra sugestão para melhorar a segurança é a separação das redes de voz e de dados. Fazer essa separação fisicamente pode se tornar muito custoso, e por isso se sugere o uso de VLANs, sendo uma para cada tipo de rede. Assim, com os tráfegos separados, pode-se utilizar ferramentas específicas para cada tipo de rede, além de facilitar definição de regras de acesso como, por exemplo, liberação de acesso por MAC do telefone, simplificando a configuração e controle da rede.

Apesar da eficácia dos métodos acima, eles são complementares. É necessária uma segurança na transmissão dos pacotes de mídia no VoIP, e para isso tem-se o SRTP, como já descrito anteriormente ele é responsável por criptografar os pacotes transmitidos pelo protocolo RTP.

A partir da versão 11 o Asterisk (*software* para implementação de VoIP) já possui suporte nativo para o SRTP, porém essa função vem desabilitada por padrão, por ser uma função opcional, e também por consumir processamento extra. É necessário apenas ativar o SRTP para se ter o fluxo de mídia do VoIP criptografado. Vale ressaltar que a segurança deve estar habilitada em ambos os pontos para funcionar, então é necessário ativar o SRTP tanto na aplicação quanto nos dispositivos VoIP.

É necessário também proteger a troca de mensagens de sinalização do SIP, pois toda a troca de chaves para a criptografia do tráfego de mídia do SRTP é realizada em texto puro durante a troca das mensagens. Para isso pode-se utilizar o TLS, que criptografa as mensagens de sinalização, reforçando a segurança do SRTP.

Para demonstrar a efetividade do uso do SRTP, criou-se uma máquina virtual em laboratório e instalou-se o FreePBX versão 10.13.66, que possui o Asterisk 13. Após a instalação criou-se dois ramais (1001 e 1002), e como pode ser visto na Figura 22, foi habilitada para os ramais a criptografia de mídia por SRTP.

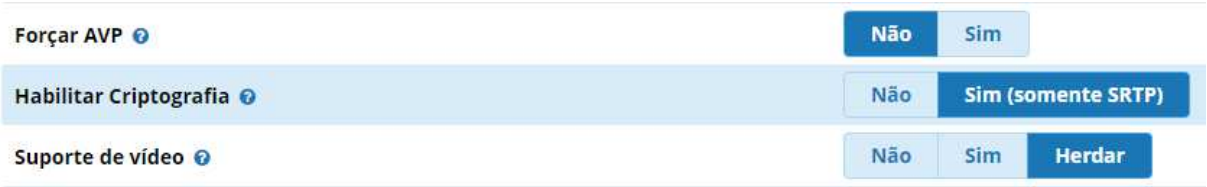

Figura 22: Habilitar SRTP na configuração de ramais
Fonte: Autor, 2019.

Como dito anteriormente, é necessário que não apenas o sistema VoIP tenha SRTP, mas que os dispositivos dos usuários também. Tendo em vista isso, utilizou-se a aplicação *MicroSIP* para *desktop* e o aplicativo *SessionTalk Softphone* no

smartphone android, pois essas são aplicações grátis e que dão suporte a utilização do SRTP.

Após configurados os ramais e habilitada a segurança de mídia por SRTP em cada aplicação, iniciou-se a captura com o *wireshark* e realizou-se uma ligação entre os ramais. Após a coleta do tráfego, utilizou-se novamente o *wireshark* para análise e como pode ser visto na Figura 23, o resultado foi um áudio apenas de ruído.

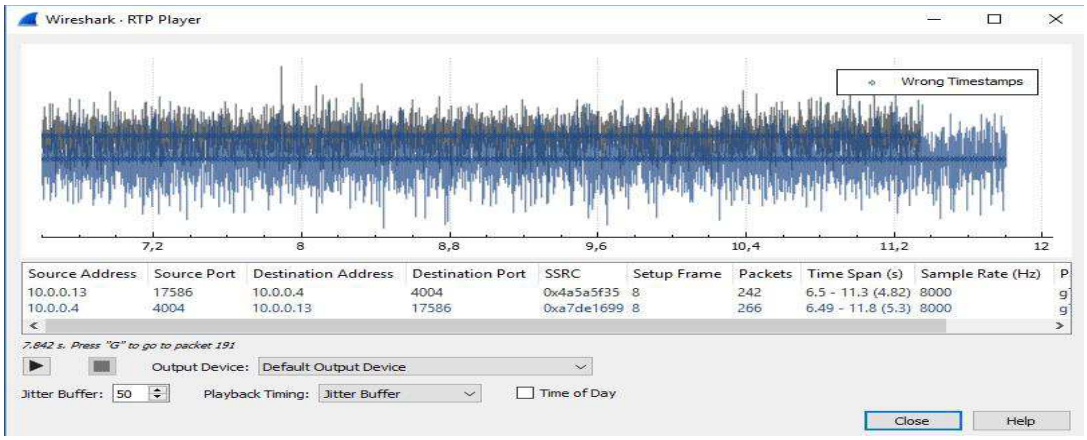

Figura 23: Fluxo de áudio com SRTP
Fonte: Autor, 2019.

5. CONCLUSÃO

A segurança de uma rede VoIP é de extrema importância, pois ataques a esses sistemas são comuns, por exemplo para buscar informações sobre determinada empresa que tragam benefícios a concorrentes, e as vezes até mesmo para realizar ligações por meio de aplicações de terceiros sem necessitar pagar pela utilização, deixando o custo para a empresa ou para um outro usuário.

Nesse trabalho foi apresentado o funcionamento do VoIP e seus protocolos, analisadas as técnicas de segurança e apresentadas algumas das diversas formas de ataques que são utilizadas para comprometer aplicações VoIP. Foi realizada uma tentativa bem-sucedida de *eavesdropping* na aplicação VoIP da UEMA utilizada nos telefones IP, demonstrando a falta de segurança no tráfego de mídia de tal aplicação. Após a realização dos testes percebeu-se que sem segurança no tráfego de mídia, toda a conversa em uma ligação VoIP pode ser capturada e reproduzida, deixando a aplicação VoIP com um grave problema de confidencialidade.

Como demonstrado com o teste em laboratório, a utilização do protocolo SRTP é viável e funciona, por isso a utilização deste foi o principal ponto abordado na sugestão de implantação de segurança, levando em conta que sua utilização deve ser

aplicada junto com uma solução de criptografia para as mensagens SIP, no caso a sugerida foi a utilização do TLS.

O objetivo do trabalho foi alcançado, pois foi possível encontrar uma vulnerabilidade na aplicação VoIP em estudo, e demonstrar a consequência dessa vulnerabilidade por meio de um ataque bem-sucedido. Além de demonstrar em outra aplicação que a sugestão dada para segurança funciona.

As Sugestões dadas para a implementação de segurança foram repassadas para os técnicos do NTI. Deixar a rede Wi-Fi UEMA com segurança de senha, deixar o acesso aos switches restritos, configurar os ramais com SRTP, verificar os telefones IP por suporte ao SRTP.

5.1. Sugestões para trabalhos futuros

Para o desenvolvimento de trabalhos futuros são sugeridos os seguintes:

- Analisar a segurança de uma aplicação VoIP quanto a ataques de *SIP Registration Hijack* (Sequestro de registro SIP), na tentativa de se passar por outro usuário.
- Mostrar que uma aplicação VoIP com STRP sem o uso do TLS não mantém o transporte dos dados da aplicação 100% em segurança.
- Analisar a segurança de uma aplicação que utiliza o protocolo H.323 como protocolo de sinalização ao invés do SIP.

REFERÊNCIAS

ALECRIM, Emerson. **Tecnologia Voip**. Disponível em: <http://www.infowester.com/voip.php>. Acesso em: 18 nov. 2018.

ANTON. Marcelo Bublitz. **UMA PROPOSTA DE ARQUITETURA VOIP PARA SMARTPHONES COM SITEMA OPERACIONAL ANDROID**. 2011. 74f. Trabalho de Conclusão de Curso - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2011. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/31024/000782119.pdf>. Acesso em: 25 maio 2019.

ARKKO, J. et al. **RFC 3830 - MIKEY: Multimedia Internet KEYing.** Disponível em: <https://tools.ietf.org/html/rfc3830>. Acesso em: 31 maio 2019.

ARMÊNIO NETO, João; GRAEML, Alexandre Reis. **VoIP: Inovação Disruptiva no Mercado de Telefonia Corporativa**. Revista Alcance, Biguaçu, vol 17, núm. 1, p. 7-21, jan-mar. 2010.

BAUGHER, M. et al. **RFC 3711 - The Secure Real-time Transport Protocol (SRTP).** Disponível em: <https://tools.ietf.org/html/rfc3711>. Acesso em: 31 maio 2019.

BERNAL FILHO, Huber. **Telefonia IP.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialtelip/pagina_3.asp>. Acesso em: 27 maio 2019.

BORDIM, Jacir L. **Introdução à Voz sobre IP e Asterisk**. 2010. 260 p. Disponível em: <https://www.portalgsti.com.br/2014/04/voip-voz-sobre-ip-e-asterisk-ebook-gratuito.html>. Acesso em: 24 maio 2019.

BUTCHER, David; LI, Xiangyang; GUO, Jinhua. (2007). **Security Challenge and Defense in VoIP Infrastructures.** Disponível em: < https://www.researchgate.net/publication/3421877_Security_Challenge_and_Defense_in_VoIP_Infrastructures>. Acesso em: 30 maio 2019.

CABRAL, Elder Leandro. **SEGURANÇA EM AMBIENTES VOIP: RISCOS E VULNERABILIDADES**. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS09A/Eder%20Leandro%20Cabral%20-%20RSS09A.pdf>. Acesso em: 28 nov. 2018.

CARDOSO, Rômulo Mendes. **VoIP.** Disponível em: <https://www.gta.ufrj.br/grad/04_2/VoIP/CaptuloIIntroduo.html>. Acesso 27 maio 2019.

CLEMENTE, Ricardo Gomes. **UMA SOLUÇÃO DE STREAMING DE VÍDEO PARA CELULARES: CONCEITOS, PROTOCOLOS E APLICATIVO.** 2006. 64fl. Trabalho de Conclusão de Curso – Universidade Federal do Rio de Janeiro, 2006. Disponível em: <https://www.gta.ufrj.br/ftp/gta/TechReports/Clemente06/Clemente06.pdf>. Acesso: 27 maio 2019

GOODE, Bur. **Voice over Internet protocol (VoIP)**. Disponível em: < https://www.researchgate.net/publication/2986029_Voice_over_Internet_protocol_VoIP>. Acesso em 19 maio 2019.

IPNEWS. **Segurança em VoIP: nem os telefones IP estão isentos de fraudes.** Disponível em: <https://ipnews.com.br/seguranem-voip-nem-os-telefones-ip-estisentos-de-fraudes/>. Acesso em: 30 maio 2019.

KUROSE, Jim F. ROSS, Keith W. **Redes de computadores e a internet.** 6 ed. São Paulo: Pearson Education do Brasil, 2013.

LESSA, E. M.; SOUZA, L. C. X. **VOICE OVER IP.** Disponível em: <https://www.gta.ufrj.br/grad/07_1/voip/principal.htm>. Acesso em 19 maio 2019.

MORENO, Jose Ignacio; SOTO, Ignacio; LARRABEITI, David. **Protocolos de Señalización para el transporte de Voz sobre redes IP.** Novática: Revista de la Asociación de Técnicos de Informática, núm. 151, p. 14-20, maio-jun. 2001. Disponível em: <https://e-archivo.uc3m.es/bitstream/handle/10016/4295/protocolos_soto_N_2001.pdf?sequence=1&isAllowed=y>. Acesso em: 27 maio 2019.

OLCHIK, Alejandro. **Segurança em Voz Sobre IP.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialsegvoip/pagina_5.asp>. Acesso em: 31 maio 2019.

OLIVEIRA, Júlio César Mondadori de. **MeGaCo: Conheça o protocolo de sinalização de Mídia Gateways VoIP.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialmegaco/pagina_1.asp>. Acesso em: 27 maio 2019.

PASSITO, Alexandre. **Análise de desempenho de tráfego VoIP utilizando o Protocolo IP Security.** Disponível em: <https://www.researchgate.net/profile/Edjair_Mota2/publication/228754530_Analise_de_desempenho_de_trafego_VoIP_utilizando_o_Protocolo_IP_Security/links/0046351d244fbbc7ea000000/Analise-de-desempenho-de-trafego-VoIP-utilizando-o-Protocolo-IP-Security.pdf>. Acesso em: 30 maio 2019.

PAZ, Glauco Aguiar da. **VoIP I: Análise e Desempenho da Tecnologia VoIP via Rede PLC Indoor Residencial.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoipindoor1/default.asp>. Acesso em 24 maio 2019.

PERKINS, Colin. **RTP: Audio and Video for the Internet.** Boston: Pearson Education, Inc. 2002.

PHITHAKKITNUKOON, Santi; DANTU, Ram; BAATARJAV, Enkh-Amgalan. (2008). **VoIP Security - Attacks and Solutions.** Disponível em: < https://www.researchgate.net/publication/220449868_VoIP_Security_-_Attacks_and_Solutions>. Acesso em: 30 maio 2019.

PILON, Guilherme. **SIP - O protocolo para convergência nas redes de nova geração.** Disponível em: <http://www.tcc.sc.usp.br/tce/disponiveis/97/970010/tce-

23022015-141107>. Acesso em: 28 nov. 2018.

RAMSDELL, B. **RFC 3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification**. Disponível em: <https://www.ietf.org/rfc/rfc3851.txt>. Acesso em: 30 maio 2019.

REGISTRO. **Introdução ao Protocolo SIP**. Disponível em: <http://eng.registro.br/inoc/SIP_iNOC.pdf>. Acesso em: 18 nov. 2018.

Revista Gestão Universitária. **Voip - uma revolução nas telecomunicações e sua aplicabilidade no cotidiano dos usuários da internet**. Disponível em: <http://gestaouniversitaria.com.br/artigos/voip-uma-revolucao-nas-telecomunicacoes-e-sua-aplicabilidade-no-cotidiano-dos-usuarios-da-internet>. Acesso em: 19 maio 2019.

RIBEIRO, Glaucia. **VoIP.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoipconv2/default.asp>. Acesso em: 12 de nov. 2018.

RIBEIRO, N. J.; MENDES, L. A. M. **VoIP – Tecnologia de Voz sobre IP**. Disponível em: <http://ftp.unipac.br/site/bb/tcc/tcc-6930aa4e21db90a985797092d43a775c.pdf>. Acesso em: 28 nov. 2018.

RIBEIRO. Glaucia da Silva. **Voz sobre IP I: A Convergência de Dados e Voz.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoipconv/default.asp>. Acesso em: 12 nov. 2018.

ROSENBERG, J. **RFC 3261 - SIP: Session Initiation Protocol.** Disponível em: <https://tools.ietf.org/html/rfc3261>. Acesso em: 28 maio 2019.

ROSS, Julio. **VoIP - Voz sobre IP.** Rio de Janeiro: Antenna Edições Técnicas Ltda., 2007.

SANTOS, Carlos César dos. et al. **VOZ - SOBRE IP: TECNOLOGIAS, UTILIZAÇÃO E CRESCIMENTO.** Disponível em: <http://www.ria.net.br/index.php/ria/article/download/9/9>. Acesso em: 24 maio 2019.

SCHWEITZER, Vitor. **Propostas de segurança para o ambiente de telefonia IP da Universidade Federal de Santa Catarina.** Disponível em: <https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/182182/Monografia_Vitor_Schweitzer.pdf>. Acesso em: 28 nov. 2018.

SOUZA, Wendley. **Protocolos VOIP**. Disponível em <https://brasilescola.uol.com.br/informatica/protocolos-voip.htm>. Acesso em: 28 maio 2019.

TANENBAUM, Andrew S. **Redes de Computadores.** 4 ed. Rio de Janeiro: Editora Campos Elsevier, 2003.

TW SOLUTION TELECOM. **Protocolos VoIP: quais são os principais e como funcionam?.** Disponível em: <https://www.twsolutions.com.br/protocolos-voip-quais-sao-os-principais-e-como-funcionam/>. Acesso em: 27 maio 2019.

VAZ, Igor; DINAU, Priscilla. UFRJ. **Sip**. Disponível em: <http://www.gta.ufrj.br/grad/06_1/sip/Definindooqueumprotocolodesinalizao.html>. Acesso em: 14 nov. 2018.

VOIP do Brasil. **A História do Voip**. Disponível em: <https://www.voipdobrasil.com.br/blog/a_historia_do_voip/>. Acesso em: 19 maio 2019.

YOSHIOKA, Sergio. **Protocolos para telefonia IP.** 2003. 60f. Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Computação, Campinas, SP. Disponível em: <http://www.repositorio.unicamp.br/handle/REPOSIP/276306>. Acesso em: 27 maio 2019.

ZIMMERMANN, P.; JOHNSTON, A.; CALLAS, J. **RFC 6189 - ZRTP: Media Path Key Agreement for Unicast Secure RTP.** Disponível em: <https://tools.ietf.org/html/rfc6189>. Acesso em: 31 maio 2019.

APENDICE I

UNIVERSIDADE ESTADUAL DO MARANHÃO – UEMA
CENTRO DE CIÊNCIAS TECNOLÓGICAS – CCT
CURSO DE ENGENHARIA DA COMPUTAÇÃO

Termo de Anuência

Eu, Luís Carlos Costa Fonseca, Coordenador de Tecnologia da Informação e Comunicação, autorizo a realização da pesquisa “Análise da segurança do ambiente de telefonia VoIP da Universidade Estadual do Maranhão” a ser realizada pelo aluno Christiann Dênys da Fonseca Vieira, do curso de Engenharia da Computação, acompanhado pelo seu orientador, o Professor Wesley Batista Dominices de Araújo, Mestre em Engenharia de Computação.

Autorizo aos pesquisadores a realizarem a tentativa de ataque a rede de telefonia VoIP da Universidade Estadual do Maranhão, a qual envolve uma tentativa de escuta telefônica, com o intuito de encontrar uma vulnerabilidade de segurança.

Ao mesmo tempo os pesquisadores se comprometem a repassar todos os achados para a equipe técnica da UEMA e manter sigilo até que as devidas correções sejam aplicadas.

São Luís, 01 de maio de 2019.

_____

Prof. Luís Carlos Costa Fonseca
Doutor em Informática na Educação
Coordenador de Tecnologia da Informação e Comunicação – CTIC

_____

Prof. Wesley Batista Dominices de Araújo (Orientador)
Mestre em Engenharia de Computação
Universidade Estadual do Maranhão

_____

Christiann Dênys da Fonseca Vieira
Graduando em Engenharia da Computação