

ANÁLISE DE DESEMPENHO DOS CODECS SUPORTADOS PELO ASTERISK COM E SEM CRIPTOGRAFIA

Ricardo c. C. Ferrari¹

Rafael M. Jesus¹

Elerson Gaetti-Jardim Jr.³

Ailton A. Shinoda¹

Christiane M. Schweitzer²

¹Departamento de Engenharia Elétrica, FEIS/UNESP, Ilha Solteira, São Paulo

²Departamento de Matemática, FEIS/UNESP, Ilha Solteira, São Paulo

³Departamento da Patologia e Propedêutica Clínica, FOA-UNESP, Araçatuba-SP, Brasil

RESUMO

O objetivo principal do trabalho é analisar o desempenho de alguns codecs suportados pelo Asterisk com e sem criptografia utilizando o protocolo RTP e SRTP, respectivamente, oferecendo dados importantes para uma tomada de decisão na implementação de um sistema VoIP com o Asterisk. Assim, é possível perceber que tanto os codecs como o protocolo podem ser escolhidos dependendo da aplicação, ou seja, se a característica principal do sistema é velocidade na troca de pacotes, nível de segurança ou menor tolerância para chamadas mal sucedidas. Para isso, foram feitos testes com os codecs, com e sem o uso de criptografia, para obter algumas conclusões sobre o uso de dos mesmos, dando mais atenção para o tempo de resposta para o início de uma chamada.

Palavras-chave: VoIP, Asterisk, SRTP.

ABSTRACT

The main objective is to analyze the performance of some codecs supported by Asterisk with and without encryption using RTP and SRTP, respectively, providing important data for decision-making in the implementation of a VoIP system with Asterisk. Thus, it is possible to realize both codecs as the protocol can be chosen depending on the application, or the system's main feature is the speed packet switching, security level or lower tolerance for unsuccessful calls. For this, tests were made with the codec with and without the use of cryptography to obtain some findings on the use of the same, giving more attention to the response time for the start of a call.

Keywords: VoIP, Asterisk, SRTP.

1 INTRODUÇÃO

Com o aumento na utilização da internet e da necessidade de se comunicar por meio de telefonia, as tecnologias VoIP evoluíram, proporcionando mais escalabilidade em relação à telefonia tradicional de comutação de circuitos, permitindo novas funcionalidades, como correio de voz, música e espera, transferência de chamadas e conferências, com baixo custo. Sendo possíveis estas funcionalidades através da internet ou uma rede IP privada.

Neste trabalho, serão analisados aspectos de desempenho e segurança, para que seja feita a escolha correta para determinado tipo de aplicação VoIP, ou seja, uma instalação e configuração de um PBX (*Private Branch eXchange*) Asterisk, pois cada aplicação pode ter necessidades diferentes.

O Asterisk é um software open source e gratuito que suporta vários protocolos (SIP, IAX e H.323) e codecs (G.711, SPEEX, GSM, iLBC, AMR, G.723, G.726, G.729 e G722), permitindo tanto a utilização de telefones em software (softfones), como telefones físicos (telefones VoIP ou telefones comuns com adaptadores).

Os testes são realizados em uma rede com um servidor, um cliente e um espião, com cenários possuindo codecs diferentes utilizando criptografia ou não para a realização das chamadas. Assim, alguns codecs são comparados para identificar quais são suas características no mesmo ambiente utilizando os protocolos RTP e SRTP, identificando taxa de chamadas mal sucedidas, tempo médio de resposta e vulnerabilidade na comunicação.

Considera-se uma chamada mal sucedida, aquela que não é inicializada e finalizada perfeitamente, ou seja, com todos os pacotes necessários recebidos pelas duas partes na comunicação. Já a média de tempo de resposta, refere-se ao intervalo de tempo que o cliente faz o convite da chamada e a chamada é estabelecida. Por fim, a vulnerabilidade sendo uma possível escuta não autorizada da chamada pelo espião com quase nenhum esforço, apenas utilizando uma ferramenta de captura de pacotes com sua instalação padrão. Nas chamadas realizadas pelo cliente o servidor é capaz de atender e responder com uma gravação pré-definida.

O trabalho está organizado da seguinte forma. No capítulo 2 serão apresentados uma visão geral sobre transporte de voz sobre IP, como estado da arte, aplicações e transmissão de conteúdo de multimídia. No capítulo 3 são discutidos aspectos de roteamento, desempenho e segurança dos protocolos de VoIP, sendo eles, H.323, SIP e 3GPP. No capítulo 4 são descritos alguns codecs suportados pelo Asterisk, são eles: G.711, G.722, G.726, G.729, GSM, iLBC e SPEEX. No capítulo 5 encontra-se os requisitos e métricas de desempenho para serviços de VoIP. No capítulo 6 estão as características e aplicações do Asterisk. Por fim, mas não menos importante estão as experimentações e testes realizados para definir as diferenças entre os codecs, utilizando ou não criptografia, principalmente tratando-se de desempenho. Concluindo, no capítulo 8 são dadas as conclusões e trabalhos que ainda podem ser feitos futuramente.

2 TRABALHOS RELACIONADOS

Pesquisas estão sendo realizadas no intuito de analisar a escolha do codec para determinado tipo de aplicação. O trabalho desenvolvido por RUGHINIS E ICONARU (2008, p. 61-64), apresenta uma análise do desempenho do servidor Asterisk como um servidor SIP e seu consumo de largura de banda, utilizando o codec G.711. Já em (SOUSA, 2008), é feito um trabalho mais aprofundado com várias alterações nas configurações do Asterisk, com chamadas ponto a ponto, chamadas em conferência e chamadas interativas, sendo que para todos os testes foram utilizados codecs diferentes para análise de desempenho e segurança na transmissão dos dados. Por fim, em (VILLACIS, ACOST e LARA CUEVA, 2013, P. 22-24) é analisado o desempenho dos protocolos SIP e IAX combinados com os codecs GSM, G.711, SPEEX e G.726, com foco no uso de CPU e memória RAM, alcançando o melhor desempenho com o uso do protocolo IAX e o codec GSM.

3 ASTERISK

Com o aumento das redes IP (*Internet Protocol*) surgiu a ideia de transmitir voz utilizando essa infraestrutura, com isso foi criada a tecnologia VoIP, ou seja, voz sobre IP. Desta forma, vieram novas soluções. Em 1999 Mark Spencer criou uma central telefônica PABX (*Private Automatic Branch eXchange*) em software chamado Asterisk. Esse software é distribuído pela empresa Digium com licença GPL (GNU General Public License).

Por se tratar de uma distribuição GPL o Asterisk conta com programadores em todo o mundo, segundo KELLER (2011) aproximadamente 400 colaboradores ativos, desenvolvendo novas funcionalidades, melhorando as existentes e corrigindo erros do software.

O Asterisk foi desenvolvido para Linux, mas hoje pode ser instalado e executado em diversos sistemas operacionais, como: Windows, FreeBSD, OpenBSD, NetBSD, Mac OS e Solaris.

Através de protocolos como, SIP, H.323, IAX2 e MGCP o Asterisk pode possuir funcionalidades de URAs (Unidade de Resposta Audível), correio de voz, conferência e distribuição de chamadas, sendo capaz de ser incrementado com módulos escritos em C e scripts AGIs (Asterisk Gateway Interface).

Basicamente as operações feitas pelo Asterisk usam quatro componentes:

- Protocolos: MGCP, IAX2, SIP, H.323, RTP e outros;
- Canal de comunicação (Ramal): Identificação do cliente no sistema;
- Codecs: forma de digitalização do áudio para transporte na rede;
- Tipos da aplicação: ações do Asterisk, como atender canal (*Answer*), aguarda um tempo (*Wait*) e tocar arquivo de áudio (*PlayBack*).

3.1 Aspectos de Desempenho e Segurança

Para garantir o desempenho de um sistema VoIP precisamos primeiro garantir a infraestrutura de rede que esse sistema vai utilizar, pois o Asterisk implanta a utilização de VoIP e isso quer dizer que tráfego de áudio vai ser transmitido em uma rede TCP/IP (KELLER, 2011). Depois de garantir o bom funcionamento da rede, devemos nos preocupar com algumas questões para definir qual a melhor configuração do servidor. Assim, algumas características devem ser analisadas, como o total de chamadas simultâneas, se haverá gravação de voz e a banda disponível. Segundo KELLER (2011) os processos que mais consomem o servidor são codificação, decodificação e gravação de chamadas. Com isso, a Digium informa que para 120 chamadas simultâneas com codecs G.711 e G.729a é necessário um servidor Intel Dual Xeon 3.0 Ghz, 4 GB de RAM, já testes realizados por KELLER (2011) indicam 300 chamadas simultâneas com codec G.711 com um AMD Sempron 2800 e 1 GB de RAM.

De acordo com KELLER (2011), a segurança está relacionada ao grau de importância, disponibilidade e qualidade do sistema telefônico. Assim quatro itens são considerados essenciais:

- Encriptação do áudio;
- Interoperabilidade entre fabricantes e desenvolvedores;
- Servidores e criptografia totalmente seguros;
- Gerenciamento centralizado.

Como essas características não refletem a realidade em um ambiente VoIP, algumas ameaças são frequentes, como visto em (KELLER, 2011):

- Negação de Serviço (Denial of Service – DoS);
- Ataque de modificação de QoS;
- Injeção de pacotes VoIP;
- Sequestro de chamadas ou interceptação;
- Sequestro de registro.

Para se prevenir contra essas ameaças alguns cuidados devem ser tomados, como limitar o acesso de pessoas ao servidor, privilégios no login remoto, atualização do sistema operacional, separar infraestrutura de rede de dados e de telefonia, firewall, limitar número de chamadas simultâneas e esquema de autenticação (KELLER, 2011).

4 CODECS

Como definido em (SOUSA, 2008), o codec, que é a concatenação de duas palavras (COder/DECoder), é um algoritmo para codificar e decodificar fluxos de voz. Como ouvimos o som na forma analógica, para enviar em uma rede de pacotes IP é necessário a conversão de analógico para digital. Assim, o processo inverso é realizado no receptor, passando de digital para analógico, para que o usuário possa ouvir. Existem várias formas para codificar e decodificar os dados, sendo que um dos

objetivos pode ser a redução de largura de banda durante a transmissão dos pacotes. Sendo assim, podemos considerar que um bom codec pode codificar e decodificar um fluxo de voz no menor tempo possível, mantendo a qualidade/eficiência na conversação entre as partes envolvidas. Considerando que a largura de banda em uma rede é sempre finita, a quantidade de chamadas simultâneas que uma conexão permite está relacionada ao codec que está sendo utilizado. Alguns codecs possuem o recurso de detecção de silêncio, muito útil para diminuir a utilização da rede quando pacotes não estão sendo transmitidos. Um ruído mais baixo pode ser gerado apenas para dar a sensação de que a ligação não caiu.

Existem vários codecs para sistemas VoIP, na Tabela 1 podemos ver os principais e suas taxas de bits (SMITH, MEGGELEN e MADSEN, 2005 e VOIP-INFO, 2013):

Tabela 1 – Codecs

Codec	Taxa de bits (Kbits/s)
G.711	64
G.722	48 / 56 / 64
G.726	16 / 24 / 32 / 40
G.729	8
GSM	13
iLBC	13,3 / 15,2
Speex	2,15 – 24,6

Fonte: Adaptada de (SMITH, MEGGELEN e MADSEN, 2005 e VOIP-INFO, 2013)

4.1 G.711

De acordo com VOIP-INFO (2013), G.711 é um padrão ITU (International Telecommunication Union) com alta taxa de bits (64 Kbps), sendo considerado a língua nativa da rede de telefonia digital moderna, sendo suportado pela maioria dos provedores VoIP. Embora padronizado em 1988, foi inventado por Bell Systems e introduzido no início dos anos 70. Existem duas versões do codec: A-law e U-law. O padrão U-law é usado na América do Norte e no Japão, já o A-law é usado no resto do mundo. A diferença está no método do sinal analógico a ser amostrado. Em ambos os regimes, o sinal não é amostrado de forma linear, mas de forma logarítmica. A-law prevê uma gama mais dinâmica ao contrário de U-law. O resultado é um som menos "confuso", como artefatos de amostragem são melhor suprimida. O G.711 para VoIP vai dar uma melhor qualidade de voz, uma vez que é o mesmo codec usado pela rede PSTN (Public Switched Telephone Network) e ISDN (Integrated Services Digital Network), como se estivesse usando um telefone comum ou ISDN. Ele também tem baixa latência, porque existe pouca ou nenhuma necessidade de buferização, que exige mais processamento. A desvantagem é que ele tem mais largura de banda do que outros codecs, até 84 Kbps, incluindo toda a sobrecarga do UDP e IP. No entanto, com o aumento da largura de banda larga, isso não deve ser um problema.

Em (SMITH, MEGGELEN e MADSEN, 2005) diz que muitas pessoas podem dizer que o G.711 é um codec descompactado. Isso não é exatamente verdadeiro, pois compactação (técnica de compressão e expansão de sinais para efeitos de redução de ruídos e quantização) é considerada uma forma de compressão. O que é verdade é que o G.711 é o codec de base do qual todos os outros são derivados.

4.2 G.722

De acordo com PERETZ e GUMUSOGLU (2004), o G.722 foi padronizado em 1988, sendo o primeiro algoritmo de codificação de banda larga padronizado para ser utilizado com uma taxa de amostragem de 16 kHz. O Codec G.722 leva 14 bits de dados em 16 kHz (largura de banda de 50 Hz a 7 kHz) e comprime 224 kbit/s para 64, 56 e 48 kbit/s de acordo com o modo selecionado. O sistema de codificação utiliza *Sub-Band Adaptive Differential Pulse code modulation* (SB-ADPCM) dentro uma taxa de bits de 64 kbit/s. O codificador G.722 utiliza 64 kbit/s, em todos os momentos, independentemente do modo de operação, porém o descodificador utiliza 64, 56, ou 48 kbit/s, dependendo do modo de operação.

Em (CISCO, 2013) também podemos ver que à medida que o poder de processamento do processador de sinal digital aumenta, a capacidade de dispositivos de voz, para executar um algoritmo de compressão de voz torna-se mais fácil e mais barata. Assim, houve uma mudança no mundo da voz para proporcionar qualidade de voz e o codec mais utilizado para proporcionar melhor qualidade de voz para voz sobre IP é o G.722 de banda larga. O G.721, definido 7 anos antes, define Adaptive Differential PCM (ADPCM) e apresenta a capacidade de reduzir o fluxo de dados de áudio de 64 para 16 kbps. A recomendação G.722 usou o mesmo ADPCM para compressão de voz, mas em vez de comprimir 64 kbps para 16 kbps como G.721, G.722 manteve a mesma taxa de bits, mas dobrou o conteúdo de áudio. Dobrar o conteúdo de áudio significou que o codec G.722 poderia apoiar uma faixa de frequência de voz maior dentro do mesmo fluxo de 64 kbps. O aumento da faixa de resposta é aparente quando você compara as amostras do codec G.722 com o G.711. O Codec G.711 tem uma taxa de amostragem de 8 kHz e qualquer sinal acima de 3,44 kHz é bloqueada. Com o G.722, a taxa de amostragem é aumentada para 16 kHz, dobrando a faixa de frequências. G.722 funciona por ter o sinal de voz de entrada em um filtro digital que separa o sinal de áudio de 0-4 kHz e 4-8 kHz. Estas sub-bandas são codificadas usando ADPCM. Como a maioria da energia de voz está concentrada na metade inferior da faixa de áudio (0-4 kHz), 48 kbps de banda é dedicada para a sub-banda inferior e os outros 16 kbps atribuídos a sub-banda superior. Ao realizar a codificação ADPCM em cada sub-banda separadamente, G.722 pode fornecer ambas as frequências baixas e altas que irá fornecer o áudio mais rico e melhor na recriação do sinal original.

4.3 G.726

Como visto em SMITH, MEGGELEN e MADSEN (2005) o codec G.726 também é conhecido como Adaptive Differential Pulse-Code Modulation (ADPCM) e pode ser executado em várias taxas de bits, sendo que as taxas mais comuns são de 16 Kbps, 24 Kbps e 32 Kbps. Como pode ser confirmado nos testes deste trabalho, o Asterisk atualmente suporta apenas a taxa ADPCM-32, que é de longe a taxa mais popular para este codec. O codec G.726 oferece quase a mesma qualidade do codec G.711, porém utiliza apenas metade da largura de banda. Isto é possível porque em vez de enviar o resultado da medição de quantização, envia somente a informação necessária para descrever a diferença entre a amostra atual e a anterior. Apesar dos pontos fortes do G.726 ele acabou entrando em crise em 1990, devido à sua incapacidade para transportar sinais de fax e modem, mas por causa de seu desempenho banda larga/CPU está retornando. Por fim, o G.726 acaba sendo um codec interessante pois não exige uma grande quantidade de trabalho computacional do sistema.

Assim, IFSC (2013) conclui que o codec G.726 possui uma qualidade parecida com o codec G.711, mas consumindo menos banda. Outra conclusão é que ele está perdendo espaço para o codec G.729, pois não trabalha com bandas tão baixas quanto as trabalhadas pelo G.729, mas ainda é muito usado em sistemas telefônicos.

4.4 G.729

Conforme SMITH, MEGGELEN e MADSEN (2005), mesmo que o codec G.729A utiliza pouca largura de banda, ainda assim proporciona qualidade de som impressionante, fazendo isso através do uso de *Conjugate-Structure Algebraic-Code-Excited Linear Prediction* (CS-ACELP). Por causa de patentes, para o uso desse é necessário o pagamento de uma taxa de licenciamento, porém é extremamente popular e possui suporte muitos celulares e sistemas diferentes. Para conseguir essa taxa de compressão impressionante, o codec requer uma quantidade de esforço de CPU na mesma proporção.

Segundo DIGIUM (2013), o codec G.729 comprime a carga para 8kbit/s, dando-lhe até vezes de capacidade na mesma conexão. Ideal para uso em cenários de banda limitada, como: conexões ADSL, serviço de VoIP internacional, conexões via satélite, etc. Várias versões do G.729 são definidos de acordo com os padrões da indústria. Asterisk e Digium possuem uma implementação de apoio do G.729 (G.729a).

A CISCO está incluindo no Cisco Unity 2.4.5. O codec é usado na gravação e reprodução de mensagens de voz e pode ser uma alternativa para o codec de u-Law, que foi utilizado no passado. u-Law ainda é o codec padrão, mas G.729a agora pode ser selecionado pelo administrador se preferir. Sites que permitirem o suporte não sentirão impacto significativo sobre o uso da CPU, como descrito em CISCO (2013).

4.5 GSM

Nas palavras de SMITH, MEGGELEN e MADSEN (2005), GSM (Sistema Global para Comunicações Móveis) é o queridinho dos codecs no Asterisk. Esse codec não vem sobrecarregado com a exigência de licenciamento da maneira que G.729A faz e oferece um excelente desempenho no que diz respeito à demanda de CPU. A qualidade do som é geralmente considerado como sendo de um grau menor do que a produzida por G.729A, mas grande parte disso se resume a opinião pessoal.

Como descrito por VOIP-INFO (2013), o GSM inclui um codec, muitas vezes referida apenas como o GSM quando se discute codecs. A “Full Rate” do codec de voz GSM opera em uma taxa de 13 kbp e é chamado de RPE-LTP (*Regular Pulse Excitation Long-Term Prediction*). Este codec usa as informações a partir de amostras anteriores, a fim de prever o tamanho da amostra. O sinal de voz é dividida em blocos de 20 ms e estes blocos são então passadas para o codec de voz, de modo a obter blocos de 260 bits. Mais recentes sistemas GSM utilizam um par de codecs mais atuais:

- EFR (*Enhanced Full Rate*) utiliza ACELP (*Algebraic Code Excited Linear Prediction*);
- HR (*Half Rate*) utiliza CELP-VSELP (*Code Excited Linear Prediction - Vector Sum Excited Linear Prediction*).

O GSM fornece boa qualidade, sendo que sua principal vantagem em relação a outros codecs de taxa baixa é a sua simplicidade e custo/benefício.

4.6 iLBC

Conforme SMITH, MEGGELEN e MADSEN (2005), o codec iLBC (*Internet Low Bitrate Codec*) fornece uma mistura atraente de baixo uso de banda e qualidade e especialmente adequado para sustentar uma qualidade razoável em links de rede com perdas. Possui suporte ao Asterisk, mas não é tão populares como os codecs ITU, podendo não ser compatível com telefones IP comuns e sistemas VoIP comerciais. IETF RFC 3951 e 3952 foram publicados em apoio iLBC e iLBC e aprovou a padronização do codec iLBC, como pode ser visto em VOIP-INFO (2013). Pelo fato do iLBC utilizar algoritmos complexos para atingir os seus elevados níveis de compressão, acaba tendo um custo relativamente elevado de CPU no Asterisk. Enquanto você está autorizado a usar o iLBC sem pagar taxas, o titular da patente iLBC, GIPS (*Global IP Sound*), quer saber quando o codec for utilizado em uma aplicação comercial. A maneira de fazer isso é fazendo o download e imprimir uma cópia da licença iLBC, assiná-lo e devolvê-la à GIPS. iLBC opera em 13.3 Kbps (30 quadros ms) e 15.2 Kbps (20 ms frames).

Para VOIP-INFO (2013), o iLBC é um codec de voz livre adequado para comunicação robusta de voz sobre IP. O codec é projetado para voz de banda limitada e resulta em uma taxa de bits de *payload* de 13,33 Kbit/s, com comprimento do quadro de codificação de 30 ms e uma taxa 15,20 kbps com um comprimento de 20 ms. O codec iLBC permite uma degradação suave da qualidade da voz no caso perda de quadros, o que ocorre em conexões onde há perdas ou atrasos de pacotes IP. Basicamente a qualidade é maior que a do codec G.729A, por ser mais robusto à perda de pacotes. O consórcio PacketACable e outros fabricantes tem adotado o iLBC como codec preferencial.

4.7 Speex

De acordo com SMITH, MEGGELEN e MADSEN (2005), Speex é um codec de taxa de bits variável (VBR - Variable BitRate), o que significa que ele é capaz de alterar dinamicamente sua taxa de bits para responder às mudanças das condições da rede. Ele é oferecido em versões de banda limitada e banda larga, dependendo da qualidade do que desejada no telefone. Speex é um codec totalmente livre, licenciado sob a variação Xiph.org da licença BSD, sendo parte do projeto GNU.

Speex é projetado para compressão de, visando diminuir a barreira de entrada para aplicações de voz, oferecendo uma alternativa gratuita aos caros codecs de voz proprietários. Além disso, Speex é bem adaptado para aplicações de Internet e oferece recursos úteis que não estão presentes na maioria dos outros codecs (VOIP-INFO, 2013).

Finalizando, Speex é baseado em CELP e é projetado para comprimir voz a taxas de bits que vão de 2-44 kbps. Algumas das características do Speex incluem (SPEEX, 2013):

- Banda Estreita (8 kHz), banda larga (16 kHz) e ultra-banda larga (32 kHz);
- Ocultação de perda de pacotes;
- Detecção de Atividade de Voz (VAD);
- Cancelador de eco acústico;
- Supressão de ruído.

5 MATERIAIS E MÉTODOS

Para a realização dos testes foi projetado um ambiente com três máquinas virtuais, sendo um servidor, uma máquina cliente e uma máquina espiã que tentava capturar a fala transmitida. Como o objetivo principal é verificar tanto uma comunicação segura como uma não segura, a combinação de um bom desempenho e uma comunicação segura pode implicar na escolha do codec. A Figura 3 apresenta o ambiente utilizado para testes.

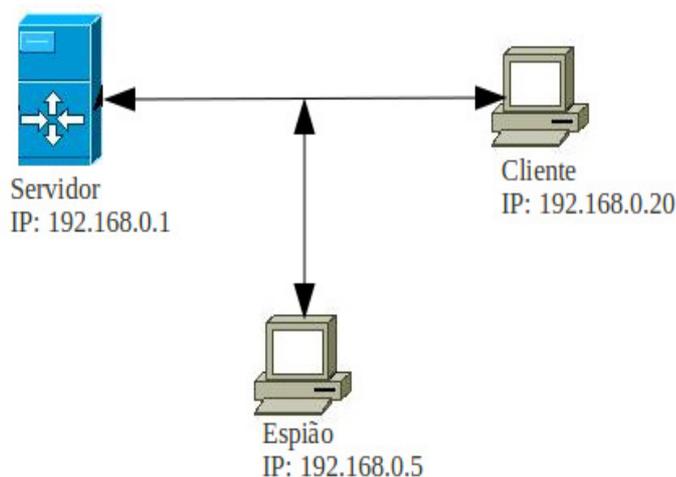


Figura 1 - Ambiente utilizado para testes.

5.1 Equipamentos

O equipamento utilizado para a criação do ambiente de testes foi um notebook da marca Itautec com a seguinte configuração:

- Sistema operacional Ubuntu Desktop 10.04;
- Kernel Linux 2.6.32-51-generic-pae;
- 4GB de memória RAM;
- Processador Pentium Dual Core T4300 2.10 Ghz.

Desta forma, foram criadas as máquinas virtuais utilizando o software de virtualização VirtualBox 3.1.6, com a seguinte configuração para cada máquina virtual:

- Servidor:
 - Sistema operacional Ubuntu Server 10.04.04 LTS;
 - 512 GB de memória RAM.
- Cliente:
 - Sistema operacional Ubuntu Desktop 11.10;
 - 512 GB de memória RAM.
- Espião:
 - Sistema operacional Ubuntu 12.04.3 LTS;
 - 512 GB de memória RAM.

Todas essas máquinas virtuais ligadas na mesma rede virtual do próprio VirtualBox.

5.2 Ferramentas

Para os testes serem realizados, foram utilizados os softwares, VirtualBox, SIPP, Wireshark e Asterisk. Assim, vamos descrever os softwares:

- VirtualBox: VirtualBox é um produto poderoso de virtualização de x86 e AMD64/Intel64 para empresas ou uso doméstico. VirtualBox não é apenas um produto extremamente rico e de alto desempenho para clientes corporativos, mas é também a única solução profissional que está disponível gratuitamente como software de código aberto sob os termos da *GNU General Public License (GPL)* versão 2. Atualmente, o VirtualBox roda em Windows, Linux, Macintosh e Solaris e suporta um grande número de sistemas operacionais convidados. VirtualBox está ativamente em desenvolvimento, com lançamentos frequentes e uma lista sempre crescente de funcionalidades. VirtualBox é um esforço da comunidade apoiada pela Oracle, garantindo que o produto sempre satisfaça os critérios de qualidade profissional (VIRTUALBOX, 2013);
- SIPP: é uma ferramenta de teste e gerador de tráfego de código aberto para o protocolo SIP. Ele inclui alguns cenários básicos e estabelece e realiza várias chamadas com os métodos de *INVITE* e *BYE*. Ele também pode ler arquivos XML com cenários personalizados descrevendo dos mais simples aos mais complexos fluxos de chamadas. Ele apresenta a visualização dinâmica de estatísticas sobre a execução dos testes (número de chamadas e o atraso de ida e volta, por exemplo). Outras características avançadas incluem suporte de IPv6, TLS, SCTP, autenticação SIP, cenários condicionais, retransmissões UDP e mais. SIPP também pode enviar tráfego de mídia RTP. A mídia pode ser de áudio ou vídeo. SIPP pode ser usado para testar vários equipamentos SIP reais, como proxies SIP, B2BUAs, servidores de mídia SIP, gateways SIP PBX e muito útil para emular milhares de agentes de usuário chamando o sistema SIP (SOURCEFORGE, 2013);
- Wireshark: é um analisador de protocolo de rede, ele permite que você veja o que está acontecendo em sua rede em um nível microscópico. É utilizado em muitas indústrias e instituições de ensino. O desenvolvimento do Wireshark prospera graças às contribuições de especialistas em rede em todo o mundo. É a continuação de um projeto que começou em 1998 (WIRESHARK, 2013).

5.3 Plano de Testes

Para realizar os testes foram utilizadas as três máquinas virtuais, sendo que a máquina cliente fosse responsável pelas chamadas com o a utilização da ferramenta SIPP, a máquina servidora pelo atendimento dessas chamadas com o Asterisk e a máquina espia capturando pacotes com o Wireshark. A máquina cliente realizou oito testes para os codecs: G.711 PCMA, G.711 PCMU, SPEEX/8, SPEEX/16, GSM, G.722 e G.726/32, quatro testes utilizando o protocolo RTP (sem criptografia) e quatro com o uso do

SRTP (com criptografia), em cada teste foram feitas 2000 chamadas para cada codec, totalizando 16000 chamadas para cada codec, 8000 com criptografia e 8000 sem criptografia, a fim de analisar o tempo de resposta dos codecs com e sem criptografia. Para isso, no arquivo sip.conf do Asterisk a opção *encryption* foi ativada para “yes” e o cenário de teste foi alterado para enviar pedidos de chamadas com o uso de SRTP, para os testes com SRTP.

6 RESULTADOS

Depois de ter realizado quatro testes com 2000 chamadas para cada codec em cada teste com transmissão de voz por RTP e mais quatro testes com 2000 chamadas para cada codec em cada teste com transmissão de voz por SRTP, dos oito testes para cada codec (16000 chamadas), quatro foram com RTP (8000 chamadas) e quatro foram com SRTP (8000 chamadas), somando 16000 chamadas para cada codec. Assim, foram obtidos alguns dados, como: pico de chamadas simultâneas, chamadas mal sucedidas e bem sucedidas para cada codec, veja os resultados:

Tabela 2 – Chamadas dos quatro testes com o protocolo RTP.

Codec	Chamadas bem sucedidas	Chamadas mal sucedidas
G.711 PCMU	7992	8
G.711 PCMA	7996	4
Speex/8	7995	5
Speex/16	7994	6
GSM	7986	14
G.722	7997	3
G.726/32	8000	0

Tabela 3 – Chamadas dos quatro testes com o protocolo SRTP.

Codec	Chamadas bem sucedidas	Chamadas mal sucedidas
G.711 PCMU	7996	4
G.711 PCMA	7996	4
Speex/8	7999	1
Speex/16	7999	1
GSM	7984	16
G.722	7995	5
G.726/32	7999	1

Desta forma, conseguimos obter dados importantes para encontrar qual codec possui o melhor tempo de resposta. Assim, foram feitas as médias do tempo de resposta para cada teste e uma média geral.

Tabela 4 – Média do tempo de resposta de cada teste e o geral com o protocolo RTP.

Codec	Média teste 1	Média teste 2	Média teste 3	Média teste 4	Média Geral
G.711 PCMU	146,000000	77,195000	145,545000	83,055000	112,948750

G.711 PCMA	135,915000	143,625000	125,605000	136,195000	135,335000
Speex/8	129,435000	128,300000	131,565000	127,595000	129,223750
Speex/16	129,845000	118,995000	116,485000	123,735000	122,265000
GSM	83,220000	123,975000	80,185000	83,970000	92,785000
G.722	143,430000	94,305000	140,340000	88,970000	116,761250
G.726/32	149,405000	100,470000	136,525000	139,705000	131,526250

Tabela 5 – Média do tempo de resposta de cada teste e o geral com o protocolo SRTP.

Codec	Média teste 1	Média teste 2	Média teste 3	Média teste 4	Média Geral
G.711 PCMU	132,250000	88,770000	78,635000	135,415000	108,770000
G.711 PCMA	130,000000	92,280000	81,005000	135,265000	109,637500
Speex/8	118,915000	116,180000	118,435000	129,430000	120,740000
Speex/16	97,140000	110,900000	114,940000	119,080000	110,515000
GSM	121,340000	80,055000	76,925000	126,975000	101,447500
G.722	143,705000	100,425000	94,620000	140,145000	119,723750
G.726/32	145,385000	98,745000	102,975000	141,150000	122,063750

Sendo assim, um gráfico com a média geral dos codecs é apresentado na Figura 3.

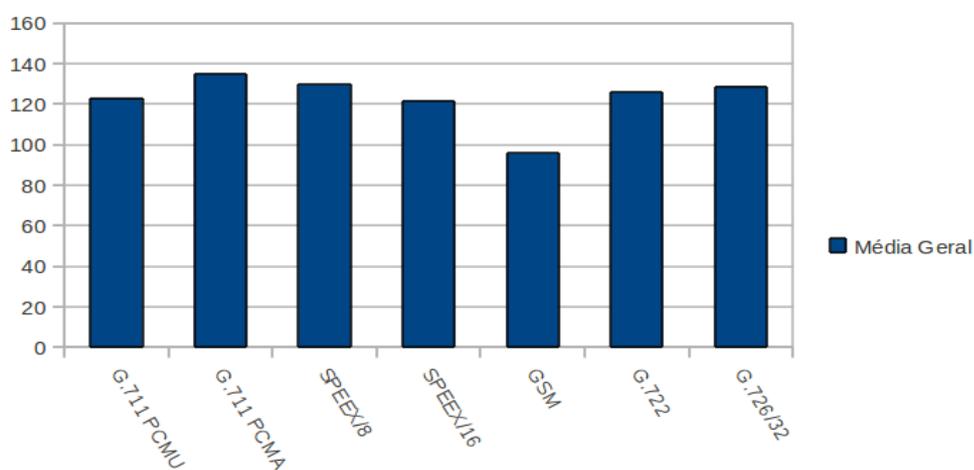


Figura 2 – Gráfico da média do tempo de resposta de cada teste e o geral com o protocolo RTP.

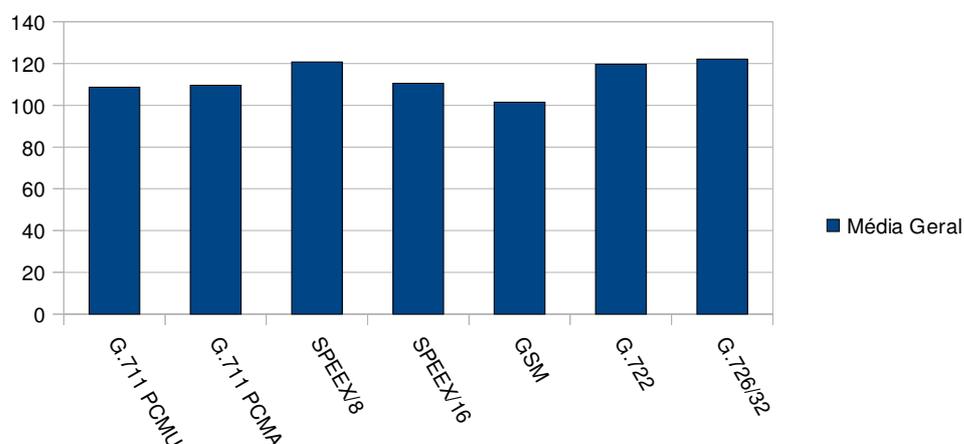


Figura 3 – Gráfico da média do tempo de resposta de cada teste e o geral com o protocolo SRTP.

Para os oito testes, foram realizadas 2000 chamadas para cada codec, ou seja, sete codecs e 14000 chamadas por teste, sendo que quatro foram utilizados RTP e quatro SRTP, com isso, temos que:

- A soma de chamadas mal sucedidas dos quatro testes com RTP foi de 14, 8, 6, 5, 4, 3 e 0, para os codecs GSM, G.711 PCMU, SPEEX/16, SPEEX/8, G.711 PCMA, G.722 e G.726/32, respectivamente, com GSM com maior número de chamadas mal sucedidas e G.726/32 com 100% de aproveitamento;
- A soma de chamadas mal sucedidas dos quatro testes com SRTP foi de 16, 5, 4, 4, 1, 1 e 1, para os codecs GSM, G.722, G.711 PCMA, G.711 PCMU, SPEEX/8, SPEEX/16 e G.726/32, respectivamente, com GSM com maior número de chamadas mal sucedidas e G.726/32 apenas 1 chamada mal sucedida;
- A média de tempo de resposta dos *invites* com RTP foram, do mais rápido para o mais lento, GSM (92.785), G.711 PCMU (112.94875), G.722 (116.76125), SPEEX/16 (122.265), SPEEX/8 (129.22375), G.726/32 (131.52625) e G.711 PCMA (135.335);
- A média de tempo de resposta dos *invites* com SRTP foram, do mais rápido para o mais lento, GSM (101,4475), G.711 PCMU (108,77), G.711 PCMA (109,6375), SPEEX/16 (110,515), G.722 (119,72375), SPEEX/8 (120,74) e G.726/32 (122,06375);
- Com o protocolo RTP, apenas os codecs G.711 PCMU e G.711 PCMA foram decodificados pelo Wireshark, permitindo que a transmissão de voz fosse ouvida pelo computador espião;
- Com o protocolo SRTP, nenhum codec foi decodificado, garantindo total segurança contra o Wireshark.

7 CONCLUSÃO

Através dos testes realizados foi possível avaliar a flexibilidade que o Asterisk possui na utilização de diferentes codecs na comunicação de voz. Desta forma, tivemos dois codecs que se destacaram nas comparações, o GSM e o G.726/32, o primeiro com menor média no tempo de resposta dos *invites* (92.785 para RTP e 101,4475 para SRTP) e o segundo com nenhuma chamada mal sucedida

para RTP e apenas uma com SRTP, não esquecendo que os dois conseguiram um mínimo de segurança quando seu pacotes foram capturados pelo Wireshark utilizando RTP.

As recomendações de atraso e perda de pacotes para uma rede com boa qualidade da chamada são:

- Atraso fim a fim deve ser menor que 150ms;
- Taxa de perda limitada a 3% (mas o recomendável é ser inferior a 0,50%).

Assim, podemos dizer que todos os codecs ficaram dentro das recomendações de [66], pois o codec G.711 PCMA foi o que teve a maior média de respostas dos *invites* nos testes com o uso do RTP (135.335 ms) e o G726/32 com o uso do SRTP (122,06375). O GSM com a maior taxa de perde de pacotes (14 para RTP e 16 para SRTP), somando os quatro testes para cada tipo de protocolo. Porém, como já dito, o GSM foi o mais rápido e mesmo que tenha sido o codec com maior taxa de perda de pacotes, 14 com RTP e 16 com SRTP em 8000 chamadas para cada protocolo, ainda mostra um ótimo desempenho, pois isso corresponde a 0,175% (RTP) e 0,2% (SRTP) de perda de pacotes, sendo que o recomendável é inferior a 0,5%.

Com isso, podemos concluir que o GSM foi o codec com maior eficiência no tempo de resposta, além de ser um dos codecs mais conhecidos em sistemas móveis. Já o G.726/32 está sendo substituído pelo codec G.729, como foi tratado nesse trabalho.

Por fim, uma preocupação comum em sistemas de comunicação é o *Mean Opinion Score* (MOS), utilizado para medir a qualidade de voz e que não foi explorado por esse trabalho, sendo um ótimo assunto de pesquisa para trabalhos futuros, podendo analisar se o codec GSM consegue um nível de satisfação aceitável pelos usuários em um ambiente específico.

REFERENCIAS BIBLIOGRÁFICAS

RUGHINIŞ, R.; ICONARU, C.; **A Practical Analysis of Asterisk SIP Server Performance**; in The 7th RoEduNet International Conference, 2008, pp. 61–64.

SOUSA, L.; A.; P.; **Avaliação de desempenho do PBX Asterisk**, Tese Mestrado, IST, 2008.

VILLACIS, D.; ACOST, F. R; LARA CUEVA, R. A. **Performance analysis of VoIP services over WiFi-based systems**, in Communications and Computing (COLCOM), 2013 IEEE Colombian Conference on 22-24 May 2013.

KELLER, A.. **Asterisk na prática**, 2ª ed., São Paulo, Novatec Editora, 2011. ISBN 978-85-7522-286-7.

SMITH, J.; MEGGELEN, J. V.; MADSEN, L.. **Asterisk: The Future of Telephony**, O'Reilly, 2005

<http://www.voip-info.org/wiki/view/Codecs>. Acesso em: 13 set. 2013.

PERETZ, A.; GUMUSOGLU, C.; **G.722 Wideband Speech Codec Implementation on Bf-533 Dsp**, Tese Mestrado, TEK/avd, 2004.

Disponível em:

<http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps8537/prod>

[white_paper0900aecd806fa57a.html](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps8537/prod/white_paper0900aecd806fa57a.html). Acesso em: 13 set. 2013.

Disponível em: http://wiki.sj.ifsc.edu.br/wiki/index.php/G.726_ou_ADPCM. Acesso em: 13 set. 2013.

Disponível em: <http://www.digium.com/en/products/software/g729-codec>. Acesso em: 13 set. 2013.

Disponível em:

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_tech_note09186a0080093f56.shtml. Acesso em: 13 set. 2013.

Disponível em: <http://www.speex.org/>. Acesso em: 13 set. 2013.

Disponível em: <https://www.virtualbox.org>. Acesso em: 20 set. 2013.

Disponível em: <http://sipp.sourceforge.net>. Acesso em: 20 set. 2013.

Disponível em: <http://www.wireshark.org/about.html>. Acesso em: 20 set. 2013.

CONFLITO DE INTERESSES

Os autores declaram não haver conflitos de interesse.

AUTOR PARA CORRESPONDÊNCIA

Ricardo Ferrari
Faculdade de Engenharia de Ilha Solteira
15385-000, Ilha Solteira (SP), Brasil
rccferrari@hotmail.com

Submetido em 15/10/2014

Aceito em 19/12/2014