Automatização de Testes SIP

David Gonçalves* , Pedro Sousa*, António Amaral† and António Costa*
*Centro Algoritmi, Universidade do Minho, pg19724@alunos.uminho.pt, {pns,costa}@di.uminho.pt
†PT Inovação, antonio-mn-amaral@ptinovacao.pt

***Abstract*—As redes IP são actualmente as principais infra-estruturas de comunicação utilizadas por um conjunto crescente de aplicações e serviços heterogéneos, nos quais se incluem os serviços de voz. Neste sentido, as funções de transmissão e gestão de sessões são muitas vezes asseguradas por protocolos dedicados, como seja o exemplo do *Real-Time Transport Protocol* (RTP) e o *Session Initiation Protocol* (SIP).**

O protocolo SIP apresenta um papel preponderante na gestão de sessões, desempenhando funções vitais num conjunto extenso de soluções. Contudo, a disseminação do protocolo acarreta alguns desafios, tais como a validação e teste de soluções SIP. Estes processos de validação necessitam de considerar diversos fatores, como seja o caso da análise de cabeçalhos, validação de valores dinâmicos, verificação de fluxos de mensagens, entre outros. Nesta perspetiva, a validação manual de soluções SIP apresenta-se como um processo moroso e dispendioso, sendo crucial o desenvolvimento de processos automatizados nesta área.

Neste contexto, este resumo alargado aborda e analisa de forma integrada a temática geral da validação de soluções SIP, apresentando também ferramentas e aplicações capazes de auxiliarem os processos de automatização de testes de soluções SIP.

I. Introdução

A proliferação das redes IP veio mudar o modo como as pessoas interagem e comunicam. O impacto desta tecnologia faz-se sentir tanto nos utilizadores como nos fornecedores de serviço, tendo pois consequências no que respeita às receitas obtidas pelas redes de telecomunicações [1].

As soluções de comunicação por voz em redes IP denominam-se usualmente por soluções Voice over IP (VoIP), caracterizando-se como soluções capazes de converter sinais analógicos de voz em sinais digitais passíveis de serem transmitidos sobre uma rede comutada de pacotes. No que diz respeito às vantagens do VoIP, estas apresentam-se distintas para utilizadores finais, empresas e operadores tendo contudo, um principio base comum, diminuição de custos comparativamente com serviços das redes telefónicas.

Em termos protocolares, as soluções VoIP necessitam de possuir por base mecanismos de sinalização e transmissão dos *media*, capazes de permitir o estabelecimento de uma sessão e a correspondente troca de dados sobre a mesma. Em relação aos protocolos usados para a transmissão de dados, destaca-se o protocolo Real-Time Transport Protocol (RTP) [2], caracterizado como um protocolo de transporte de dados independente das camadas inferiores.

Este trabalho é financiado por Fundos FEDER através do Programa Operacional Fatores de Competitividade – COMPETE e por Fundos Nacionais através da FCT – Fundação para a Ciência e Tecnologia no âmbito do Projeto: FCOMP-01-0124-FEDER-022674. Agradeço à PT Inovação, a possibilidade para a realização do trabalho descrito neste artigo.

No que respeita à sinalização, o protocolo Session Initiation Protocol (SIP) [3] apresenta-se como um protocolo preponderante no estabelecimento de sessões, sendo o mesmo definido na RFC 3261 [3]. Em termos funcionais, o protocolo SIP opera a nível aplicacional seguindo o modelo cliente-servidor para a troca de mensagens entre os participantes da sessão.

No que respeita às mensagens trocadas, o SIP apresenta as mensagens em formato texto, sendo de simples interpretação para o utilizador, mas de difícil interpretação integral para os sistemas computacionais.

Embora o formato das mensagens SIP favoreça a validação manual, a diversidade destas torna o processo de validação manual moroso e propenso a erros, verificando-se a necessidade de automatizar o processo de validação. Contudo, a implementação e validação de soluções com elevada diversidade, tal como acontece com o protocolo SIP, torna a tarefa de automatização árdua e de difícil implementação.

Ao longo do resumo são discutidas as dificuldades associadas aos processos de validação de soluções SIP bem como estratégias gerais de um possível processo de automatização.

II. Motivação

Em termos gerais, a qualidade de um projeto encontra-se diretamente relacionada com a capacidade dos testes validarem todos os requisitos considerados. Contudo, o mapeamento de requisitos em testes e a execução destes na sua totalidade apresenta-se como uma tarefa morosa e de difícil alcance.

No que respeita à realização de validações de soluções SIP, estas necessitam de ser validadas sobre o conjunto de equipamentos que possuem intervenção no fluxo de mensagens, tendo pois cada equipamento de ser validado de forma singular.

Em termos de condicionantes, para além do elevado número de validações a realizar sobre diferentes equipamentos, verificam-se obstáculos associados com as próprias características das mensagens, quer seja devido à multiplicidade de informação presente, ao dinamismo de certos valores ou relacionadas com o tipo de mensagem e a sua integração no fluxo geral de mensagens.

A nível estrutural as mensagens SIP seguem o modelo definido na RFC 2822 [4], sendo constituídas por uma *start-line*, um conjunto de cabeçalhos e o corpo das mensagens. Aquando da validação de soluções SIP, o foco principal centra-se na validação dos valores associados com os cabeçalhos presentes nas mensagens. Sendo estes em grande número, encontrando-se definidos só na RFC base mais de 40 cabeçalhos distintos [3].

Juntamente com o elevado número de cabeçalhos verificam-se dificuldade na validação dos mesmos pelo dinamismo

que estes apresentam. Os valores dos cabeçalhos SIP são definidos por uma gramática Augmented Backus–Naur Form (ABNF) [5] apresentando-se restritos, mas com um grau de dinamismo elevado comparativamente com os cabeçalhos da maioria dos protocolos.

Este conjunto extenso de problemáticas tem relevância tanto ao nível académico como empresarial apresentando-se util para equipas multidisciplinar que operem directa ou indirectamente com o protocolo SIP. Verificando-se assim a necessidade de desenvolver métodos capazes de analisarem soluções SIP de forma rápida e eficaz, permitindo a realização cómoda de validações e teste de soluções SIP.

III. Metodologia de teste e validação de cenários SIP

Tendo como ponto de partida as dificuldades de validação de soluções SIP anteriormente identificadas, começou-se a desenvolver trabalho tendo como propósito final a criação de uma solução/metodologia capaz de validar soluções SIP de forma rápida e simples. Neste processo terão que ser consideradas as questões centrais do controlo dos *inputs* e *outputs* dos equipamentos, e a execução dos testes em condições em tudo semelhantes às condições que a solução terá no ambiente final.

O controlo dos *inputs*, *outputs* é fundamental. A solução a validar sobre o ponto de vista do equipamento possui mecanismos de tratamento das mensagens SIP consoante a informação que chega ao equipamento na mensagem, sendo crucial conhecer e controlar bem a informação que é enviada para e do equipamento para se conseguir testar diferentes cenários com a precisão necessária.

A solução proposta para esta temática identifica a necessidade de ostracizar o elemento a validar para um ambiente controlado onde os *inputs* e *outputs* encontram-se ao encargo da equipa de validações.

Neste tipo de cenários é configurado o equipamento para operar com dois terminais a executar *software* de emulação SIP. A escolha de ferramentas de emulação em detrimento de terminais físico justifica-se pela capacidade que estas ferramentas possuem de manipular diretamente as mensagens do fluxo, permitindo criar cenários idênticos aos presentes na rede onde o equipamento a validar se encontrara implementado.

Relativamente à criação das mensagens, como indicado anteriormente, as mensagens SIP possuem um tamanho avultado sendo assumido por alguns autores o valor médio de 731 bytes por mensagem [6]. Estes valores põem em causa a criação manual das mensagens no *script* a emular, sendo necessário desenvolver mecanismos automáticos de geração de *scripts*. Para endereçar esta questão, optou-se pelo uso de aplicações capazes de através de capturas de rede gerar *scripts* de emulação de tráfego. Desta forma consegue-se garantir a exatidão dos comportamentos, avaliando se os mesmos estão alinhados com a realidade.

IV. Ferramentas *Open Source*

Ao nível de ferramentas de emulação de tráfego SIP, existe um conjunto extenso de possibilidades, tais como Seagull [7], SIP Tester [8], SIPp [9], entre outros. Das ferramentas analisadas a que se revelou mais adequada foi o SIPp, devido aos mecanismos que possui de validação de mensagens, à aceitação que a ferramenta tem por parte de entidades relevantes na área do SIP como a Fraunhofer [10] e pelo conjunto de aplicações de tratamento de tráfego que dispõe.

No que respeita a geração de cenário, são analisadas duas aplicações que através de capturas de rede (ficheiros PCAP) redigem cenários SIPp.

A. *SIPp*

O SIPp é um projeto *open source* desenvolvido tendo como propósito a geração de tráfego SIP e a validação do mesmo [9]. Em termos de modelo funcional, o SIPp opera sobre ficheiros XML onde são descritos os cenários a executar de forma simples e concisa, sendo fácil o processo de adaptação dos mesmos.

Ao nível protocolar, a ferramenta encontra-se equipada com suporte para protocolos diversos como o IPv4, IPv6, UDP, SCTP entre outros, permitindo o desenvolvimento de cenários próximos da realidade, conjugando *scripts* de emulação com equipamentos físicos. Relativamente a cenários de testes, um caso prático de integração da ferramenta de emulação com equipamentos, apresentar-se-ia semelhante a Figura 1.

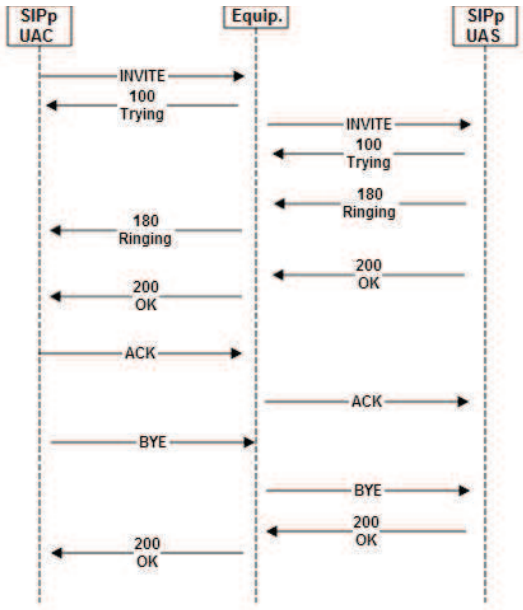

Fig. 1: Fluxo de estabelecimento de sessão entre UAC e UAS

Os ficheiros SIPp representados como UAC (cliente) e UAS (servidor) apresentam o mesmo fluxo, mas com comportamento complementar um do outro. Como indicado anteriormente o SIP segue um modelo cliente-servidor onde para um dado *request* (ex. INVITE), é enviada uma *response* (ex. 200 OK).

Quando o SIPp UAC faz o envio de um *request* o UAS tem no seu fluxo a indicação do *request* enviado pelo UAC e vice-versa mantendo desta forma o fluxo das mensagens (excerto I de cenário entre o UAC e o UAS).

Aquando do término da criação dos cenários SIPp, existe a necessidade de aplicar expressões regulares ao mesmo de

Exc. I: Interligação entre o INVITE do UAC e UAS

<send>	*<recv request="INVITE" >*
INVITE ...	
</send>	*</recv>*

forma a validar valores específicos da mensagem. Em termos funcionais, na mensagem que se quer validar indica-se o valor expectável para o cabeçalho a validar, estando este mapeado numa expressão regular. Aquando da execução, o próprio SIPp encarrega-se de analisar a mensagem recebida e verificar se a mesma apresenta o valor esperado.

O conteúdo da expressão é validado dentro de uma *tag* *<ereg>* indicando que componente da mensagem se pretende validar, que tipo de validação e qual a expressão regular com que se pretenda que exista *match*. Em termos estruturais apresenta-se semelhante ao evidenciado no excerto de código IV.

B. Preparação de testes a partir de cenários reais

Como referido anteriormente de forma a tornar o processo de geração de *scripts* uma tarefa menos penosa recorre-se ao uso de aplicações capazes de, forma automática, gerar os cenários pretendidos. De entre as aplicações destacam-se o *pcap2sipp* [11], *sniff2sipp* [12].

Das aplicações de estudadas o *sniff2sipp* apresentou-se como a aplicação mais adequada para a geração de *scripts*, apresentando-se como uma aplicação mais madura, operando com um conjunto de protocolos superior e capaz de realizar *scripts* através de capturas ou de *traces* diretos na rede.

V. Exemplo de Utilização

O conjunto das ferramentas apresentadas possibilita a validação de soluções SIP sobre diferentes cenários. A título de exemplo demonstra-se de seguida os diferentes passos a seguir para a validação de um equipamento SIP com funções de encaminhamento e manipulação de cabeçalhos.

A validação dos testes inicia-se com o processo de criação dos *scripts* SIPp, sendo esta tarefa levada a cabo pelo *sniff2sipp*. Tendo a captura com o comportamento a validar, basta executar a aplicação indicando o nome da captura a gama de portos usada pelo SIP como verificado na excerto II.

Exc. II: Comando de arranque da aplicação sniff2sipp

```
./sniff2sipp -f call.cap -p 5060-5062
```

Após a execução do comando são gerados os ficheiros do cliente e do servidor. No ficheiro do cliente é apresentado o INVITE a ser enviado para o equipamento a validar (excerto III), enquanto que do lado do servidor é indicada a mensagem que se espera receber.

Com o envio e a espera de receção da mensagem já se valida a solução ao nível do fluxo. Contudo, o equipamento a validar substitui o *user-part* do cabeçalho *To* pelo valor *"siphomenetwork"*, sendo necessário aplicar uma expressão regular ao INVITE a receber no servidor (excerto IV)

Estando os cenários SIPp preparados e com as expressões regulares embebidas, basta executar os mesmos.

Exc. III: Mensagem INVITE em cenário SIPp UAC

```
INVITE sip:[service]@[remote_ip] [remote_port] SIP/2.0
Via: SIP/2.0/UDP [local_ip]:[local_port];branch=[branch];rport
Max-Forwards: 70
Contact: <sip:test1@[local_ip]:[local_port]>
To: <sip:[service]@[remote_ip]:[remote_port]>
From: <sip:test1@[local_ip]:[local_port]>;tag=[pid]
Call-ID: [call_id]
CSeq: 1 INVITE
```

Exc. IV: Mensagem INVITE em cenário SIPp UAS

```
<recv request="INVITE" crlf="true">
<action >
<ereg regexp="<sip:siphomenetwork@*" search in="hdr" header="To"/>
</action>
</recv>
```

Através da plataforma, consegue-se realizar validações em ambiente emulado como se de tráfego real se tratasse permitindo assim executar e validar os diferentes cenários de forma mais autónoma e controlando o cenário de testes na sua totalidade.

VI. Conclusões

As soluções tecnológicas envolvendo o protocolo SIP encontram-se cada vez mais presentes no dia-a-dia das pessoas, verificando-se a necessidade de desenvolver estratégias auxiliares na resolução de tarefas morosas e dispendiosas, como é o caso dos processos de validação e testes de infra-estruturas VoIP. Desta forma, a definição de estratégias eficazes, recorrendo à utilização de ferramentas de automatização, torna-se uma mais-valia indispensável nesta área. A utilização destes mecanismos é útil, tanto no processo de validação de soluções, como no auxílio ao estudo de anomalias, permitindo pois um mais rápido desenvolvimento e implementação de soluções nos clientes finais.

Através da solução delineada, que tem por base ferramentas *open source*, é pois possível acelerar todo o processo de desenvolvimento de soluções SIP, possibilitando às equipas de desenvolvimento a definição de um framework simples mas eficaz para o teste e deteção de anomalias nestes ambientes.

References

[1] Antonio Cuevas, J.I. Moreno, P. Vidales, and H. Einsiedler. The ims service platform: a solution for next-generation network operators to be more than bit pipes. *Communications Magazine, IEEE*, 44(8):75–81, 2006.

[2] H. Schulzrinne S. Casner R. Frederick V. Jacobson. Rtp: A transport protocol for real-time applications, 7 2003. RFC 3550.

[3] J. Rosenberg H. Schulzrinne G. Camarillo A. Johnston J. Peterson R. Sparks M. Handley E. Schooler. Sip: Session initiation protocol, 6 2002. RFC 3261.

[4] P. Resnick. Internet message format, 4 2001. RFC 2822.

[5] D. Crocker P. Overell. Augmented bnf for syntax specifications: Abnf, 1 2008. RFC 5234.

[6] Masataka Ohta. Overload control in a sip signaling network. *International Journal of Electrical and Electronics Engineering*, 2009.

[7] HP OpenCall Software. Seagull: an open source multi-protocol traffic generator @ONLINE, 2 2009.

[8] StarTrinity.com. Freeware sip tester (call generator, sip/rtp stressing tool, dos simulator) @ONLINE, 2013.

[9] R. Day. Welcome to sipp @ONLINE, 4 2013.

[10] Fraunhofer FOKUS. Links for ims developers @ONLINE, 2008.

[11] C. Oancea. pcap2sipp @ONLINE, 4 2013.

[12] Digium. digium: The asterik company @ONLINE, 2013.