Skype 发送模型及其应用*

周井泉,姬德浪
(南京邮电大学 电子科学与工程学院,江苏 南京 213000)

摘 要:为了提高 Skype 语音流的检测效率,在分析 Skype 流量特征和负载特征的基础上,提出了 Skype 语音源的发送模型。该模型体现了 Skype 发送端帧结构的特征,大大简化了接收端识别的过程。

关键词:语音源模型;业务识别;流;Skype

中图分类号:TP393.02 **文献标识码**:A

Source model of Skype and its application in the traffic identification

ZHOU Jing Quan, JI De Lang
(College of Electronic Science & Engineering, Nanjing University of Posts and Telecommunications, Nanjing 213000, China)

Abstract: To improve the efficiency of Skype voice flow identification, the characteristics of flow Skype and load were analyzed thoroughly and the source model of Skype is proposed, which will simplify the process of the traffic identification.

Key words: source model; traffic identification; flow; Skype

Skype 是世界一流的 P2P(对等方到对等方)网络语音沟通工具,以无缝穿透网络地址转换器(NAT)和防火墙的工作能力、良好的通话质量,成为发展最快的基于 IP 语音(VoIP)系统。Skype 使用了专用的通信协议,并用高强度密码加密负载,但至今为止没有公布过任何有关协议或其他技术专题的文档。对于使用了高强度的加密算法和专用通信协议的 Skype 系统,目前检测其流量的效果并不理想。

面对这种现状,许多学者希望建立一种常规模型。一方面可以加深对 Skype 系统的了解;另一方面简化 Skype 业务设别的过程。

自 Skype 得到广泛应用以来,很多研究人员对其进行了分析研究。参考文献[1]分析了 Skype 报文在应用层的协议特征字和端口的某些规律,揭示了 Skype 不仅可以通过 UDP 和 TCP 进行通信,而且通信端口不固定。指出其登录过程可以分为 UDP 探测、TCP 握手和 TCP 认证 3 个部分,分析了各个过程中存在的应用层特征字。提出了一种根据 Skype 用户和超级节点连接的特征字和报文长度、顺序来识别 Skype 的方法。参考文献[2]使用了报告 UDP 的 Skype 报文结构,发现了部分未加密的功能字段的特征,为准确识别基于 UDP 的 Skype 流量提供了一种可能。通过实际收集并分析 Skype 语音通信的流量,参考文献[3]提出了一种独特的模型来量化 VoIP 用户满意度,其中使用了两阶段过滤方法来识别 Skype VoIP 会话,即先用一种启发式算法过滤出可能的 Skype 流量存储在磁盘中,采用离线识别算法提取 Skype 通信流量,该离线方法计算复杂度较高。参考文献[4]讨论了识别超级节点的两阶段方法,即先采用参考文献[5]给出的过滤器方法识别 P2P 流量,再用超级节点过滤器区分超级节点和普通节点。

综上分析,以前的理论研究缺少完善的 Skype 语音源模型,造成业务识别过程复杂。本文建立了一种通用 Skype 语音源模型,简化了 Skype 业务识别的整个过程。

1 插件模型

Skype 业务包括语音业务、数据业务等,因其之间有相关性,所以本文只对 Skype 的语音业务进行建模。按其通信的终端不同,可以分成以下两类:

(1)通信双方是安装 Skype 客户端的 PC,称为 E2E。

(2)一端安装 Skype 客户端的 PC;另一端是传统的电话机,称为 E2O。

1.1 KM 模型

插件模型简称为 KM 模型。图 1 所示为 Skype 语音

*基金项目:国家 863 计划资助项目(2009AA01Z202);江苏省科技支撑项目(BE2008134)

信号建立的模型，首先语音源通过语音编码器将语音的脉冲编码调制(PCM)样值编码成少量的比特(帧)。在帧被创建好之前加入一些头部，如图中的H_1、H_2等。图中的存档器和加密功能是通过一些算法对数据流进行压缩和加密。最后，帧在被发送出去之前在其头部会加上未加密的开始信息特殊字段，这对于流量的识别非常重要。这时不论帧被封装在TCP还是UDP中，发送出去的就是Skype信息。

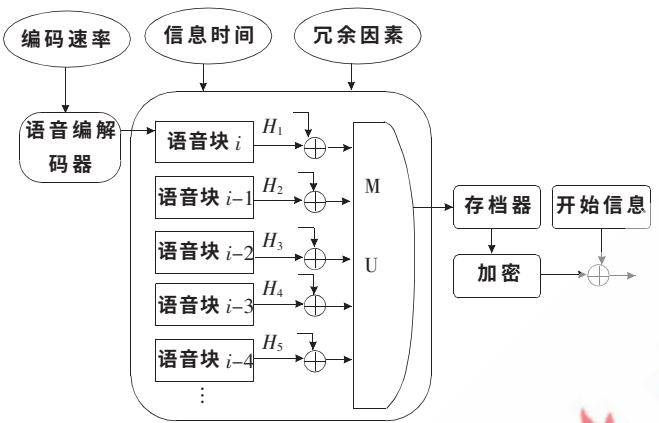

图1 Skype语音信号模型

在KM模型中，3个参数决定了业务的特征：(1)速率V_i，表征语音的编码速率；(2)信息时间T，表征1个帧的长度；(3)冗余因数RF，表征相对于当前的帧，重传帧的数量(与编码方式无关)。

1.2 开始信息

根据参考文献[6]，Skype用AES和RSA算法加密信息，对传输层协议的选择有着重要的意义。TCP执行定向可靠传输的连接，能够保证按照正确顺序接收数据。因此，利用TCP协议可以加密整个信息。但UDP协议提供的连接服务并不可靠，不能保证数据是有序的全部得到传输。当利用UDP协议时，接收端需要从应用层中提取出一些头部探测和处理不正确的数据流，不能通过加密来传输，只能通过单一数据包的有效载荷功能进行伪装，因此利用UDP协议时不能加密整个信息。此外，Skype利用固定端口发送和接收UDP部分。

基于上面的分析，发现当Skype信息被封装在UDP协议的数据流中，通过检测UDP静态负荷部分设别出一部分Skype信息。这个静态信息为开始信息。

(1)E2E信息

在2个Skype客户端之间寻找封装在UDP中的信息时，可以识别出ID号、干扰信号和结构标志。ID号是16比特长的识别标志符，在发送端被随意选取，在接受端被拷贝。干扰信号是5比特长的识别标志符，伪装在呈现有效载荷类型的1个字节中。其3个随机比特可以通过0X8f位掩码去除。结构标志包含编码序列和语音块的复序列。ID号和干扰信号是开始信息字段的一部分。

(2)E2O信息

E2O呼叫时，在客户端和超级节点之间有初始的信令连接。观察封装在UDP协议中的有效载荷，在一系列初始信息中，前4个字节总是相同的，与E2E相比，E2O有着不同的开始信息的格式。可以把这4个字节作为唯一的识别标志符，从第5字节以后就没有实质性的意义。

2 KM模型在语音设别中的应用

KM模型可以用χ^2分布来判断被分析的信号是否满足Skype信息的格式。χ^2分布能够判断信息的加密部分。在识别的过程中主要分为3类：

(1)应用UDP协议传输的E2E，干扰信号是透明的，其他信号被加密。假定编码器处于最佳编码状态，被编码的信息可出现完全随机(例如均匀分布)。

(2)应用UDP协议传输的E2O，其前4个字节是透明的，即识别标志符。其余字节全是加密的，相应的比特出现是随机的。

(3)应用TCP传输的Skype流，整个信息都被加密，和前面2种情况不同的是整个信息出现全是随机的。

在实验中对于每个属于Skype流的信息，考虑前G个组，每个组有b比特，即首先考虑Gb比特的数据流。对于每个数据块$g=1,\cdots G$，变量O_i^g表征第g数据块中值i出现的次数。在流的末端，评估每个组的χ^2的值。如表1所示。

表1 Skype KM模型的信息结构特征

Skype模式	开始信息			有效载荷
字节位置	1~2	3	4	5~…
E2E/UDP	随机	混合	随机	随机
E2O/UDP	透明	透明	透明	随机
E2E-E2O/TCP	随机	随机	随机	随机

$$\chi_g^2=\sum_{i=0}^{2^b-1}\frac{(O_i^g-E_i)^2}{E_i}\quad g=1,\cdots G \tag{1}$$

必须将试验得出的χ^2的值和预计的值进行比较。期望依靠流的的类型特征和传输层的协议(表1)识别出Skype业务信息。

为了检测g组是随机、混合还是透明的，χ^2分布可从平均分布中获得。在这种情况下，对于所有可能的值i，$E_i=n/2^b$，其中n为流中所有值的数量，利用一些门限值和得出的值比较。门限值为χ_1^2、χ_2^2、χ_3^2，分别代表随机、混合和透明。为了实验的简单性，选择$b=4$，$G=16$，根据以下标准来区分业务：

(1)E2E/UDP

$$\max_{g\in\varphi}(\chi_g^2)>\chi_1^2 \text{且} \min_{g\in\{5,6\}}(\chi_g^2)>\chi_2^2\quad \varphi=\{g|1\leqslant g\leqslant G,g\neq 5,6\} \tag{2}$$

$\varphi=\{g|1\leqslant g\leqslant G,g\neq 5,6\}$是E2E随机部分，这个标准

的依据是随机部分与均匀分布类似，导致 χ^2 分布的值较小。同时，混合情形包括一些透明部分，得出的值较大，因为在一定意义上，典型的随机信号偏离较大。

(2)E2O/UDP

$$\min_{g=1,\cdots,8}(\chi_g^2)>\chi_3^2 \text{ 且 } \max_{g=9,\cdots,16}(\chi_g^2)>\chi_1^2 \quad (3)$$

在此业务中，KM 模型开始信息是透明的，其他的是随机的。

(3)E2E/TCP E2O/TCP

$$\max_{g=1,\cdots,16}(\chi_g^2)<\chi_1^2 \quad (4)$$

其所有数据流全是随机的。

3 实验

为了验证本文提出的模型，通过实验环境，利用 RAW SOCKET 获取流过本机的所有数据包，并将其所有信息导入 1 个数据库中，实现 Skype 业务基于 TCP、UDP 传输协议的识别。

本地测试环境为 WindowsXP 系统，实验室局域网环境。由于检测速度的原因，采用非实时检测。先把数据放到数据库中，再对数据库中的数据进行检测和分析。

表 2 实验数据

项目	获取数据	确认数据	FP
E2E	1 654	1 468	186
E2O	207	202	5

测试结果分析：FP 为误判数，即非 Skype 通信数据被当作 Skype 测试数据，测试结果如表 2 所示。

根据实验结果得出基于 KM 模型，χ^2 分布可以有效地识别出 Skype 的语音业务。

本文根据对 Skype 流量特征的分析，提出一种基于流外部特征的模型来识别 Skype，并且对 KM 模型进行实验验证。此实验模型不但可以有效地识别 P2P 应用，而且可以对 Skype 的通话类型进行区分，以便对 E2O 的电话进行计费。另外本文提出的 Skype 模型具有很好的扩展性。可以对 Skype 的数据业务、实时业务统一到 KM 模型中，实现更加通用的 Skype 发送端模型。虽然 KM 模型通用可行，但是识别率还达不到网络所规定的要求，这需要在模型和算法中进一步地改进。

参考文献

[1] EHLERT S, PETGANG S. Analysis and signature of Skype VoIP session traffic [C]. Berlin: Fraunhofer FOKUS, Technical Report: NGNI2SKYPE206b, 2006.

[2] BIONDIP, DESCLAUXF. Silver needle in the Skype [C]. Amsterdam: Black Hat Europe'06, 2006.

[3] CHEN Kuan2ta, HUANG Chun2ying, POLLY H, et al. Quantifying Skype user satisfaction[C]. Pisa: Proceedings of ACM Sigcomm'06, 2006.

[4] ONEILL D, KANGH, KIM J,et al. Transport layer identification of P2Psupernodes [C]. Taormina: Proceeding of Internet Measurement Conference, 2004.

[5] KARAGIANNIST, BROIDOA, FALOUTSOSM, et al. Transport layer identification of P2P traffic [C]. Taormina: Proceeding of Internet Measurement Conference, 2004.

[6] BERSON T. Skype security evaluation. [DB/OL].http://www.skype.com/security/files/2005-031securityevaluation.pdf, 2005.

(收稿日期：2009-09-14)

作者简介：

周井泉，男，1963 年生，博士，教授，主要研究方向：研究现代通信系统通信网络(包括有线网络和无线网络)系统。

姬德浪，男，1984 年生，硕士，主要研究方向：通信网的可靠性。