使用时间相关功能表征加密和 VPN 流量

会议论文·2016 年 2 月

DOI: 10.5220 / 0005740704070414

4 位作者：

阿拉什·哈比比（Arash Habibi Lashkari）

97 出版物 **1,681 个**引用

查看个人资料

杰拉德·德雷珀·吉尔

欧盟委员会

18 出版物 **267** 引文

查看个人资料

穆罕默德·马蒙（Mohammad Mamun）

加拿大国家研究委员会

28 出版物 **396 个**引文

阿里·戈尔巴尼（Ali A.Ghorbani）

新不伦瑞克大学

271 出版物 **7,605 个**引用

查看个人资料

使用与时间相关的 功能表征加密和 VPN 流量

杰拉德 德雷珀 吉尔，阿拉什 哈比比 拉什卡里，穆罕默德 赛义夫 伊斯兰 马蒙和阿里 戈尔巴尼
新不伦瑞克大学，弗雷德里克顿 NB E3B 5A3，新不伦瑞克，加拿大
{ gerard.draper，msi.mamun，a.habibi.l，ghorbani } @ unb.ca

关键字： 流量分类，加密流量特征，基于流时间的功能，VPN 流量特征，流超时值。

抽象的：

流量表征是当今安全行业的主要挑战之一。新应用程序和服务的不断发展和生成以及加密通信的扩展使其成为一项艰巨的任务。虚拟专用网（VPN）是加密通信服务的一个示例，它已成为一种流行的加密通信服务，它可以绕过审查并访问在地理位置上锁定的服务。在本文中，我们研究了基于时间的，与时间相关的功能在检测 VPN 流量以及将加密流量表征为不同类别（根据浏览，流等）的有效性方面的有效性。我们使用两种不同的知名方法机器学习技术（C4.5 和 KNN）来测试我们功能的准确性。

1 引言

在过去的十年中，由于实施了网络服务质量（QoS），安全性，计费，设计和工程设计机制，流量分类技术受到了越来越多的关注。网络行业以及研究界已经为这些技术的研究做出了很多努力，并提出了几种分类技术（Callado 等，2009）。但是，Internet 和移动技术的不断扩展正在创造一个动态的环境，每天都有新的应用程序和服务出现，而现有的应用程序和服务也在不断发展。此外，加密在当今的 Internet 中正变得越来越普遍，成为安全通信的基础。这种不断的创造，进化，

流量分类可以基于其最终目的进行分类：将流量与加密（例如，加密的流量），协议封装（例如，通过 VPN 或 HTTPS 隧道传输）相关联；根据特定的应用程序（例如 Skype）或根据应用程序类型（例如流媒体，聊天），也称为流量表征。某些应用程序（例如 Skype，Facebook）支持多种服务，例如聊天，语音通话，文件传输等。这些应用程序需要同时识别应用程序本身和与之关联的特定任务。文献中很少有交通分类技术能够解决这一挑战性趋势（Wang 等，2014；Rao 等，2011；Coull 和 Dyer，2014）。

在 90 年代初期，最初的流量分类技术将传输层端口与特定的应用程序相关联，这是一种简单而又快速的技术。但是，它的低准确性和不可靠性使得深度数据包检测（DPI）方法得以发展。DPI 方法分析数据包，并根据一些存储的签名或模式对它们进行分类。但是，需要进行有效负载检查的 DPI 技术的计算效率不高，尤其是在高带宽网络上。此外，它们经常被无法进行有效负载分析的封装，加密或混淆流量所规避。

选择有效和可靠的功能进行流量分析仍然是一个严峻的挑战。一般来说，网络流量的分类主要分为两类：基于流的分类，使用诸如每秒流字节数，每个流的持续时间等属性；基于分组的分类，使用诸如大小，分组间持续时间等属性。第一个（或 n）个数据包，等等。

在本文中，我们专注于分析常规加密流量和通过虚拟专用网络（VPN）隧道传输的加密流量。特征

G.Draper-Gil，A.Lashkari，M.Mamun 和 A.Ghorbani
使用与时间相关的功能表征加密和 VPN 流量。
在第二届信息系统安全与隐私国际会议（ICISSP2016）的会议记录中，第 407-414 页
国际标准书号（ISBN）： 978-989-758-167-0

VPN流量的分配是一项有挑战性的任务，有待解决。VPN隧道用于维护通过数据包级加密在物理网络连接上共享的数据的私密性，因此很难识别通过这些 VPN 服务运行的应用程序。

我们在本文中的**贡献**是双重的。首先，我们提出一种基于流的分类方法，以仅使用与时间相关的特征来表征加密和 VPN 流量。此外，我们通过将特征集减少到可以以低计算复杂度提取的特征集来减少计算开销（Kim 等，2008； Li 等，2009）。其次，我们生成并发布带有加密流量的广泛标记的数据集，其中包含 14 种不同的标签（常规加密流量为 7 个，VPN 流量为 7 个）。我们仅选择与时间相关的功能以加快效率并确保独立于加密的流量分类器。

本文的其余部分安排如下：第 2 节概述了加密的流量分类。在第 3 节中，我们描述数据集。第 4 节介绍了对捕获的数据集执行的实验，而第 5 节介绍并讨论了获得的结果。最后，第 6 节介绍了结论和未来的工作。

2 相关工作

Paxson 等人于 90 年代初开始研究基于数据包大小和流的流量分类。在（Paxson，1994；Paxson 和 Floyd，1995）中，一些统计特征（如数据包长度，到达间隔时间和流持续时间）被认为适合跟踪协议。后来的 Belzarena 等。（Gomez Sena and Belzarena，2009）和 Li 等人。（Li 等人，2009 年）使用流的前几个数据包中的统计信息来提高效率。此外，为了加快在大规模，高速网络中的分类效率，Nucci 等人*（2003 年）提出了一种新的方法。*（Yeganeh et al。，2012）和 Pescap et *al*。（Aceto 等人，2010）提出了一种基于签名的流量识别方案。尽管他们减少了对流进行分类的时间，但他们未能检测到未知或手动创建的签名。

流量表征技术在当前文献中并未得到广泛解决。而且，它们大多数都集中在特定的应用程序类型或设备上。Wang 等。（Wang et al。，2014）提出了一个表征 P2P 流量的模型。他们从多个流中提取特征，然后将流聚合到群集中，提取 P2P 应用程序行为。Coull 等人（Coull 和 Dyer，2014 年）提出了一项有关 iMessage 协议以识别设备类型的研究。在（Rao et al。，2011），Rao et *al*。为两个最受欢迎的视频流服务 Netflix 和 YouTube 提出网络特征模型。在（Mauro and Longo，2015）中，Mauro 和 Longo 提出了一种检测加密的 WebRTC 流量的方法。Mamun 等。（Mohammad SI Mamun and Ghorbani，2015）提出了一种通过测量数据包有效载荷的熵来识别加密流量的方法雪利酒等。（Sherry et al。，2015）提出了一种 DPI 系统，该系统可以检查加密的有效负载而无需将其解密，从而保持通信的私密性，但它只能处理 HTTPS 流量。

在文献中已经提出了许多基于流的机器学习分类方法（Bernaille 和 Teixeira，2007； Moore 和 Zuev，2005）和基于包的特征（Iliofotou 等，2007； Karagiannis 等，2005）。准确识别流量。但是，主要用于出于隐私原因隐藏用户身份的封装协议（例如，使用代理服务器或 VPN 隧道）的流量分类具有挑战性，因此在文献中并未得到广泛研究。然而，最近，Heywood 等。（Aghaei-Foroushani 和 Zincir-Heywood，2015 年）提出了一种数据驱动的分类器，以使用流量信息识别来自代理服务器后面的客户端的流量。

据我们所知，我们是第一个提出广义上表征 VPN 流量的方法的方法，可识别 7 种不同的流量类别。

3 DATASET GENERATION

为了创建一个有代表性的数据集，我们捕获了实验室成员产生的实际流量。我们为用户 Alice 和 Bob 创建了帐户，以便使用 Skype，Facebook 等服务。在表 1 中，我们提供了数据集中包含的各种流量和应用程序的完整列表。对于每种流量类型（VoIP，P2P 等），我们捕获了一个常规会话和一个基于 VPN 的会话，因此，我们共有 14 种流量类别：VOIP，VPN-VOIP，P2P，VPN-P2P 等。，我们将详细介绍所产生的不同类型的流量：

浏览：在此标签下，我们具有用户在浏览或执行任何使用浏览器的任务时生成的 HTTPS 流量。例如，当我们使用环聊捕获语音呼叫时，即使浏览不是主要活动，我们也捕获了多个浏览流程。

表 1：已捕获的协议和应用程序列表。

交通	内容
网页浏览	Firefox 和 Chrome
电子邮件	SMPTS，POP3S 和 IMAPS
聊天	ICQ，AIM，Skype，Facebook 和环聊
流媒体	Vimeo 和 YouTube
文件传输	使用 Filezilla 和外部服务的 Skype，FTPS 和 SFTP
网络电话	Facebook，Skype 和环聊语音通话（持续 1h）uTorrent 和传输（Bittorrent）
对等	

表 2：基于时间的功能列表。

特征	描述
持续时间	流的持续时间。
菲亚特比亚迪流动性活跃空闲	Forward Inter Arrival Time（转发间隔到达时间），即两个数据包之间向前发送的时间（平均值，最小值，最大值，标准差）。Backward Inter Arrival Time，向后发送两个数据包之间的时间（平均值，最小值，最大值，标准差）。Flow Inter Arrival Time，两个方向之间发送的两个数据包之间的时间（平均值，最小值，最大值，标准）。流量在进入空闲状态之前处于活动状态的时间（平均值，最小值，最大值，标准差）。
fb_psec	流量在变为活动状态之前处于空闲状态的时间量（平均值，最小值，最大值，标准差）。
fp_psec	每秒流字节数。
	每秒流量包。

电子邮件：使用 Thunderbird 客户端以及 Alice 和 Bob Gmail 帐户生成的流量样本。客户端被配置为通过 SMTP / S 传递邮件，并在一个客户端中使用 POP3 / SSL 和在另一个客户端中使用 IMAP / SSL 接收邮件

聊天：聊天标签标识即时消息应用程序。在此标签下，我们通过 Web 浏览器，Skype，使用名为 pidgin 的应用程序的 IAM 和 ICQ 拥有 Facebook 和环聊。

流：流标签标识需要连续且稳定的数据流的多媒体应用程序。我们使用 Chrome 和 Firefox 捕获了来自 YouTube（HTML5 和 Flash 版本）和 Vimeo 服务的流量。

文件传输：此标签标识主要用于发送或接收文件和文档的交通应用程序。对于我们的数据集，我们捕获了 Skype 文件传输，SSH 上的 FTP（SFTP）和 SSL 上的 FTP（FTPS）流量会话。

VoIP： IP 语音标签将语音应用程序生成的所有流量分组。在此标签中，我们使用 Facebook，环聊和 Skype 捕获了语音呼叫。

P2P：此标签用于标识文件共享协议，例如 Bittorrent。为了产生这种流量，我们从公共资源库（*archive.org* 下载了不同的.torrent 文件， 并使用 uTorrent 和 Transmission 应用程序捕获了流量会话-

阳离子。

使用 Wireshark 和 tcp-dump 捕获了流量，生成了总计 28GB 的数据。对于 VPN 流量，我们使用了外部 VPN 服务提供商，并使用 OpenVPN 与之连接。为了生成 SFTP 和 FTPS 流量，我们还使用了外部服务提供商，并使用 Filezilla 作为客户端。

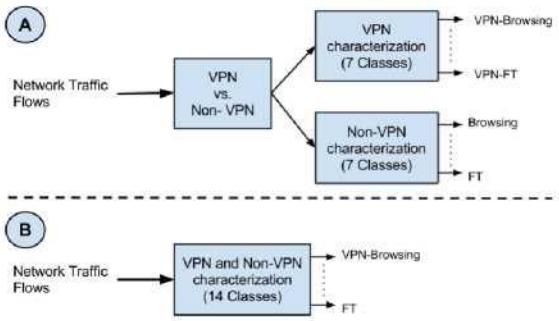


图 1：表征方案。

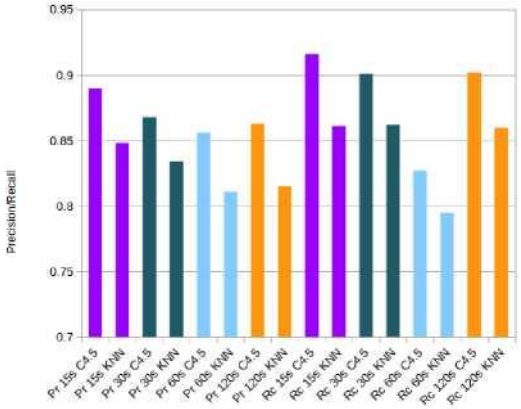
4 实验

我们定义了两个不同的场景 A 和 B，如图 1 所示。如第 3 节所述，我们使用了 4 个不同的流超时值来生成我们的数据集，并且我们选择了 2 种机器学习算法（C4.5 和 KNN）。因此，我们必须将每个实验执行 8 次。我们有

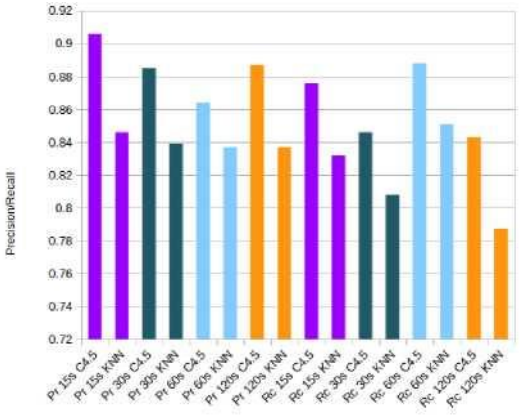
设计了总共 3 个实验，其中 2 个用于方案 A，一个用于方案 B：

方案 A：该**方案**的目的是通过 VPN 识别来表征加密流量，例如，我们将区分语音呼叫（VOIP）和通过 VPN 隧道传输的语音呼叫（VPN-VOIP）。结果，我们将拥有 14 种不同类型的流量，7 种常规类型的加密流量和 7 种 VPN 类型的流量。在此方案中，我们分两步进行表征。首先，我们区分 VPN 和非 VPN 流量，然后分别描述每种流量（VPN 和 Non-VPN）。为了做到这一点，我们将数据集分为两个不同的数据集：一个具有常规的加密流量，而另一个具有 VPN 流量。

方案 B：在此方案中，我们使用混合数据集一步来进行表征。分类器的输入是常规加密流量和 VPN 流量，作为输出，我们具有相同的 14 个不同类别（第 3 节）。



（a）方案 A VPN 定位和召回



（b）场景 A 非 VPN 定位和召回

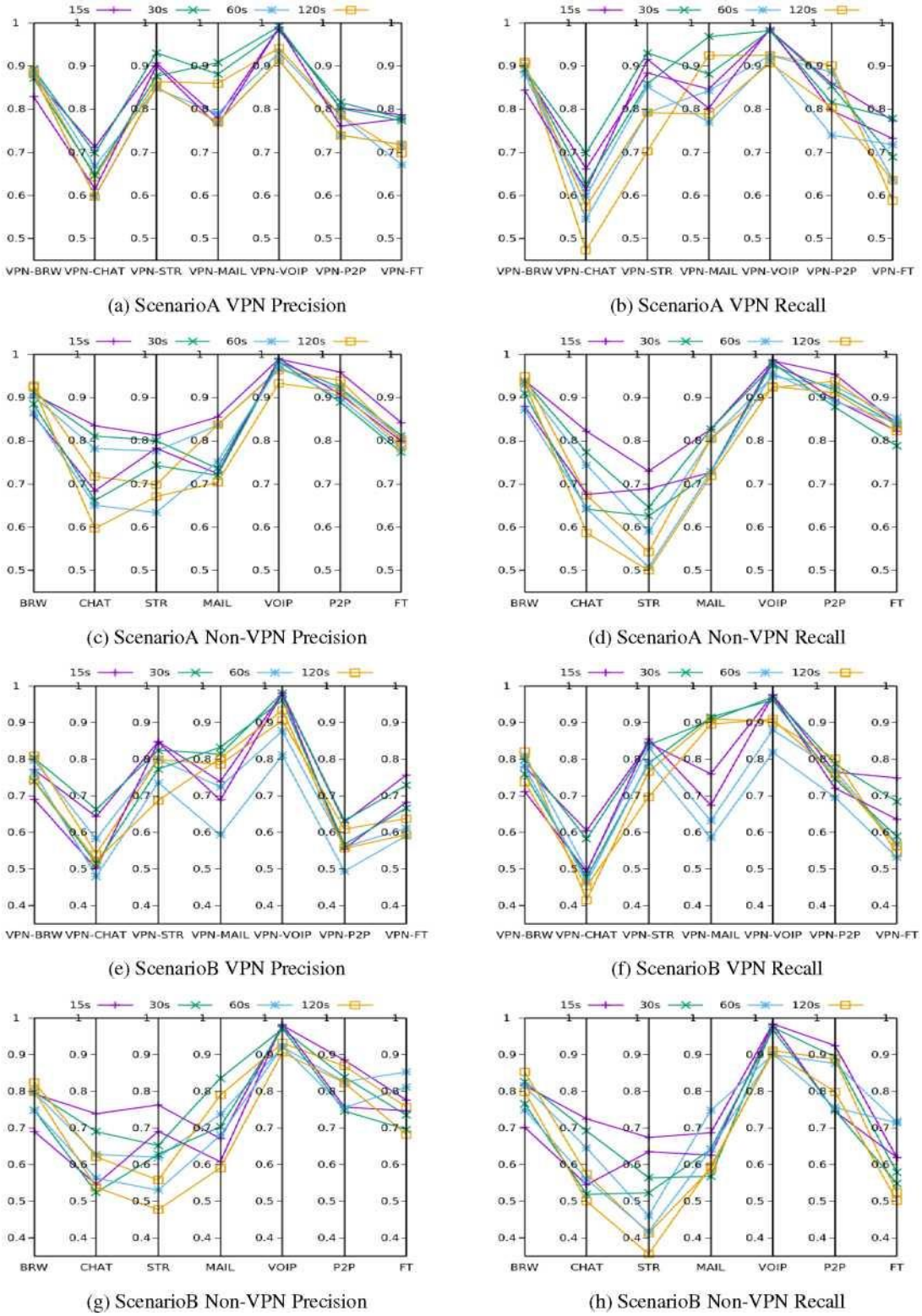
图 2：方案 A-1：VPN 检测。

4.1 流程和特征生成

我们使用流的通用定义，其中流是由一系列数据包定义的，这些数据包具有*{源 IP，目标 IP，源端口，目标端口*和*协议（TCP 或 UDP）}*相同的值。在大多数评论的论文中，流被认为是双向的（正向和反向）（例如，（McGregor 等，2004；Zander 等，2005；Bernaille 等，2006；Williams 等，2006）。；Palmieri 和 Fiore，2009 年）。随着流的生成，我们必须计算与每个流相关的特征。文献中的许多论文都使用一种称为 NetMate 的工具来生成流程和特征，但是作为我们工作的一部分，我们开发了一个应用程序 ISCXFlowMeter。它是用 Java 编写的，在选择我们要计算的功能，添加新功能以及更好地控制流超时的持续时间方面，为我们提供了更大的灵活性。ISCXFlowMeter 生成双向流，其中第一个数据包确定前向（从源到目的地）和后向（从目的地到源）方向，因此与统计时间相关的特征也分别在正向和反向方向上计算。请注意，TCP 流通常在连接断开时（通过 FIN 数据包）终止，而 UDP 流通常通过流超时终止。可以通过单独的方案任意指定流超时值，例如，对于（Aghaei-Foroushani 和 Zincir-海伍德（Heywood），2015 年）。在本文中，我们研究了在同一数据集上的多个流超时（ftm）值及其对应的分类器精度。特别是，我们将流的持续时间设置为 15、30、60 和 120 秒。

在我们的实验中，分类器的响应时间为（FT + *FE* + ML）秒，其中 *FT* 是自定义流程时间，*FE* 是特征提取时间，而 *ML* 是执行分类的机器学习算法时间。已经观察到，对于所有分类器，最大精度都通过 *(FT* = 15s ）实现。在当前的实现中，我们发现所获得的平均延迟约为。（FT + *FE* + *ML* = 15 + 。001 + 。01 *(kNN）或 1 。26 (C4 。5)* = 15 。011 *秒 (kNN) 或* 16 。261 *秒 (C4 。5)* ）的 VPN 分类器和（FT + *FE* + *ML* = 15 + 。001 + 。01 （的 kNN ）*或 1 。49 (C4 。5)* = 15 。011 *秒 (kNN) 或* 16 。491 *秒 (C4 。5)* ）的业务类型分类器。

如前所述，我们专注于与时间相关的功能。选择与时间相关的功能时



(a) ScenarioA VPN Precision

(b) ScenarioA VPN Recall

(c) ScenarioA Non-VPN Precision

(d) ScenarioA Non-VPN Recall

(e) ScenarioB VPN Precision

(f) ScenarioB VPN Recall

(g) ScenarioB Non-VPN Precision

(h) ScenarioB Non-VPN Recall

图 3：流量表征的精度和召回率。

实际上，我们考虑两种不同的方法。在第一种方法中，我们测量时间，例如数据包之间的时间或流保持活动状态的时间。在第二种方法中，我们确定时间并测量其他变量，例如每秒字节数或每秒数据包数。在表 2 中，我们提供了这项工作中提取的功能的完整列表。从表 2 中可以看到，除了持续时间（它显示了一个流程的总时间）外，还有六组要素。前三组分别是：-fiat，-biat 和-flowiat，分别集中在正向，反向和双向流上。关于空闲到活动状态或活动到空闲状态计算第四和第五组特征，并将其命名为-空闲和-活动。最后，

4.2 机器学习方法

为了执行实验，我们使用了 Weka（Hall 等，2009），这是一种众所周知的工具，可以实现不同的机器学习算法。我们使用其默认设置进行 10 倍交叉验证。尽管 Weka 包含许多用于聚类和分类的算法，但就先前的研究工作和人类可读性而言，我们还是从有监督和无监督的家庭中选择了两种算法：C4.5 决策树和 KNN。

C4.5 决策树：该算法由 Ross Quinlan 开发，是机器学习和数据挖掘中最流行的分类技术之一。它基于信息熵的概念。该算法需要一组训练对{inputs-output}，其中输出是相应的类。数字和分类数据都受支持，并且结果以树的形式显示，使其对人类可读。

KNN： K 最近邻算法是机器学习中最简单的算法之一。它基于相似性度量，因此取决于用于计算示例之间距离的度量。分类的输出是类别成员资格，该类别成员资格是根据其 K 个最近邻居的多数票决定的。

为了评估分类过程的质量，我们将使用两个常用指标：精度（Pr）或正预测值和召回率（Rc）或灵敏度。

$$Pr = \frac{TP}{TP + FP} \qquad Rc = \frac{TP}{TP + FN}$$

其中 TP 是正确分类为 A 的实例数，FP 是错误分类为 A 的实例数，而 FN 是错误分类为 Not-A 的实例数。

5 结果分析

在图 2 和 3 中，我们可以看到不同结果的 Precision 和 Recall。总体而言，C4.5 和 KNN 的结果相似，尽管 C4.5 的表现要好一些。但有趣的是，结果取决于所选的超时值。因此，我们选择将注意力集中在这些结果上。对于每个流平局值，我们有两种不同的表示形式（两行），其中一种表示 C4.5 结果，另一种表示 KNN。

5.1 场景 A 分析

在图 2 中，我们获得了方案 A 的第一部分的 Precision（Pr）和 Recall（Rc）结果，其中将流量分为 VPN 和 Non-VPN。我们可以看到流超时（ftm）值与分类器的性能之间存在直接关系。特别是，C4.5 VPN 流量分类器的精度（Pr）从使用 15 秒的 0.890 降低到使用 120 秒的 0.86，非 VPN 流量的 Pr 从 0.906 降低到 0.887。在 KNN 算法的情况下，我们可以看到类似的行为，其中 VPN 流量的 Pr 从 0.848 降至 0.815，非 VPN 流量的 Pr 从 0.846 降至 0.837。使用 C4.5 算法和 15s ftm 可获得最佳结果：VPN 为 0.89，非 VPN 为 0.906。这意味着，使用与时间相关的功能，我们可以将 VPN 与非 VPN 区分为 15 秒的延迟（建立流所花费的时间）。这些结果表明，将时间相关功能用于 VPN 和非 VPN 流量分类时，使用较短的超时值可以提高准确率。

方案 A 的第二部分分别关注 VPN 和非 VPN 流量的特征（请参见图 3，a，b，c，d 部分）。根据第 3 节中定义的流量类别对输入进行分类。同样，较短的 ftm 值的结果要好于较大的值，但 VPN 分类器（图 3a，3b）除外，就像 VPN-MAIL 一样，以 30 秒的 ftm 可获得最佳结果。对于非 VPN 分类器（图 3c，3d），这种趋势可以清楚地看到。

对于 VPN 和非 VPN 分类器，使用 C4.5 和 15s of ftm 可获得最佳结果（平均 Pr）：分别为 0.84 和 0.89。此外，所有流量类别的平均 Pr 均高于 0.84，

这意味着与时间相关的功能是表征加密和 VPN 流量的良好分类器。

5.2 场景 B 分析

在此方案中，所有加密流量和 VPN 流量都混合在一个数据集中，其目的是在不事先将 VPN 与非 VPN 流量分开的情况下表征流量，因此，我们将有 14 种流量：7 种加密流量和 7 种 VPN 流量类别。结果示于图 3（部分 e，f，g，h）。

在这种情况下，我们看不到模式*"更短的超时-更好的准确性"*，就像上一个场景（5.1）一样清晰。例如，使用 C4.5 算法，VPN-浏览，VPN-Mail 和 Mail 的 15 秒的 Pr 分别为 0.771、0.739、0.671，该值低于 120 秒获得的 0.809、0.786、0.79。KNN 结果相似，VPN 浏览，VPN 聊天和 VPN 邮件流量类别的 Pr 分别为（0.691，0.501，0.688）15 秒。ftm，小于 120 秒获得的 Pr（0.743、0.501、0.688）。另一方面，对于 C4.5 和 CNN 算法，来自不同 ftm 值的最高平均 Pr 约为 0.783，比情景 A 的最佳值低约 0.5 点。

6 结论

在本文中，我们研究了时间相关功能的效率，以解决加密流量表征和 VPN 流量检测这一具有挑战性的问题。我们提出了一组与时间相关的功能以及两种常见的机器学习算法 C4.5 和 KNN 作为分类技术。我们的结果证明，我们提出的一组与时间相关的特征是很好的分类器，其准确度达到 80％以上。尽管 C4.5 取得了更好的结果，但在所有实验中 C4.5 和 KNN 的性能都相似。从提出的两个场景（两个步骤（场景 A）的特征化与一个步骤（场景 B）的特征化）中，第一个产生了更好的结果。除了我们的主要目标，我们还发现，当使用较短的超时值生成流时，分类器的性能会更好，这与使用 600s 作为超时持续时间的普遍假设相矛盾。在将来的工作中，我们计划将工作扩展到其他应用程序和类型的加密流量，并进一步研究基于时间的功能在表征加密流量方面的应用。

参考

Aceto，G.，Dainotti，A.，de Donato，W.和 Pescape，A.（2010）。Portload：在流量分类中充分利用两个方面的优势。在 *IEEE 会议上的计算机通信研讨会，* INFOCOM 2010，第 1-5 页。IEEE。

Aghaei-Foroushani，V.和 Zincir-Heywood，A.（2015）。基于流量模式的代理标识符。在 *IEEE 第 16 届高保障系统工程国际研讨会上，* HASE 2015，第 118125 页。IEEE。

Bernaille，L.和 Teixeira，R.（2007）。尽早识别加密的应用程序。在*第八届无源和有源网络测量国际会议论文集中，* PAM'07，第 165-175 页，海德堡，柏林。施普林格出版社。

Bernaille，L.，Teixeira，R.，Akodkenou，I.，Soule，A.和 Salamatian，K.（2006）。即时进行流量分类。*ACM SIGCOMM 计算机通信评论，*36（2）：23-26。

Callado，A.，Kamienski，C.，Szabo，G.，Gero，B.，Kelner J.，Fernandes，S.和 Sadok，D.（2009）。互联网流量识别调查。*通讯调查与指南，IEEE，* 11（3）：37-52。

Coull，SE 和 Dyer，KP（2014）。加密消息传递服务的流量分析：Apple 的不懈追求。*ACM SIGCOMM 计算机通信评论，* 44（5）：5-11。

Gomez Sena，G.和 Belzarena，P.（2009）。使用支持向量机的早期流量分类。在*第五届国际拉丁美洲网络会议论文*集中 LANC '09，第 60-66 页，美国纽约。ACM。

Hall，M.，Frank，E.，Holmes，G.，Pfahringer，B.，Reutemann，P.，and Witten，IH（2009）。weka 数据挖掘软件：一个更新。*ACM SIGKDD 勘探通讯，* 11（1）：10-18。

Iliofotou，M.，Pappu，P.，Faloutsos，M.，Mitzenmacher，M.，Singh，S.和 Varghese，G.（2007）。使用流量分散图（tdgs）进行网络监控。在*第七届 ACM SIGCOMM 互联网度量会议记录中，* IMC '07，第 315-320 页，美国纽约。ACM。

T.Karagiannis，K.Papagiannaki 和 M.Faloutsos（2005）。Blinc：黑暗中的多级别流量分类。在*"2005 年计算机通信的应用程序，技术，体系结构和协议会议"上，* SIGCOMM '05，第 229-240 页，美国纽约，纽约。ACM。

Kim，H.，Claffy，K.，Fomenkov，M.，Barman，D.，Faloutsos，M.和 Lee，K.（2008）。互联网流量分类揭开神秘面纱：神话，警告和最佳做法。在 *2008 年 ACM CoNEXT 会议记录中，*CoNEXT '08，第 11：1-11：12 页，美国纽约。ACM。

Li，W.，Canini，M.，Moore，AW 和 Bolla，R.（2009 年）。高效的应用程序识别和分类架构的时空稳定性。*计算机网络：国际计算机和电信网络杂志，* 53（6）：790-809。

医学博士毛罗（Mauro）和医学博士隆戈（Longo，M.）（2015）。通过机器学习工具显示加密的 WebRTC 流量。在*《第十二届国际安全和密码学会议论文集》中，* SECRYPT '15，第 259-266 页。SciTePress。

McGregor，A.，Hall，M.，Lorier，P.和 Brunskill，J.（2004）。使用机器学习技术进行流聚类。在*"被动和主动网络测量"中，《计算机科学讲座》第* 3015 卷，第 205-214 页。施普林格 柏林 海德堡。

Mohammad SI Mamun，NS 和 Ghorbani，AA（2015）。使用机器学习的基于熵的加密流量分类。在*第 17 届国际信息和通信安全*会议（ICICS 2015）上，海德堡，柏林。施普林格出版社。

Moore，AW 和 Zuev，D.（2005 年）。使用贝叶斯分析技术的 Internet 流量分类。在 *2005 年 ACM SIGMETRICS 国际计算机系统测量和建模会议上，* SIGMETRICS '05，第 50-60 页，纽约，纽约，美国。ACM。

Palmieri F.和 Fiore U.（2009）。一种基于非线性，递归的流量分类方法。*计算机网络：国际计算机和电信网络杂志，* 53（6）：761-773。

Paxson，V。（1994）。基于经验的广域 TCP 连接分析模型。*IEEE / ACM Transactions on Networking，* 2（4）：316-336

Paxson，V.和 Floyd，S.（1995）。广域流量：泊松建模失败。*IEEE / ACM Transactions on Networking，* 3（3）：226-244

Rao，A.，Legout，A.，Lim，Y.-s.，Towsley，D.，Barakat，C.和 Dabbous，W.（2011）。视频流流量的网络特征。在*《第七届新兴网络性能和技术*联盟*会议录》中，* CoNEXT '11，第 25：125：12 页，纽约，纽约，美国。ACM。

Sherry，J.，Lan，C.，RA，Popa 和 Ratnasamy，S.（2015）。Blindbox：通过加密流量进行深度数据包检查。在 *2015 年 ACM 数据通信特别兴趣小组会议论文集* SIGCOMM '15，第 213-226 页，美国纽约，纽约。ACM。

Wang，D.，Zhang L.，Yuan，Z.，Xue，Y.，and Dong，Y.（2014 年）。表征应用程序行为以对 p2p 流量进行分类。在*国际计算机，网络和通信大会上，* ICNC'14，第 21-25 页。IEEE。

威廉姆斯（N.）威廉姆斯（Williams），美国南桑德（Zander）和 G.阿米蒂奇（Armitage）（2006）。五个针对实际 ip 流量分类的机器学习算法的初步性能比较。*ACM SIGCOMM 计算机通信评论，* 36（5）：5-16。

Yeganeh，S.，Eftekhar，M.，Ganjali，Y.，Keralapura，R.和 Nucci，A.（2012）。可爱：使用术语对流量进行分类。在*第 21 届国际计算机通信和网络会议上，* ICCCN '12，第 19 页。IEEE

Zander，S.，Nguyen，T.和 Armitage，G.（2005）。自动化流量分类和应用识别机器学习。在 *IEEE 本地计算机网络会议 30 周年会议记录中，* LCN '05，第 250-257 页，美国华盛顿特区。IEEE 计算机协会。