doi:10.3772/j.issn.1002-0470.2013.10.003

基于主机行为关联的加密 P2P 流量实时分类方法①

熊 刚②[*] [**] [***] 赵 咏[**] 曹自刚[****]

([*]中国科学院计算技术研究所 北京 100190)
([**]中国科学院信息工程研究所 北京 100093)
([***]中国科学院大学 北京 100049)
([****]北京邮电大学计算机学院 北京 100876)

摘 要 提出了一种基于主机行为关联的加密 P2P 流量实时分类方法,该方法基于 P2P 系统中节点间的连接关系,以一定的先验知识为初始条件进行节点发现,并根据网络行为不断进行迭代检测,持续发现 P2P 网络中的新节点及其对应的流量,从而达到对加密 P2P 流量实时分类的目的。真实流量环境中的对比实验表明,该方法对典型加密 P2P 流量的分类准确率、召回率均超过95%,计算代价小、性能高,不依赖于内容检测,不侵犯用户隐私,能有效应用于实时流分类环境中。

关键词 加密 P2P 流量,主机行为,关联,流量分类,实时分类

0 引 言

P2P(Peer to Peer)应用消耗大量网络带宽,近年来很多 P2P 软件采用加密方式进行传输,给运营商的网络管理带来很大挑战。为有效进行网络管理,保障服务质量,运营商希望能够在高带宽环境下较准确地对加密 P2P 流量进行实时分类。

由于加密 P2P 的流量为密文,而且通信端口随机,因此传统的基于端口和基于载荷的深度包检测(deep packet inspection,DPI)技术[1]对其无法有效检测,且后者存在侵犯隐私的问题。

目前,对加密 P2P 流量的分类方法主要有基于流量统计属性的机器学习分类方法和基于主机行为的分类方法。前者主要是基于机器学习的理论进行统计分析,计算复杂度高,难以应用于高速实时场景中。后者一般根据连接模式、持续时间等行为属性来判断,耗时较长,只能做到粗粒度的分类,且在实际应用中难以有效应对网络地址转换(network address translation,NAT)、连接信息不全等挑战。

为了克服上述挑战,本文从主机流量的关联关系入手,设计了一种新颖的主机行为关联算法。基于 P2P 系统中节点间的连接关系,进行迭代关联检测,持续发现 P2P 网络中的新节点及其对应的流量。该算法计算代价小,能有效应用于实时流分类环境。

1 相关工作

网络流量分类的方法主要有 4 类:基于端口、基于载荷、基于主机行为、基于机器学习。其中,基于端口和基于载荷的方法明显无法对加密流进行分类。

目前针对加密 P2P 的分类方法主要集中在基于流量统计特征的机器学习上,但此类方法计算开销较大、精确度较低,难以应用于实时分类的场景,且当流量统计特征变化时,算法有效性将大幅度降低,相关研究还处于实验阶段,未投入在线实际应用中[2]。此外,利用统计特性来区分流量隐含的前提是,不同应用具有可以区分彼此的统计属性[3],但该前提在实际高速网络、复杂应用流量环境下可能不再成立。

基于主机行为的流量分类方法中,最典型的是 Karagiannis 等人的 BLINC 方法[4]。该方法对主机

① 863 计划(2011AA010703),国家自然科学基金(61070184),国家科技支撑计划(2012BAH46B02)和中国科学院战略性先导科技专项课题(XDA06030200)资助项目。
② 男,1977 年生,博士;研究方向:网络信息安全;联系人,E-mail:xionggang@ict.ac.cn
(收稿日期:2012-10-30)

行为模式建立指纹,对单台主机,记录一段时间内与其通信的主机的 IP 地址和端口信息,并将该信息与事先建立好的不同应用模型的指纹进行对比。如果与某种应用指纹匹配,则将这些流量都判定为该指纹代表的应用流量。该方法的优点是在网络应用的行为模式层面进行流分类,不因加密而影响分类质量。缺点是在高速网络环境下分类准确率较低且需要对很长时间段内(长达 10 天)的数据做统一的运算分析,无法实时分类。

Iliofotou 等人的基于图的 P2P 流量分类方法是对 BLINC 方法的扩展[5]。他们将观测视野由单台主机上升到了整个网络,采用 K-means 算法聚类、构造 cluster、相似度合并、构图,最终依据图中各点的联通程度判断某一个类是否属于 P2P 应用。作者声称对 P2P 的分类效果远高于 BLINC 方法,可以达到 90%,但该方法的计算代价仍然很大,难以做到实时的分类,且结果依然是粗粒度的分类。

Hurley 等人采用基于主机行为的启发式方法对 Web 与 P2P 这两类协议集进行了离线和实时分类研究[6]。通过对流的源主机、目的主机、主机间连接、流行为等四个方面分析来获得启发信息。当对每个网络流监测到第 20 包时,对 P2P 的成功识别率达 70% 以上。但该方法仅对两大类流量进行粗分类,且未实现实时分类。

由此可见,虽然基于行为的方法可以对加密流量进行分类,但是已有方法涉及到大量的运算、结果相对延迟,难以实时分类,且均无法细粒度分类。

为了更好地在大流量环境下对加密 P2P 流量进行实时分类,本文将从主机流量之间的关联关系入手,设计并实现一个基于主机行为关联的加密 P2P 流量实时分类方法。

2　基于主机行为实时关联的分类方法

流量的行为或主机的行为特征是加密难以混淆和隐藏的一种特征。现有的行为检测方法通常利用单个会话的行为特征,而这些特征并不能准确地确定该会话的所属协议,因此需要借助于统计特征和机器学习等需要大量运算的方法来提高精度。本方法从新的角度入手,将单个会话的行为特征扩展到多个会话之间的关联关系上,从而能够利用更多的行为特征。新引入的特征可用于直接确认流量行为主体的属性,从而映射到该行为主体对应的协议上,在此基础上进行流量分类,避免了大量的运算且具有较高的精度。

2.1　基本知识和定义

典型 P2P 系统中主机通信模式如图 1 所示。

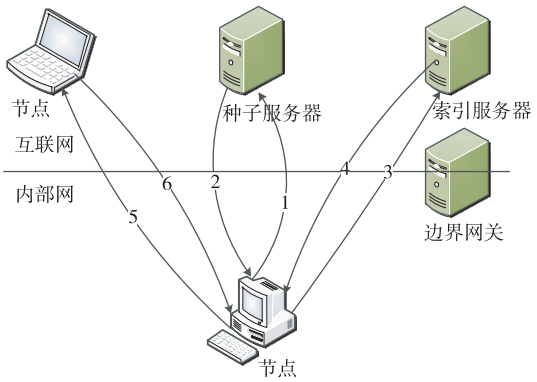

图 1　典型 P2P 系统主机通信模式

典型 P2P 网络如 BT(BitTorrent)和迅雷(Thunder)具有相似的结构和组成。网络中的主机主要有种子分发服务器(比如提供种子下载的 BT 论坛等)、索引服务器(比如 BT 的 Tracker 服务器和迅雷的资源索引服务器)和节点(Peer)。索引服务器仅保存资源和用户关系信息,不保存资源本身,而节点既可以作为下载客户端又可以作为资源存储和分享的服务器。

图 1 中第 1 步和第 2 步为 P2P 节点作为客户端从种子服务器下载资源种子文件,文件中含有资源相关的索引服务器的 IP 和端口信息。客户端通过索引服务器获取包含特定资源的真正 P2P 节点信息。

第 3 步和第 4 步为客户端从索引服务器获取资源相关节点的信息。第 5 步和第 6 步为节点和节点通信,最终实现资源传播。

实时流量分类系统的位置一般位于网络边界,因此图 1 中描绘了边界网关。

需要说明的是,在一个网络内部也可能有 P2P 节点之间的通信,但由于相关流量不经过网络边界,不会对网络出口带宽产生影响,无需也不可能在边界网关对这些流量进行分类。

在实际 P2P 网络架构中,图 1 中的这种通信模式过于简单,没有考虑实际应用场景中的网络地址转换(NAT)情况。

为了缓解 IPv4 地址短缺等问题,在世界上很多地方,尤其是中国,NAT 技术已被广泛使用。NAT 允许多台内网主机共享一个或多个公网 IP 地址,节

约 IP 资源,但由于存在内网 IP 地址和公网 IP 地址之间的端口映射问题,如果缺少 NAT 穿透技术,处在 NAT 设备后的节点无法被外部网络的其他节点成功连接。

目前,NAT 穿透技术已经成为了主流 P2P 系统必不可少的组成部分[7]。NAT 存在的情况下,通信模式如图 2 所示。

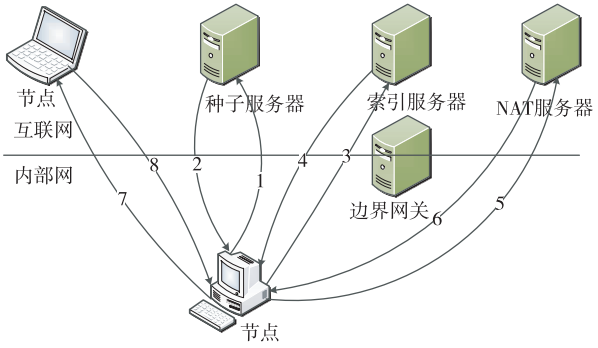

图 2 NAT 环境下的典型 P2P 系统主机通信模式

图 2 中,节点在相互通信之前,要先与 NAT 服务器通信,在获取到对方节点开放的端口信息之后才能与之成功连接。这不仅使网络与应用复杂化,也要求针对 P2P 应用的分类方法必须适应这种情况。本文的主机行为关联算法能够有效应对这种挑战。

NAT 穿越技术包括 UDP 打洞、TURN、ICE、ALG 及 SBC 等。一个典型实例就是 Skype 使用 UDP 打洞绕过防火墙和 NAT 设备。NAT 穿越技术在实现上具有一定的共性。多数方法都要求具有一个公共服务器,且该服务器拥有可公开访问的公网 IP。其中一些方法仅在建立连接时需要使用该服务器,而其它的方法则通过该服务器中继所有的数据。本文将这种用于 NAT 穿越的服务器称为 NAT 服务器。根据上述通信模式,本文将 P2P 网络中的所有端点,包括参与 P2P 连接的节点和服务器统称为主机(Host)。主机可由 IP 和 Htype 两个属性表示,其中 IP 表示 IP 地址,Htype 表示主机类型,包括服务器(Server),节点(Peer)和客户端(Client)。即主机定义为{IP,Htype},Htype ∈ {Server,Peer,Client}。不同类型的主机定义如下:

● 服务器(S):Server,定义为三元组{IP,Proto,Stype},属性依次分别为 IP 地址,传输层协议(TCP/UDP),和服务器类型。其中服务器类型包括 NAT 服务器和普通(Ordinary)服务器,即 Stype ∈ {NAT,Ordi}。

● 节点(P):Peer,定义三元组{IP,Port,Proto},属性分别为 IP 地址,监听端口和传输层协议(TCP/UDP)。

● 客户端(C):Client,定义为一元组{IP},属性为 IP 地址。客户端是未确定监听端口的节点。

为了方便讨论,本文将 P2P 网络中各类型主机的集合相应的进行如下定义:

● 服务器集合 SS(Server Set),是针对特定 P2P 应用已确认的服务器的集合。

● 节点集合 PS(Peer Set),即 P2P 网络的节点集合。

● 客户端集合 CS(Client Set),即暂未确定监听端口的节点集合。

所有类型主机的 IP 集合 HIS(Host IP Set),也是算法中关联 IP 全集 AIS(Association IP Set),可定义为:

● 关联 IP 全集(AIS),元素为一元组{IP},包括上述三个集合 SS,PS 和 CS 中的所有 IP 地址,即 AIS = {IP | IP ∈ SS 或 IP ∈ PS 或 IP ∈ CS}。

由于算法最终是通过对 IP 数据包的关联分析来发现 P2P 网络中的新主机,因此对关联模型中使用的 IP 数据包定义如下:

● IP 数据包(ippkt),定义为六元组{SIP,Sport,DIP,Dport,Proto,HitFlag},属性分别为源 IP、源端口、目的 IP、目的端口、传输层协议、命中标志。命中标志 HitFlag ∈ {0,1,2,3},0 为初始值,表示两个 IP 均未命中;HitFlag 值为 1 表示仅 SIP 命中 AIS;值为 2 表示仅 DIP 命中 AIS;值为 3 表示 SIP 和 DIP 均命中 AIS。

2.2 P2P 主机行为模式假设

P2P 网络三类主机之间的通信行为体现了主机间的关联关系。关联算法对 P2P 系统有如下一般性假设:

假设 1:与已知 P2P 主机的监听端口进行通信的主机也是参与该系统的 P2P 主机。

此假设基于 P2P 的一般性原理。P2P 网络中的普通主机一方面作为客户端向其他节点请求资源,另一方面又作为服务器监听特定端口(一般是 TCP 和 UDP 监听端口各一个),接受其他节点的资源请求并作出应答。因此,一般而言,与已知主机的监听端口进行通信的主机是作为客户端请求资源下载,所以也是参与该 P2P 系统的主机。

本文将不同类型主机间的通信归纳为 4 种情

况:(1)节点与普通服务器的通信;(2)节点与 NAT 服务器的通信;(3)节点间的 UDP 通信;(4)节点间的 TCP 通信。图 2 展示了从校园网边界路由对这 4 种通信进行观察的结果。针对上述 4 种情况,本文分别提出了以下 4 个一般性假设。

假设 2:节点使用随机端口与普通服务器进行通信。

此假设基于节点与普通服务器的通信。在 P2P 网络中,节点需要对邻居节点以及其他必要信息进行查询。虽然在纯 P2P 系统中,这些信息也可以通过其他节点获取,但是新加入的节点仍然需要访问一些初始服务器,从而能够找到最初的一批邻居节点。在目前流行的 P2P 系统中,如 eMule、BitTorrent、迅雷、PPLive 等,均存在提供查询服务的服务器(图 1 中的索引服务器)。节点与这类服务器的通信既可以是 TCP 通信也可以是 UDP 通信,而且由于这类通信大多是一次性的或突发式的,节点一般使用随机端口作为客户端与这些服务器的固定端口进行通信,这也是网络客户端程序通信的一般规律。

假设 3:节点使用固定端口与 NAT 服务器进行 UDP 通信。

此假设基于节点与 NAT 服务器的通信。在互联网中 NAT 是普遍存在的,因此 P2P 系统均具有各自的 NAT 穿透策略。根据前述对 NAT 及其穿透技术的分析,P2P 网络中必然存在用于辅助节点间进行 UDP 通信的 NAT 服务器。节点与 NAT 服务器通信的目的之一是维持 NAT 网关上内网端口与外网端口之间的绑定关系,因此它们之间存在定期的通信流量。另一方面,为了减少对外网端口的占用以及减少程序实现的复杂度,P2P 程序通常使用单个固定的端口与 NAT 服务器以及其他节点进行 UDP 通信。

假设 4:节点与 NAT 服务器通信的 UDP 端口和它与其他客户端节点通信的端口相同。

此假设基于 NAT 环境下节点间的 UDP 通信。在复杂的网络环境下,节点间的数据传输大都通过 UDP 进行。根据节点 NAT 穿透的原理,为了让其他客户端能够连接到 NAT 网络中内网节点的监听端口,此节点需要通过与 NAT 服务器通信告诉服务器其公网 IP 地址对应的监听端口,从而使该端口可被其他节点连接成功。

假设 5:节点使用 TCP 随机端口与其他节点监听的 TCP 端口建立连接。

此假设基于节点间的 TCP 通信。使用 TCP 通信的两个节点之中必须有一方拥有外网 IP 且在某端口上进行监听,另外一方作为客户端使用系统分配的随机端口与其建立连接并通信。

2.3　基于主机行为的关联分类算法

基于针对 P2P 系统的 5 个基本假设,本文提出了基于主机流量行为关联的分类算法。

整个算法开始时应该满足 AIS 不为空,即 AIS≠ø,需根据已有的先验知识,对 SS,PS,CS 中的一个或多个进行初始化,添加一些确定的元素到相应集合中(如将已知的 P2P 服务器 IP 加入 SS 中)。

对每个网络连接的两个方向的第一个 IP 数据包,首先判断此 ippkt 的 SIP 和 DIP 是否在关联集合 AIS 中,如果在,则取命中 IP,然后根据 SIP 和 DIP 属于 SS,PS 和 CS 中的不同情况(即根据主机类型)进行进一步关联分析和处理。因此,关联分析算法可以分为 4 个子模块:(1)IP 筛选;(2)服务器关联分析;(3)客户端关联分析;(4)节点关联分析。

第一步进行 IP 筛选。如果 HitFlag 值为零,则退出本次关联;否则取命中 IP,记为 HitIP,相应的另一端 IP 作为可疑 IP,记为 SusIP(保留端口和协议属性信息便于后继使用)。如果 HitFlag 值为 1 或 2,则直接取命中 IP 为 HitIP;如果 HitFlag 值为 3,此时两端同时命中 AIS,仅需对某一侧为 CS 元素的情况进行处理,取另一端 IP 为 HitIP。算法如图 3 所示。

```
if(ippkt.HitFlag==3), then
        if(DIP∈CS), then
                HitIP = ippkt.SIP;
        else if(SIP∈CS ), then
                HitIP = ippkt.DIP;
        Endif
Else if(ippkt.HitFlag==1), then
        HitIP = SIP;
Else if(ippkt.HitFlag==2), then
        HitIP = DIP;
Endif
```

图 3　子模块 1——IP 筛选

第二步对取出的 HitIP 进行关联分析。根据 HitIP 所属集合不同,即对应的主机类型 Htype 不同,分为 3 个子模块:服务器关联分析、节点关联分析和客户端关联分析。如果 HitIP 同时属于 PS 和 CS 中,则优先执行节点关联分析,再进行客户端关联分析。下面逐一介绍:

服务器关联分析算法:如果命 HitIP 是 NAT 服务器,则与之连接的必定是节点,即 SusIP 是新发现的节点;反之,如果 HitIP 是普通服务器,则与之连

接的必定是客户端,即 SusIP 是新发现的客户端。算法描述如图 4 所示。

```
if(HitIP∈SS),then:
        if(HitIP.Stype==NAT and HitIP.proto==UDP), then
                PS=PS∪{SusIP};
        Else if(HitIP.SType==Ordi and (HitFlag==1 or HitFlag==2), then
                CS=CS∪{SusIP};
        Endif
Endif
```

图 4 子模块 2——服务器关联分析算法

节点关联分析算法:如果命中一端,且该节点协议类型是 UDP,则 SusIP 是新发现的节点或者 NAT 类型服务器;反之,如果该节点的协议类型是 TCP,则 SusIP 是新发现的客户端。如果命中两端且节点类型是 UDP,则 SusIP 是新发现的节点。节点和 NAT 类型服务器的区别在于,NAT 服务器一般采用固定端口,如迅雷 NAT 服务器固定端口号为 8000。实际应用时可以根据不同 P2P 网络的先验知识进行设定,并以此区分不同的 P2P 应用。算法描述如图 5 所示。

```
if(HitIP∈PS),then
        if(HitFlag==1 or HitFlag==2),then
                if(HitIP.Proto==UDP),then
                        if(SusIP.Port==8000),then
                                SS=SS∪{SusIP};
                                SusIP.Stype = NAT;
                        Else
                                PS=PS∪{SusIP};
                        Endif
                Else
                        CS=CS∪{SusIP};
                Endif
        Else
                if(HitIP.Proto==UDP),then
                        PS=PS∪{SusIP};
                Endif
        Endif
Endif
```

图 5 子模块 3——节点关联分析算法

客户端关联分析算法:如果 HitIP 对应的 ippkt 协议类型是 UDP,且两端命中,则 SusIP 是新发现的节点或者 NAT 类型服务器,两者区分方法同上。反之,如果 HitIP 对应的 ippkt 协议类型是 TCP,且两端命中,则 SusIP 是新发现的节点。算法描述如图 6 所示。

需要说明的是,集合中的元素有一定的生命周期,因此算法中还设有超时淘汰机制。

```
if(HitIP∈CS),then
        if (ippkt.Proto==UDP), then
                if(HitFlag==3),then
                        if(SusIP.Port==8000),then
                                SS=SS∪{SusIP};
                                SusIP.Stype = NAT;
                        Else
                                PS=PS∪{SusIP};
                        Endif
                Endif
        Else
                if (HitFlag==3), then
                        PS=PS∪{SusIP};
                Endif
        Endif
Endif
```

图 6 子模块 4——客户端关联分析算法

2.4 算法普适性分析

P2P 系统可以分为两大类,一类是有中心节点型的 P2P 系统,另一类是无中心节点的 P2P 系统。

目前,BT、迅雷等都是典型的有中心节点的 P2P 系统。系统中的所有节点都会定期地访问中心节点并查询信息。因此,只要掌握中心服务器的信息,本文所提出的关联算法就可以快速地发现新的 P2P 节点。同样,对于 Gnutella 等无中心节点的 P2P 系统,节点在启动时同样需要访问内置的 Bootstrap 节点。因此,在掌握 Bootstrap 节点信息的情况下,本文提出的算法仍然可以很好地检测 P2P 流量。

除此之外,为了穿越 NAT,P2P 系统必须提供明确的 NAT 服务器进行辅助,而 NAT 服务器也可以看作是一种中心服务器。

综上所述,本方法适用于已知的两大类 P2P 系统,并且对于带有穿越 NAT 功能的 P2P 系统具有更好的效果。

3 系统实现及实验结果

迅雷系统是目前中国最为流行的 P2P 系统,而且也出现在欧洲、非洲等世界其它地区的流量排名之中[8]。自 2010 年 9 月发布版本 5.9 之后,迅雷系统对其流量采用多种加密及隐藏方式。例如,将节点与服务器的通信伪装成 HTTP 请求的负载。此外,使用专门的加密算法对每个 UDP 数据包进行内容加密及混淆。目前公开文献中,暂无有效地识别迅雷加密流量的方法。

为了验证算法的有效性,本文实现了一套原型系统,并应用到迅雷加密流量的实时分类中。

3.1 实验环境

本文在某校园网网关处对全部流量进行镜像,

实际流量约为 350Mbps 至 450Mbps。该校园网占有 4 个 C 段的公网 IP(约 1020 个),每个公网 IP 下有若干内网主机。因此该网络中的主机大部分通过 NAT 网关与外界通信。在镜像流量中,包含的 IP 地址均为公网 IP,即每个 IP 不同端口的流量有可能是由内网中不同的主机所产生。

镜像数据流由 1 台服务器全部处理(服务器配置为:4 个 Intel Xeon X5660 CPU,主频为 2.80GHz,6 核;内存为 32GB;硬盘容量 300GB;捕包网卡为 1 个千兆光卡;控制网卡为 1 个千兆电卡)。

3.2　流量分类系统

为了实现该分类系统,本文在系统中增加了相关流量处理模块来辅助关联算法的实现。流量分类系统(如图 7 所示)主要分为 4 部分:(1)关联数据检测模块;(2)DNS 应答数据检测模块;(3)DNS 应答数据解析模块;(4)关联分析模块。

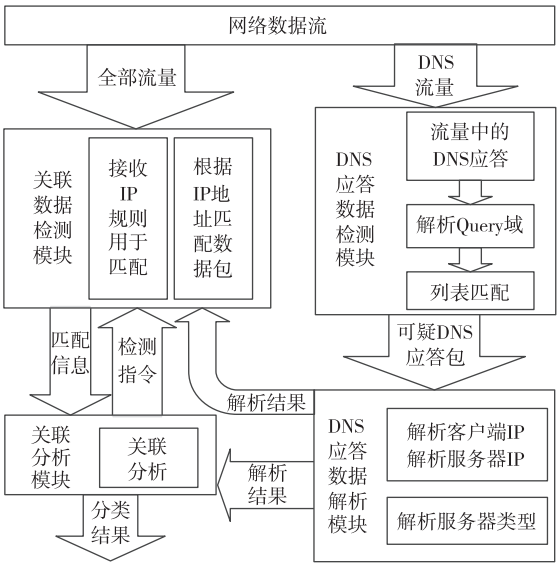

图 7　基于主机关联的流量分类系统

主机行为关联算法是一个迭代式算法,算法的起始需要初始输入。当迅雷客户端启动时,一般要查询指定的服务器域名,获取 DNS 应答,得到必需的一组服务器 IP。DNS 应答数据检测模块负责过滤 DNS 流量,比较请求域名与预存的迅雷服务器域名列表,将命中数据发给 DNS 应答数据解析模块。

DNS 应答数据解析模块对收到的 DNS 应答数据包进行解析,将解析出的迅雷服务器 IP 地址及服务器类型发送给关联数据检测模块;将解析出的迅雷服务器 IP 地址及服务器类型和该数据包对应的查询客户端的 IP 地址发送给关联分析模块进行关联分析。

关联数据检测模块收到 DNS 解析模块和关联分析模块的 IP 地址匹配规则后,根据 IP 地址对网络数据包进行过滤,将匹配的数据包的信息(数据包的源目的 IP、端口和数据包类型等)发送给关联分析模块进行分析。该模块自己管理所有收到的 IP 规则,当检测到某个 IP 匹配规则超时后将其删除。

关联分析模块接收关联数据检测模块发来的流量数据,并依据前文所述关联算法发现新的迅雷主机。对于已发现的主机,关联算法将其添加到对应的集合中,并将检测指令下达给关联数据检测模块。

3.3　分类结果验证与评估

为了验证流量分类系统的实际效果,首先需要能实时、准确地标注出迅雷数据包,以便评估。

通过对迅雷软件的逆向分析,及对其具体协议结构和加密算法的专门研究[9,10],发现迅雷对 UDP 数据包使用的加密算法是可逆的,从版本 5.5.2.252(2006 年 11 月发布)到版本 7.2.9.3634(2012 年 7 月发布)均可逆。因此,本文对流经该校园网络边界的所有流量进行实时解密,并以解密后的流量作为比对的基准,较好地解决了评估标准的问题。

将主机关联系统得到的分类结果同实时解密系统的解密结果进行对比,可实时得到包(字节)准确率、包(字节)召回率等流量分类结果。

准确率是指在被本文标注为迅雷协议的流量中,被解密算法所确认的迅雷流量所占的比例。

召回率是指在所有通过解密识别的迅雷流量中,关联算法识别的流量所占的比例,它反映算法是否能够尽量完整地识别出所有流量。

包准确率和包召回率以 IP 包数量为计量单位,字节准确率和字节召回率以字节数为计量单位。本文使用两种层次的结果是为了更加全面客观地评价本文的算法。在实验过程中,在单台服务器上同时进行关联检测和迅雷流量实时解密。每隔 5 分钟,对比一次主机关联系统和解密系统的结果。图 8、图 9 分别给出了 2012 年 8 月 16 日 0 点至 8 月 16 日 24:00 这 24 小时内的包准确率和字节准确率的统计结果。

根据本文的实验结果,在绝大部分时间内关联算法准确率均基本维持在 95% 以上,这说明关联算法很少将其他协议流量误认为迅雷流量。从包准确率和字节准确率的对比上看,两者准确率的变化趋势一致。

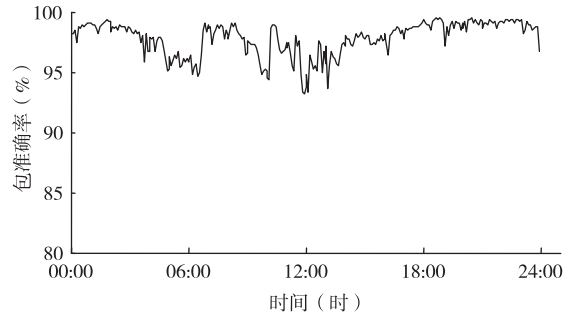

图 8 主机关联算法的包准确率

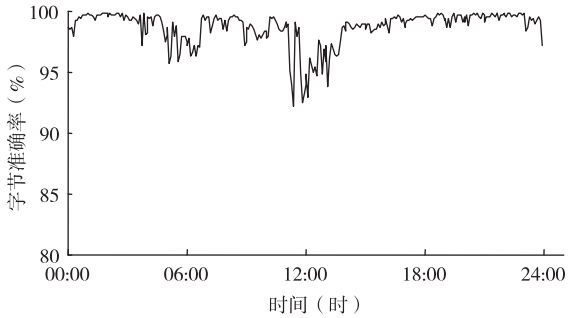

图 9 主机关联算法的字节准确率

关联算法的召回率结果如图 10 和图 11 所示。在实验开始一段时间中，召回率处于一个上升的过程中。这主要是由于部分主机在本文实验开始前就已经运行迅雷，在实验开始后本文的关联算法需要一些时间将这些主机识别出来。除此之外，关联算法的召回率可以基本维持在 95% 以上。

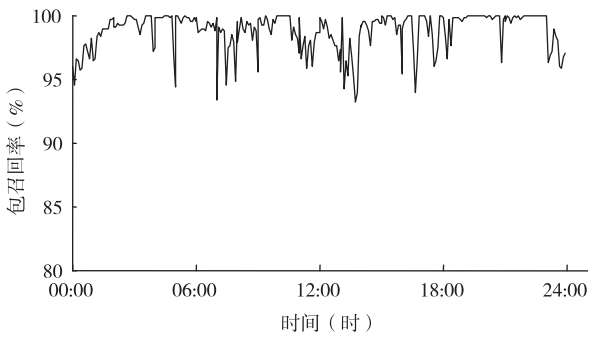

图 10 主机关联算法的包召回率

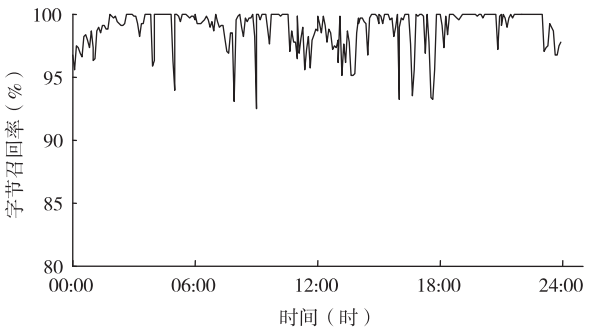

图 11 主机关联算法的字节召回率

此外，实验中，主机行为关联原型系统能够实时处理 350Mbps 至 450Mbps 的流量（约 8 万 pps ~ 15 万 pps），该系统内存使用平均不超过 80MB，CPU 消耗平均不超过 4%，证明该主机行为关联算法不仅能够在大流量网络环境中实时分类，而且还是一种内存代价小的分类方法。

4 结 论

本文利用主机行为之间的关联关系，提出了一种全新的 P2P 加密流量分类方法。该方法仅观测主机流量行为之间的关联关系，不需要检查流量负载的内容，在单机上能够达到约 400Mbps 的分类速度。大流量环境下的持续对比实验表明，该算法能够对国内最为典型的加密 P2P 软件迅雷流量实时分类，平均准确率、平均召回率均达到 95% 以上，是一种适用于高速网络环境、高精度、高召回率的加密 P2P 流实时分类方法。下一步将进行对行为关联体系架构的可扩展性改进、关联算法性能进一步优化、拓展初始行为关联源，并把该方法推广应用到其他加密 P2P 流量的分类上。

参考文献

[1] Sen S, Spatscheck O, Wang D. Accurate, scalable in-network identification of P2P traffic using application signatures. In: Proceedings of the 13th International Conference on World Wide Web, New York, USA, 2004. 512-521

[2] 熊刚，孟姣，曹自刚等. 网络流量分类研究进展与展望. 集成技术. 2012, 1(1): 31-41

[3] Nguyen T, Armitage G A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, 2008, 10(4): 56-76

[4] Karagiannis T, Papagiannaki K, Faloutsos M. BLINC: multilevel traffic classification in the dark. *ACM SIGCOMM Computer Communication Review*, 2005, 35(4): 229-240

[5] Iliofotou M, Kim H, Faloutsos M, et al. Graph-based P2P traffic classification at the Internet backbone. In: Proceedings of IEEE Conference on Computer Communications Workshops, Rio de Janeiro, Brazil, 2009. 1-6

[6] Hurley J, Garcia-Palacios E, Sezer S. Host-based P2P flow identification and use in real-time. *ACM Transactions on the Web*, 2011, 5(2): 7

[7] Liu Y, Pan J. The impact of NAT on BitTorrent-like P2P systems. In: Proceedings of IEEE 9th International Conference on Peer-to-Peer Computing, Seattle, WA, 2009. 9-11

[8] Schulze H, Mochalski K. Internet Study 2008/2009. http://www. ipoque. com/resources/internet-studies/internet-study-2008_2009: ipoque, 2009

[9] Zhao Y, Zhang Z, Wang Y, et al. Performance evaluation of Xunlei peer-to-peer network: A measurement study. In: Proceedings of the Consumer Communications and Networking Conference, Las Vegas, USA, 2011. 257-261

[10] Zhao Y, Zhang Z, Guo L, et al. XunleiProbe: A sensitive and accurate probing on a large-scale P2SP system. In: Proceedings of 12th International Conference on the Parallel and Distributed Computing, Applications and Technologies, Gwangju, Korea, 2011. 62-67

Real-time classification of encrypted P2P traffic based on host behavior association

Xiong Gang[*] [**] [***], Zhao Yong[**], Cao Zigang[****]

([*] Institute of Computing Technology, Chinese Academy of Science, Beijing 100190)

([**] Institute of Information Engineering, Chinese Academy of Science, Beijing 100093)

([***] University of Chinese Academy of Sciences, Beijing 100049)

([****] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876)

Abstract

A real-time method for classification of encrypted P2P traffic based on host behavior association is proposed. Initialized with some priori knowledge, this method finds the nodes in a P2P network according to the nodes' connection relationship, and constantly finds the P2P network's new nodes and their corresponding traffic by examining the iterating over nodes' network behavior to achieve the real-time classification of encrypted P2P traffic. The results of the experiment on a real campus network showed that, besides low computational cost, both the accuracy and recall rate of the proposed method were above 95%. Meanwhile, by classifying traffic without content inspection, the proposal violates no users' privacy, so it can be used flexibly in high-speed network environments.

Key words: encrypted P2P traffic, host behavior, association, traffic classification, real-time classification