基于侧信道特征的IPSec VPN闭合性检测方法

孙云霄, 李军, 王佰玲

引用本文

孙云霄, 李军, 王佰玲. 基于侧信道特征的IPSec VPN闭合性检测方法[J]. 计算机科学, 2023, 50(10): 308-314.

SUN Yunxiao, LI Jun, WANG Bailing. IPSec VPN Closure Detection Method Based on Side-channel Features [J]. Computer Science, 2023, 50(10): 308-314.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230500141

基于侧信道特征的 IPSec VPN 闭合性检测方法

孙云霄[1]　李　军[1]　王佰玲[1,2]
1 哈尔滨工业大学(威海)计算机科学与技术学院　山东 威海 264209
2 哈尔滨工业大学网络空间安全研究院　哈尔滨 150001
(syx@hitwh.edu.cn)

摘　要　IPSec VPN 按照应用场景的不同可以分为闭合型网络和开放型网络,闭合型网络常用于定制虚拟专用网,而开放型网络代理是规避网络审计的常用手段,因此,IPSec VPN 网络类型的识别分类对于网络监管具有重要意义。根据两种网络类型在业务复杂度上的区别,提出利用加密流量侧信道特征进行 IPSec VPN 闭合性检测的方法,提取 IPSec 加密流量帧长序列和隧道内 TCP 最大分片长度(Maximum Segment Size,MSS)的分布,引入信息熵来度量 MSS 值的分布情况,将 MSS 值信息熵和帧长序列的标准差作为特征向量,使用支持向量机和随机森林等机器学习算法进行训练和预测。实验结果表明,使用该分类方法进行闭合性检测的准确率超过了 96%,可有效识别用于开放代理的 VPN 隧道。

关键词:IPSec VPN;闭合性检测;侧信道;TCP 最大分片长度;机器学习
中图法分类号　TP309

IPSec VPN Closure Detection Method Based on Side-channel Features

SUN Yunxiao[1],LI Jun[1] and WANG Bailing[1,2]
1 School of Computer Science and Technology,Harbin Institute of Technology(Weihai),Weihai,Shandong 264209,China
2 Harbin Institute of Technology Research Institute of Cyberspace Security,Harbin 150001,China

Abstract　IPSec VPN can be divided into closed networks and open networks according to different application scenarios. Closed networks are generally used to customize virtual private networks,and open network proxies are commonly used to avoid network auditing. Therefore,the identification and classification of IPSec VPN network types is of great significance for network supervision. According to the difference in traffic complexity between the two network types,a method for IPSec VPN closure detection using side-channel features of the encrypted traffic is proposed. The distribution of IPSec encrypted traffic frame length sequence and TCP maximum segment size in the tunnel is extracted,and information entropy is introduced to measure the distribution of MSS value. The information entropy of MSS value and the standard deviation of the frame length sequence are used as feature vectors. Machine Learning algorithms such as support vector machine and random forest are used for training and prediction. Experimental results indicate that the accuracy of closure detection using this classification method exceeds 96% and can effectively identify VPN tunnels used for open proxies.

Keywords　IPSec VPN,Closure detection,Side-channel,TCP MSS,Machine learning

1　引言

IPSec VPN 可以在两个或多个公共网关间建立安全通道,提供接入认证、访问控制和数据加密等服务,能够有效保护网络通信数据的机密性。然而,互联网中众多的恶意用户利用 IPSec VPN 加密隧道来掩盖自己的恶意行为,从而规避网络审查,给网络安全带来了巨大的隐患。按照工业和信息化部发布的《电信业务分类目录》中的定义,VPN 网络根据使用场景的不同可划分为闭合型网络和开放型网络。闭合型 VPN 网络指采用 TCP/IP 协议,为用户定制互联网闭合用户群网络的服务,并提供一定的安全性和保密性,在虚拟专网内可实现加密透明分组传送,被广泛应用于组织总部和分支机构之间或两个子网之间的局域互联;而开放型 VPN 网络一般用于互联网加密代理,基于 VPN 固有的加密传输属性,对客户端到互联网的流量进行加密保护,从而规避深度包检测(Deep Packet Inspection,DPI)系统的审计与识别。

到稿日期:2023-05-21　返修日期:2023-07-25
基金项目:国家重点研发计划(2021YFB2012400);国家自然科学基金(62272129);中央高校基本科研业务费专项资金(HIT.NSRIF.2020098)
This work was supported by the National Key R&D Program of China(2021YFB2012400),National Natural Science Foundation of China(62272129) and Fundamental Research Funds for the Central Universities of Ministry of Education of China(HIT.NSRIF.2020098).
通信作者:王佰玲(wbl@hit.edu.cn)

下面给出 IPSec VPN 闭合型网络和开放型网络的一般定义。在 IPSec VPN 隧道网络中，设 C 表示客户端集合，S 表示服务端集合，集合 C 和集合 S 中的元素通过 IPSec VPN 隧道分别建立安全连接。闭合型网络中(见图 1)，考虑两种场景，一是远程接入场景，集合 C 中只有单一的用户终端通过 VPN 网关访问集合 S 中有限个数的服务器；二是子网互联场景，集合 C 和集合 S 中都只有有限个数的用户终端或者服务器，双方通过各自的 VPN 网关进行安全互联。开放型网络中(见图 2)，集合 C 包含不确定数量的用户终端，以 VPN 网关作为代理对集合 S 中的服务器发起访问，集合 S 中服务器的数量同样是不确定的，假设集合 C 中有 m 个元素，集合 S 中有 n 个元素，C 和 S 之间最多可建立 $n\times m$ 个连接。两种网络类型最根本的区别在于集合 C 和 S 中元素个数的数量级和可预测性不同。根据定义，闭合型网络中客户端和服务端建立的连接数要远远少于开放型网络。

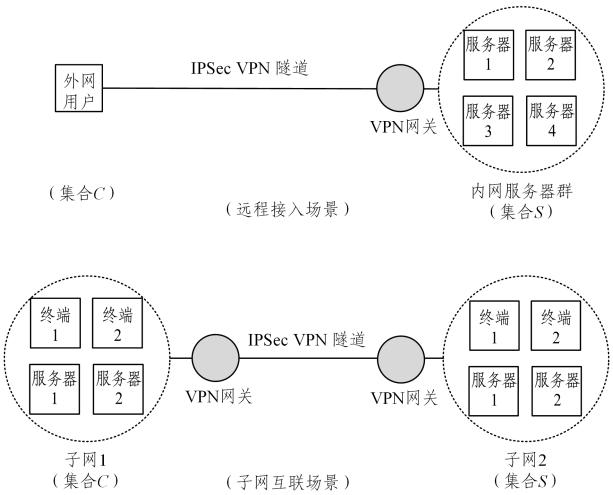


图 1 IPSec 闭合型网络

Fig. 1 IPSec closed network

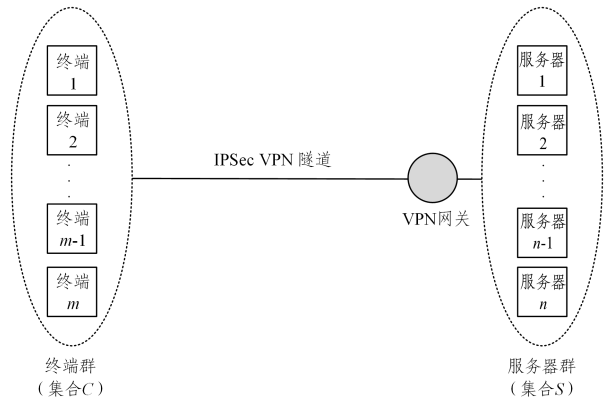


图 2 IPSec 开放型网络

Fig. 2 IPSec open network

由于传统的网络安全设备无法针对加密的 IPSec 流量进行审计，攻击者往往会通过 VPN 隧道代理恶意流量，以达到隐藏攻击行为或攻击源的目的[1]，因此研究 VPN 隧道的闭合性检测方法对于提升网络空间安全防护及攻击溯源能力具有重要意义。

IPSec VPN 隧道的闭合性检测属于加密流量分类问题的范畴，目前主流的流量分类方法包括端口过滤、深度包检测和基于流量特征的机器学习分类[2]等。端口过滤技术及深度包检测技术[3-7]已发展成熟，并衍生出了大量的网络安全产品，但难以应用于加密流量分类领域；机器学习分类算法，如随机森林[8]、K 最近邻[9-10]等也在流量分类研究中得到广泛应用，但目前尚无针对 VPN 隧道闭合性检测问题的研究。文献[11]采用混合方法对传输单一应用数据的 VPN 隧道进行业务分类，然而 VPN 隧道中往往包含多种网络应用产生的数据，该分类方法难以在实际应用中达到预期的效果。因此，本文提出了基于侧信道特征的 IPSec VPN 闭合性检测方法。

侧信道攻击方法在狭义上特指针对密码算法和密码系统的非侵入式攻击，此类方法通过分析加密电子设备在运行过程中产生的侧信息(如功耗、电磁辐射、运行噪声等)达到破解密码算法的目的[12]，主要包括针对密码算法的计时分析攻击[13]、能量分析攻击[14]和电磁分析攻击[15]等。网络加密流量侧信道分析技术借鉴了传统的侧信道攻击方法，通过分析与数据加密算法无关的内容来达到获取敏感信息的目的，包括网络流量的包长、时间序列、传输速率[16]等。由于 IPSec VPN 隧道对数据进行加密传输，无法通过网络加密流量还原其原始内容，因此只能采取侧信道分析的方法，通过提取加密流量的侧信道信息，构建可以表征不同应用模式下的流量行为特征向量，进而对网络类型进行分类识别。

本文从网络拓扑及信息流动的角度将 VPN 隧道划分成闭合型和开放型两种类型，通过网络侧信道测量来构建隧道流量特征，以刻画 VPN 内的业务类型复杂度。基于 TCP 流量分段传输的特点，引入信息熵度量 MSS 值的分布和标准差度量加密流量帧长的波动，基于 MSS 值信息熵和帧长序列标准差构建特征向量，使用机器学习算法训练得到分类器。基于典型的用户行为构建了测试环境，经实验验证，使用上述特征向量在多种机器学习算法下均能取得良好的分类识别效果。

2 IPSec 隧道流量的帧长特征

IPSec 协议簇[17]构建了 IP 层上通信安全的一整套体系结构，包括认证头(Authentication Header，AH)协议、封装安全负载(Encapsulating Security Payload，ESP)协议、网络密钥交换(Internet Key Exchange，IKE)协议，以及用于网络认证和数据加密的一系列算法等。IPSec 通过对等体间的协商来选择安全协议、确定安全算法和进行密钥交换，向用户提供访问控制、数据源认证、数据加密等安全通信保障。

IPSec 可配置为两种不同的模式，即隧道模式和传输模式，本文的分析以及实验均基于隧道模式。IPSec 建立安全通道后，受保护的上层数据经过 ESP 协议封装。封装后的 ESP 包的长度由原始报文长度、分组加密填充、完整性校验算法等因素决定，表 1 中列出了不同协议层中控制帧长的字段。在网络层中，IP 协议中用来控制帧长的字段是最大传输单元(Maximum Transmission Unit，MTU)，MTU 的值是由数据链路层决定的，其遵循“木桶原理”，即 IP 数据包的长度在传输过程中须小于所经路径上规定 MTU 的最小值。

表 1 协议层包长控制字段

Table 1 Packet length control field in protocol layers

协议层	协议类型	帧长控制字段	备注
网络层	IP	MTU	最大传输单元
传输层	TCP	MSS	最大分片长度
	UDP	—	—

在传输层中，UDP 协议没有控制帧长的字段，数据分组的长度由应用层协议决定；而 TCP 协议中用来控制帧长的字段是 MSS，MSS 字段是 TCP 协议中定义的一个选项[18]，用于在 TCP 连接建立时，收发双方协商通信时每一个报文段所能承载的最大数据长度。TCP 在向网络层发送数据时受 MTU 限制，长度超过 MTU 值的数据包将在网络层被强制分片。为达到最佳的传输效能，TCP 连接双方通过控制 MSS 值的大小来避免数据包被分片，因此 MSS 值的大小往往小于 MTU 值减去传输层和网络层的头部长度。例如，在以太网和 IPv4 网络环境中，MTU 被设置为 1 500 字节，一次 TCP 会话中双方协商的 MSS 值为 1 440 字节，该会话中出现的最长的 IP 包为 1 440 字节（TCP 最大载荷）+ 20 字节（TCP 头部）+ 20 字节（IP 头部）= 1 480 字节 < MTU 值，这样就使得每一个 TCP 数据包到达 IP 层后不会被分片，提升了数据传输效率，减少了分片可能导致的错误。

图 3 给出了 TCP 业务数据在进入 IPSec VPN 隧道之前的封装过程，首先，传输层将上层业务数据按照 MSS 值进行分片；然后添加 TCP 头部和内层 IP 头部，整体填充之后进行加密；最后，将密文作为载荷封装成 ESP 包。封装结束后会产生多个“满载帧”和一个“尾帧”，“满载帧”即内部的 TCP 分片长度达到了 MSS，而“尾帧”内部的 TCP 分片长度小于或等于 MSS。TCP 数据经过封装、填充和加密后，已经无法直接从加密数据获取 MSS 值，但内部包长达到 MSS 值的分片经过填充和加密后表现为“满载帧”或接近“满载帧”的帧长，因此，通过加密数据中“满载帧”或接近“满载帧”的帧长可以近似地反映内层 TCP 数据的 MSS 值情况。

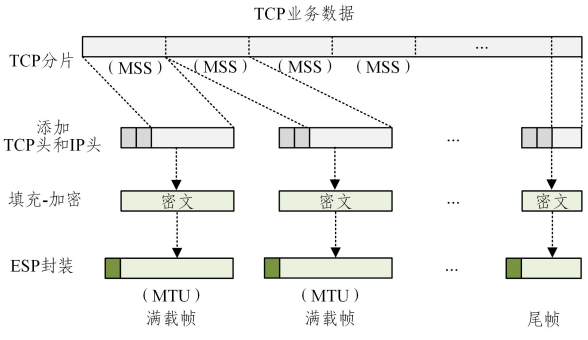


图 3 隧道内 TCP 数据封装流程

Fig. 3 Process of encapsulating TCP data in the tunnel

3 基于侧信道特征的闭合性检测方法

图 4 给出了一般情况下两种网络类型的结构和规模，在开放型网络中，客户端通过 IPSec VPN 代理服务器访问互联网中的服务器，由于应用了内容分发网络（Content Delivery Network，CDN）和网络托管等技术，互联网服务器之间存在多级连接和跳转，导致客户端发起访问时建立的会话连接数量大大增加；而在闭合型网络中，服务器数量有限，提供的业务类型也比较单一。在网络环境中有多个因素会对 MSS 值的大小产生影响，例如操作系统设定、MTU 值、TCP 窗口大小等，因此在开放型网络中，服务器和服务类型的多样性将会导致 MSS 的多样性，同时也会导致开放型网络中的“尾帧”和“短帧”（长度未达到 MSS 值的独立帧）的数量远多于闭合型网络。因此，理论上两种网络类型所产生的加密流量在 MSS 值分布和帧长的波动情况上存在较大差异。

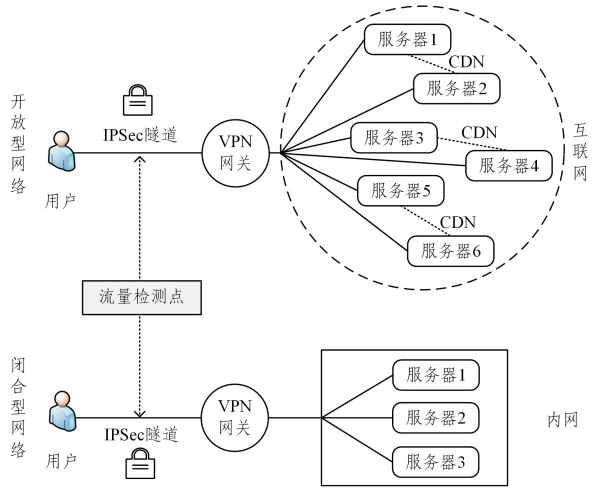


图 4 两种网络类型对比

Fig. 4 Comparison of two network types

3.1 基于侧信道特征的闭合性检测框架

基于侧信道特征的闭合性检测框架（见图 5）包括数据采集、数据预处理、特征向量提取、模型训练和分类器 5 个部分。

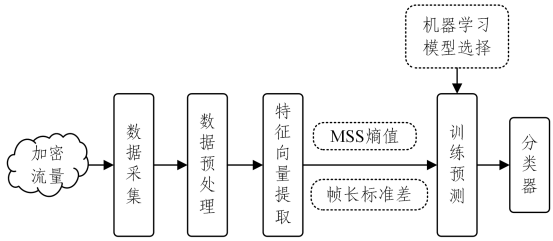


图 5 基于侧信道特征的闭合性检测框架

Fig. 5 Closure detection framework based on side-channel features

对 IPSec VPN 网络中的目标服务器 S 进行闭合性检测，S 是 VPN 网关，负责向多个客户端$\{C_1, C_2, \cdots\}$提供 IPSec 代理服务。假定网络监管部门在该网络的关键网络节点上具备获取镜像流量的能力，服务器 S 与客户端C_i一段时间内通信的双向数据流定义为$flow_{(S\text{-}C_i)}=\{P_1, P_2, \cdots, P_n\}$，其中$P_k=[IP_{\text{src}}, IP_{\text{dst}}, Port_{\text{src}}, Port_{\text{dst}}, Protocol]$表示一段时间内产生的具有相同五元组的包集合，$\{P_i\}$序列构成了服务器 S 与客户端C_i的一个双向数据流。收集服务器 S 与所有客户端$\{C_1, C_2, \cdots\}$通信的数据，经过预处理后得到数据流序列$\{flow_{(S\text{-}C_i)}\}$；将流序列作为算法的输入，提取特征向量 $\boldsymbol{F}$；根据 $\boldsymbol{F}$ 的特点选择合适的机器模型来进行训练和预测；最后，对分类效果进行评估。

3.2 特征向量选择

IPSec VPN 对 IP 数据进行了加密封装，内部信息被

隐藏，除上文中提到的 MSS 值以及帧长的分布外，还可以通过一些流量统计特征来对隧道内部数据传输情况进行测量，如平均帧长、帧间隔时间等。本文基于机器学习流量分类研究领域的前期研究成果，选择了几个可能对隧道类型分类有贡献的流量统计特征进行研究，具体的备选特征如表 2 所列。

表 2 加密流量特征

Table 2 Encrypted traffic characteristics

特征	含义
MSS_Entro	MSS 值分布
PL_Devi	帧长分布
FB_Psec	每秒字节数
FB_Psec	每秒帧数
PK_Inter	帧间隔时间
PK_Mean	平均帧长
FL_Duration	会话持续时间

在备选特征中，帧间隔时间、会话持续时间等统计特征与用户主观行为的关联度较大，因此特征稳定性和通用性较差，对于两种网络类型不能很好地区分。同样地，每秒帧数、每秒字节数、平均帧长也受到用户所发起请求类型的影响，例如，封闭型和开放型网络在进行文件传输类操作时，都会产生较为密集的长帧序列，而在一般的网页访问场景下，又都会产生稀疏的短帧。根据上文中的分析，两种网络的业务类型和服务器数量有本质区别，这就导致了它们在 MSS 值以及帧长的分布上有差异。经过实验验证，当使用 *MSS_Entro* 和 *PL_Devi* 两个特征作为特征向量时，分类精度可以达到 0.98。在达到理想分类效果的条件下，为降低特征抽取的复杂度以及分类模型的复杂度，本文选取 *MSS_Entro* 和 *PL_Devi* 两个特征作为表述隧道流量行为的特征向量。

本文通过收集目标网络中的加密流量，获取加密流量的帧长序列、载荷长度等侧信道信息，根据载荷长度计算目标服务器的 MSS 值分布，引入香农信息熵[19]来刻画分布的混乱程度。信息熵是用于衡量不确定性的指标，也就是离散随机事件出现的概率，简单地说，情况越混乱，信息熵就越大，反之则越小。信息熵的计算公式如下：

$$MSS\_Entro=-\sum_{i=1}^{n}p_i\log^{p_i} \tag{1}$$

其中，p_i 表示第 i 种 MSS 值出现的概率。

用标准差来衡量帧长序列的波动情况：

$$PL\_Devi=\sqrt{\frac{\sum_{i=1}^{N}(X_i-\mu)^2}{N}} \tag{2}$$

其中，X_i 为单帧长度，μ 为一次会话流中帧长的平均值，N 为样本总数。基于 MSS 值信息熵和帧长序列标准差构建特征向量 $\boldsymbol{F}=(MSS\_Entro, PL\_Devi)$。

具体方法是根据实际网络环境中“满载帧”的长度设置 MSS 阈值（*MSS_TS*），载荷长度超过该阈值的数据包被认为是内部封装数据达到了 TCP 数据包的最大分片长度，遍历数据流序列 $\{flow_{(S\text{-}C_i)}\}$，对于任意 $flow_{(S\text{-}C_j)}\in\{flow_{(S\text{-}C_i)}\}$，计算数据流 $flow_{(S\text{-}C_j)}$ 中每一组 P_k 的特征向量，最后组合成目标服务器 S 的特征向量集合，算法伪代码如算法 1 所示。

算法 1 提取目标服务器的特征向量

输入：目标服务器 S 的数据流序列{$\text{flow}_{(S\text{-}C_i)}$}

输出 S 的特征向量集合{**F**}

```
1. for {flow(S-Cj)} in {flow(S-Ci)} do:
2.   for Pk in {flow(S-Cj)} do:
3.     for packet in Pk do:
4.       if packet.len > MSS_TS then: /* 判断包长是否超过了阈值 */
5.         MSS_DICT.append(packet.len, packet.cnt); /* 保存至 MSS 值字典 */
6.     end for
7.     MSS_Entro = CalcEntropy(MSS_DICT) /* 使用式(1)计算 MSS 信息熵 */
8.     PL_Devi = CalcDeviation(Pk) /* 使用式(2)计算帧长标准差 */
9.     {F} ∪ [MSS_Entro, PL_Devi] /* 构建目标服务器特征向量集合 */
10.  end for
11. end for
12. return {F} /* 返回特征向量集合 */
```

算法运行后得到了目标服务器 S 的特征向量集合{$\boldsymbol{F}$}。

3.3 分类及评价标准

对 IPSec VPN 进行闭合性检测的目标是区分闭合型网络或开放型网络，是一个二分类问题。传统机器学习算法在解决二分类问题上有很好的表现，因此，选取支持向量机[20]（SVM）、随机森林（RF）和 ID3 决策树[21] 3 种算法构建分类器，利用算法 1 得到的特征向量集合{$\boldsymbol{F}$}进行训练和预测。为避免数据集划分的偶然性，本文采用随机排列交叉验证方法，将特征向量集合按一定比例随机划分为训练集和测试集进行训练和测试，将该过程重复 10 次，取 10 次结果的平均值。

定义开放型网络为正例，封闭型网络为负例，对于机器学习算法训练产生的模型，使用准确率（Accuracy）、精确率（Precision）、召回率（Recall）和 F1 值来对模型进行评价。上述 4 个评价指标的计算式如下，参数含义如表 3 所列。

$$Accuracy=\frac{TP+TN}{TP+TN+FP+FN} \tag{3}$$

$$Precision=\frac{TP}{TP+FP} \tag{4}$$

$$Recall=\frac{TP}{TP+FN} \tag{5}$$

$$F_1=\frac{2\times TP}{2\times TP+FN+FP} \tag{6}$$

表 3 评价标准参数

Table 3 Evaluation criterion parameters

参数名	含义
TP(True Positive)	开放型网络被分类成正例的数量
FN(False Negative)	开放型网络被分类成负例的数量
FP(False Positive)	闭合型网络被分类成正例的数量
TN(True Negative)	闭合型网络被分类成负例的数量

4 实验与结果分析

本文设计了用于 IPSec 闭合性检测识别的实验验证系统，如图 6 所示，包含网络流量采集模块、数据预处理模块、侧信道特征分析模块、标签分类器等。网络流量采集模块的

主要功能是在模拟环境中的监测点实时地获取网络流量并进行本地存储；数据预处理模块将流量文件进行过滤清洗，提取目标服务器会话流序列；侧信道分析模块提取会话流序列中的特征向量；标签分类器对特征向量进行训练和预测。

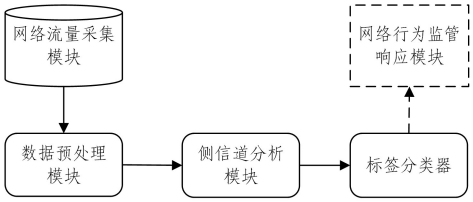


图 6 基于侧信道特征的闭合性检测功能模块

Fig. 6 Closure detection function mode based on side-channel features

4.1 模拟环境与数据采集

本文通过构建模拟环境来获取实验数据，基于开源工具 StrongSwan 分别构建了仿真的 IPSec VPN 闭合型网络和开放型网络，模拟环境均基于以太网环境下的 IPv4 协议，模拟环境拓扑图如图 7 所示，环境配置信息如表 4 所列。其中闭合型网络中终端访问内网 HTTP 服务器、FTP 服务器和 SSH 服务器等；在开放型网络中，客户端通过 IPSec 网关访问互联网中的各种服务器。在 IPSec VPN 隧道中设置流量监测点，可以获取所有流经监测点的数据包。

表 4 数据集信息

Table 4 Dataset information

网络类型	客户端数量及操作系统	服务器数量	TCP 服务种类
开放型	Linux * 2	大于 10	SSH, HTTP, HTTPS, FTP, TELNET, SMTP 等
闭合型	Linux * 2	3	HTTP, FTP, SSH 等

使用模拟环境中的终端分别访问对应的服务器，闭合型网络终端主要进行 HTTP 网页访问和 FTP 与 SSH 文件传输等操作；开放型网络访问互联网中不同的服务器，包括邮件服务器、视频网站、购物网站、社交网站、直播网站等，每一轮访问持续至包数达到预置上限时停止，将流量落盘存储为文件，在两种网络环境中分别进行 100 轮采集，共产生逾 2 000 000 帧数据，按时间序列对流量文件依次编号并打上正、反例标签。

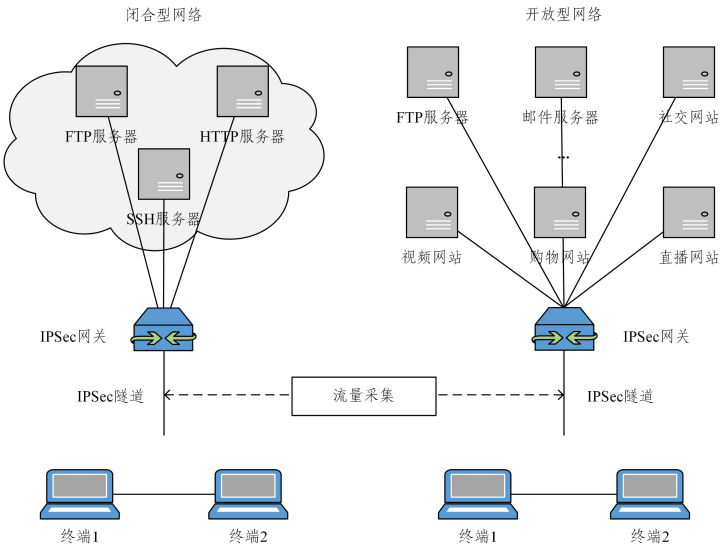


图 7 模拟环境拓扑图

Fig. 7 Topology of simulation environment

4.2 特征向量提取

分析采集到的流量文件，首先统计其 ESP 载荷的长度分布（见图 8、图 9），根据预先对网络环境中 TCP 数据的分析，将 *MSS_TS* 值设为 1 300 字节，不难发现，开放型网络中“满载帧”（载荷长度＞ *MSS_TS*）的分布明显比闭合型网络更加分散，说明开放型网络中包含的 MSS 值的种类更多。同时，相较于闭合型网络，开放型网络中的“短帧”和“尾帧”数量更多，因此帧长序列波动会更大。造成这种差异的根本原因是两种网络类型在业务复杂度方面存在差异。

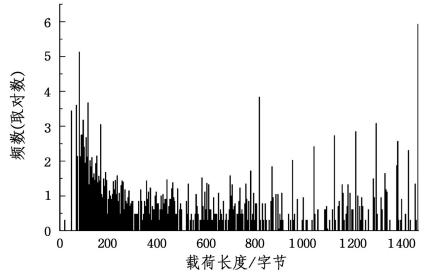


图 8 IPSec 闭合型网络 ESP 载荷长度分布

Fig. 8 ESP payload length distribution of IPSec closed network

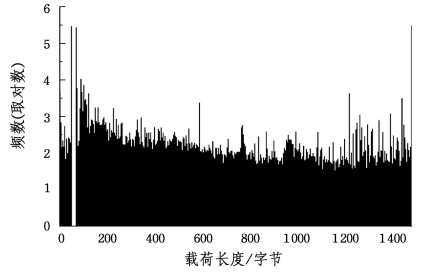


图 9 IPSec 开放型网络 ESP 载荷长度分布

Fig. 9 ESP payload length distribution of IPSec open network

对流量文件进行清洗和预处理，将数据按照五元组[IP_{src}，IP_{dst}，$Port_{src}$，$Port_{dst}$，$Protocol$]进行筛选，获取目标服务器 S 的数据流序列$\{flow_{(S\subset_i)}\}$，输入算法 1 获取特征向量集合$\{\boldsymbol{F}\}$。

4.3 分类与结果分析

分别使用 SVM，RF 和 ID3 算法对特征向量集合 $\boldsymbol{F}=(MSS_Entro, PL_Devi)$进行训练和预测，采取随机排列交叉验证的方法，训练集与测试的比例设为 3∶1，共进行 10 轮实验，每一轮的结果如表 5 所列，取各项性能指标的平均值。图 10 给出了 3 种算法的性能指标对比结果，可以看出，3 种算法的各项性能指标均超过了 0.96，都能很好地完成分类识别任务。相较于随机森林算法，支持向量机算法和 ID3 算法在准确率、召回率和F_1值上都有 1%左右的优势。通过计算 10 轮实验的F_1值的标准差可以发现 3 种算法的实验结果比较稳定，分类效果较好，但是仍存在“误报”(将闭合型网络预测为开放型网络)和“漏报”(将开放型网络预测为闭合型网络)的情况，原因可能是特征向量的选取还不够精准或者某些数据集中正例、负例的区分度不够高，存在一定的偶然性。

表 5 实验结果

Table 5 Experimental results

实验编号	*Accurary*			*Precision*			*Recall*			F_1		
	SVM	RF	ID3	SVM	RF	ID3	SVM	RF	ID3	SVM	RF	ID3
1	0.940	0.940	0.960	0.957	0.957	1.000	0.917	0.917	0.917	0.936	0.936	0.957
2	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
3	0.980	0.960	0.980	1.000	1.000	1.000	0.957	0.913	0.957	0.978	0.955	0.978
4	0.980	0.940	0.960	0.963	0.960	0.962	1.000	0.923	0.962	0.981	0.941	0.962
5	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
6	0.960	0.940	0.980	0.957	0.955	1.000	0.957	0.913	0.957	0.957	0.933	0.978
7	0.980	0.980	0.980	0.958	0.958	0.958	1.000	1.000	1.000	0.979	0.979	0.979
8	0.980	0.980	0.980	1.000	1.000	1.000	0.966	0.966	0.966	0.982	0.982	0.982
9	0.980	0.980	0.980	0.958	0.958	0.958	1.000	1.000	1.000	0.979	0.979	0.979
10	0.940	0.960	0.940	0.957	0.958	0.957	0.917	0.958	0.917	0.936	0.958	0.936
均值	0.974	0.968	0.976	0.975	0.975	0.984	0.971	0.959	0.968	0.973	0.966	0.975
标准差	0.021	0.022	0.017	0.020	0.021	0.020	0.032	0.038	0.031	0.022	0.024	0.018

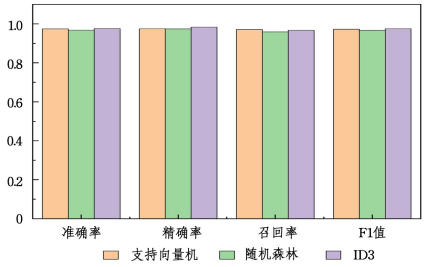


图 10 算法性能对比

Fig. 10 Comparison of algorithm performance

结束语 本文根据 IPSec VPN 开放型网络和闭合型网络在服务器数量和业务复杂度等方面的区别，提出了基于网络加密流量的侧信道特征进行闭合性检测的方法，分析加密流量的帧长序列和载荷长度等特征，提取目标服务器的 MSS 值分布和帧长序列的标准差，引入信息熵来刻画 MSS 值的分布情况，将 MSS 值信息熵和帧长序列的标准差作为特征向量，使用机器学习算法训练得到分类模型，实现了对 IPSec VPN 的闭合性检测，为网络监管和安全审计提供了一个重要的工具。下一步将继续研究 IPSec VPN 网络类型识别的相关方法，使识别依据更加丰富，分类标签更加细化。

参 考 文 献

[1] HAN Z H，CHEN X S，ZENG X M，et al. Detecting Proxy User Based on Communication Behavior Portrait[J]. The Computer Journal，2019，62(12)：1777-1792.

[2] REZAEI S，LIU X. Deep Learning for Encrypted Traffic Classification：An Overview [J]. IEEE Communications Magazine，2019，57(5)：76-81.

[3] ALSHAMMARI R，ZINCIR-HEYWOOD N. Generalization of signatures for SSH encrypted traffic identification[C]// Proceedings of Computational Intelligence in Cyber Security Conference. 2009：167-174.

[4] ANDERSON B，PAUL S，MCGREW D. Deciphering Malware's Use of TLS(without Decryption)[J]. Journal of Computer Virology and Hacking Techniques，2018，14(3)：195-211.

[5] ANDERSON B，MCGREW D. Machine learning for encrypted malware traffic classification：accounting for noisy labels and non-stationarity[C]// Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2017：1723-1732.

[6] L7 filter[EB/OL]. [2023-02-10]. http://l7-filter. sourceforge. net/.

[7] OpenDPI[EB/OL]. [2023-02-10]. https://github. com/thomasbhatia/OpenDPI.

[8] WANG L，FENG H M，LIU B，et al. SSL VPN encrypted traffic identification based on hybrid method[J]. Computer Applications and Software，2019，36(2)：321-328.

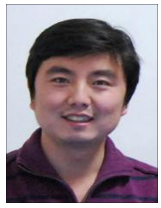
[9] SU M Y . Using clustering to improve the KNN-based classifiers for online anomaly network traffic identification[J]. Journal of Network & Computer Applications，2011，34(2)：722-730.

[10] WU D，CHEN X，CHEN C，et al. On addressing the imbalance problem：a correlated KNN approach for network traffic classification[C]// Proceedings of International Conference on Network and System Security. Cham：Springer International Publishing，2014：138-151.

[11] ZHOU Y M，LIU F Z，WANG Y. IPSec VPN Encrypted Traffic

Identification Based on Hybrid Method[J]. Computer Science, 2021, 48(4): 295-302.
[12] WANG A, GE J, SHANG N, et al. Practical cases of side-channel analysis[J]. Journal of Cryptologic Research, 2018, 5(4): 383-398.
[13] KOCHER P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]// Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology. 1996: 104-113.
[14] KOCHER P C, JAFFE J, JUN B. Differential power analysis [C]// Advances in Cryptology—CRYPTO'99. 1999: 388-397.
[15] GANDOLFI K, MOURTEL C, OLIVIER F. Electromagnetic analysis: Concrete results[C]// Cryptographic Hardware and Embedded Systems(CHES 2001). 2001: 251-261.
[16] TAYLOR V F, SPOLAOR R, CONTI M, et al. Appscanner: Automatic fingerprinting of smartphone apps from encrypted network traffic[C]// 2016 IEEE European Symposium on Security and Privacy(EuroS&P). IEEE, 2016: 439-454.
[17] IETF. Security Architecture for the Internet Protocol [EB/OL]. [2023-02-10]. https://www.ietf.org.
[18] IETF. Requirements for Internet Hosts-Communication Layers [EB/OL]. [2023-02-10]. https://www.ietf.org/.
[19] SHANNON C E. A mathematical theory of communication[J]. The Bell System Technical Journal, 1948, 27(3): 379-423.
[20] DRAPER-GIL G, LASHKARI A H, MAMUN M S I, et al. Characterization of encrypted and vpn traffic using time-related [C]// Proceedings of the 2nd International Conference on Information Systems Security and Privacy(ICISSP). 2016: 407-414.
[21] DAI J, CHEN Y, CHEN Y, et al. An analysis of Network Traffic Identification based on Decision Tree[C]// 2021 International Conference on Artificial Intelligence and Electromechanical Automation(AIEA). IEEE, 2021: 308-311.

SUN Yunxiao, born in 1989, Ph.D. His main research interests include network security communication protocol and so on.



WANG Bailing, born in 1978, Ph.D, professor, Ph.D supervisor, is a member of China Computer Federation. His main research interests include industrial Internet security, information security and financial security.

(责任编辑:何杨)