

基于流谱理论的 SSL/TLS 协议攻击检测方法

郭世泽^{1,2,3}, 张帆^{1,2,3,4}, 宋卓学^{1,2,3,5}, 赵子鸣^{1,2,3}, 赵新杰^{1,2,3}, 王小娟⁶, 罗向阳⁷

(1. 浙江大学计算机科学与技术学院, 浙江 杭州 310027;

2. 浙江大学网络空间安全学院, 浙江 杭州 310027;

3. 浙江大学控制科学与工程学院, 浙江 杭州 310027;

4. 浙江省区块链与网络空间治理重点实验室, 浙江 杭州 310027;

5. 移动终端安全浙江省工程实验室, 浙江 杭州 310027;

6. 北京邮电大学电子工程学院, 北京 100876;

7. 信息工程大学河南省网络空间态势感知重点实验室, 河南 郑州 450001)

摘要: 网络攻击检测在网络安全中扮演着重要角色。网络攻击检测的对象主要为僵尸网络、SQL 注入等攻击行为。随着安全套接层/安全传输层 (SSL/TLS) 加密协议的广泛使用, 针对 SSL/TLS 协议本身发起的 SSL/TLS 攻击日益增多, 因此通过搭建网络流采集环境, 构建了包含 4 种 SSL/TLS 攻击网络流与正常网络流的网络流数据集。针对当前网络攻击流检测的可观测性有限、网络流原始时空域分离性有限等问题, 提出流谱理论, 将网络空间中的威胁行为通过“势变”过程从原始时空域空间映射到变换域空间, 具象为“势变谱”, 形成可分离、可观测的特征表示集合, 实现对网络流的高效分析。流谱理论在实际网络空间威胁行为检测中的应用关键是在给定变换算子的情况下, 针对特定威胁网络流找到势变基底矩阵。由于 SSL/TLS 协议在握手阶段存在着强时序关系与状态转移过程, 同时部分 SSL/TLS 攻击间存在相似性, 因此对于 SSL/TLS 攻击的检测不仅需要考虑到时序上下文信息, 还需要考虑到 SSL/TLS 网络流的高分离度的表示。基于流谱理论, 采用威胁模板思想提取势变基底矩阵, 使用基于长短时记忆单元的势变基底映射, 将 SSL/TLS 攻击网络流映射到流谱域空间。在自建 SSL/TLS 攻击网络流数据集上, 通过分类性能对比、势变谱降维可视化、威胁行为特征权重评估、威胁行为谱系划分评估、势变基底矩阵热力图可视化等手段, 验证了流谱理论的有效性。

关键词: 安全套接层/安全传输层攻击; 网络流检测; 流谱理论; 长短时记忆

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022004

收稿日期: 2022-01-12; 修回日期: 2022-02-08

通信作者: 张帆, fanzhang@zju.edu.cn

基金项目: 国家重点研发计划 (2020AAA0107700); 国家自然科学基金 (62072398, U1804263, 62172435); 信息系统安全技术重点实验室基金; 浙江省重点研发计划 (2021C01116); 浙江省引进培育领军型创新创业团队 (2018R01005); 网络空间国际治理研究基地; 中原科技创新领军人才计划 (214200510019)

Foundation Items: The National Key R&D Program of China (2020AAA0107700), The National Natural Science Foundation of China (62072398, U1804263, 62172435), National Key Laboratory of Science and Technology on Information System Security, Zhejiang Key R&D Program (2021C01116), Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang (2018R01005), Research Institute of Cyberspace Governance in Zhejiang University, Zhongyuan Science and Technology Innovation Leading Talent Project (214200510019)

引用格式: 郭世泽, 张帆, 宋卓学, 等. 基于流谱理论的 SSL/TLS 协议攻击检测方法[J]. 网络与信息安全学报, 2022, 8(1): 30-40.

Citation Format: GUO S Z, ZHANG F, SONG Z X, et al. Detection of SSL/TLS protocol attacks based on flow spectrum theory[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 30-40.

Detection of SSL/TLS protocol attacks based on flow spectrum theory

GUO Shize^{1,2,3}, ZHANG Fan^{1,2,3,4}, SONG Zhuoxue^{1,2,3,5}, ZHAO Ziming^{1,2,3},
ZHAO Xinjie^{1,2,3}, WANG Xiaojuan⁶, LUO Xiangyang⁷

1. College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China

2. School of Cyber Science and Technology, Zhejiang University, Hangzhou 310027, China

3. College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China

4. Zhejiang Key Laboratory of Blockchain and Cyberspace Governance, Hangzhou 310027, China

5. Engineering Laboratory of Mobile Security of Zhejiang Province, Hangzhou 310027, China

6. School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

7. Information Engineering University, Key Laboratory of Cyberspace Situation Awareness of Henan Province, Zhengzhou 450001, China

Abstract: Network attack detection plays a vital role in network security. Existing detection approaches focus on typical attack behaviors, such as Botnets and SQL injection. The widespread use of the SSL/TLS encryption protocol arises some emerging attack strategies against the SSL/TLS protocol. With the network traffic collection environment that built upon the implements of popular SSL/TLS attacks, a network traffic dataset including four SSL/TLS attacks, as well as benign flows was controlled. Considering the problems that limited observability of existing detection and limited separation of the original-flow spatiotemporal domains, a flow spectrum theory was proposed to map the threat behavior in the cyberspace from the original spatiotemporal domain to the transformed domain through the process of “potential change” and obtain the “potential variation spectrum”. The flow spectrum theory is based on a set of separable and observable feature representations to achieve efficient analysis of network flows. The key to the application of flow spectrum theory in actual cyberspace threat behavior detection is to find the potential basis matrix for a specific threat network flow under the condition of a given transformation operator. Since the SSL/TLS protocol has a strong timing relationship and state transition process in the handshake phase, and there are similarities between some SSL/TLS attacks, the detection of SSL/TLS attacks not only needs to consider timing context information, but also needs to consider the high-separation representation of TLS network flows. Based on the flow spectrum theory, the threat template idea was used to extract the potential basis matrix, and the potential basis mapping based on the long-short-term memory unit was used to map the SSL/TLS attack network flow to the flow spectrum domain space. On the self-built SSL/TLS attack network flow data set, the validity of the flow spectrum theory is verified by means of classification performance comparison, potential variation spectrum dimensionality reduction visualization, threat behavior feature weight evaluation, threat behavior spectrum division assessment, and potential variation base matrix heatmap visualization.

Keywords: SSL/TLS attacks, network traffic detection, flow spectrum theory, long short-term memory

0 引言

当今互联网中 90% 以上的网络流数据已采用安全套接层/安全传输层 (SSL/TLS) 协议加密^[1]。与此同时, 针对 SSL/TLS 协议的攻击行为层出不穷^[2], 一些典型的攻击会造成受害者个人隐私的泄露。SSL/TLS 攻击检测的过程以网络流数据为输入, 通过网络流检测相关方法对 SSL/TLS 攻击行为进行识别, 并将其报告给网络管理人员。

当前对于攻击行为的网络流检测主要聚焦于典型的攻击策略, 如 SQL 注入、僵尸网络, 对 SSL/TLS 攻击的关注较少。然而, 在过去的几年, 发生了许多针对 SSL/TLS 的攻击, 如 POODLE 攻击、BREACH 攻击, 并造成了重大影响^[2]。因此, 本文重点关注 SSL/TLS 攻击流的检测。

随着加密网络流在互联网占比的不断提高, 传统的基于端口号^[3]、基于负载^[4]的网络流检测方法已不再适用, 基于机器学习和深度学习的网络

流检测方法已成为网络流检测的主流方法^[5]。然而, 基于机器学习和深度学习的网络流检测方法存在一定的问题。一方面, 基于机器学习和深度学习的网络流检测方法更多的是一种黑盒模型, 缺乏对检测分析结果的可观测能力。另一方面, 基于机器学习和深度学习的网络流检测方法主要在网络流原始时空域空间中进行分析, 在原始时空域空间网络流有限的分离性, 会导致训练的模型存在一定的瓶颈。

本文针对上述问题, 提出流谱理论, 通过流谱理论, 实现对网络攻击流的高效分析。本文的主要贡献有以下几点:

- 1) 通过搭建 SSL/TLS 攻击流采集环境, 构建了包含 4 种典型 SSL/TLS 攻击流的数据集;
- 2) 提出了流谱理论, 通过对复杂网络流进行变换映射, 达成可分离、可观测的网络流检测, 实现对网络攻击流的高效分析;

- 3) 在 SSL/TLS 攻击流上对流谱理论的有效性进行验证, 提供了网络流检测分析的新视角。

本文首先对 SSL/TLS 协议攻击与网络流检测相关工作进行介绍, 之后阐述流谱理论以及基于流谱理论的 SSL/TLS 攻击检测方法, 最后通过实验对方法的可分离性、可观测性进行评估。

1 相关工作

1.1 SSL/TLS 攻击

SSL/TLS 协议^[6-7]位于传输层与应用层之间, 对应用层数据进行加密, 保障数据传输的机密性与完整性。SSL/TLS 协议主要由握手协议与记录协议组成, 其中握手协议负责在会话初始阶段完成通信双方的认证与密钥交换, 记录协议负责对数据进行加密。针对 SSL/TLS 的攻击往往发生在握手阶段, 因此本文主要对握手阶段的网络流进行检测。

SSL/TLS 攻击指的是攻击者通过利用协议本身的设计漏洞、协议的实现漏洞或证书漏洞, 达到窃取受害者隐私数据的目的。SSL/TLS 攻击种类繁多, 本文选取了 4 种典型的 SSL/TLS 攻击作为研究对象, 分别是 POODLE (padding oracle on downgraded legacy encryption) 攻击^[8]、BREACH (browser reconnaissance and exfiltration via adap-

tive compression of hypertext) 攻击^[9]、RC4NOMORE 攻击^[10]与 THC-SSL-DoS 攻击。POODLE 攻击通过利用 SSL 3.0 中 CBC 加密模式的漏洞达到攻击目的。尽管 SSL 3.0 已经不被推荐使用, 但许多客户端与服务器保留了降级选项, 从而被攻击者利用。BREACH 攻击是一种针对 HTTPS 压缩的侧信道攻击。攻击者利用 HTTPS 压缩算法 DEFLATE 产生的压缩数据模式, 可以猜测出用户数据。RC4NOMORE 攻击利用密钥流中的统计偏差信息, 通过产生大量的请求并通过最大似然估计法得到用户会话数据。THC-SSL-DoS 攻击利用 SSL/TLS 握手协商阶段密钥计算验证过程, 产生大量的重协商报文, 要求服务器不断进行密钥计算验证, 从而消耗服务器的资源。

1.2 SSL/TLS 网络流检测相关工作

SSL/TLS 加密网络流的检测工作主要侧重于识别 SSL/TLS 协议加密传输的网络流类型, 包括加密应用网络流识别与加密恶意网络流识别。在加密应用网络流识别方面, Korczyński 等^[11]应用一阶马尔可夫链对 SSL/TLS 加密应用网络流构建指纹, 从而对网络流进行识别分类。Shen 等^[12]通过使用二阶马尔可夫链进一步提高了加密应用网络流指纹的可靠性与网络流识别分类的准确性。Liu 等^[13]提出了一种端到端的网络架构 FS-Net, 在加密应用网络流分类上, 该架构的精确率达到了 99.14%。在加密恶意网络流识别方面, Radford 等^[14]将循环神经网络应用于入侵网络流检测, 采用 LSTM 捕捉网络流在时序上的上下文信息。Mirsky 等^[15]提出了 Kitsune, 通过集成自动编码器提取正常与异常网络流模式, 实现加密恶意网络流的热插拔识别。Fu 等^[16]提出了一种实时鲁棒的加密恶意网络流检测框架 Whisper, 通过使用傅里叶变换提取加密恶意网络流的频域特征, 使网络流检测不易受到躲避攻击, 更具有鲁棒性。

1.3 公开问题

SSL/TLS 加密网络流的检测工作主要侧重于识别 SSL/TLS 协议加密传输的网络流类型, 包括加密应用网络流识别与加密恶意网络流识别, 缺乏对于 SSL/TLS 协议攻击网络流的检测识别, SSL/TLS 协议攻击网络流的检测识别是 SSL/TLS

加密网络流检测的公开问题之一。同时, SSL/TLS 加密网络流主要基于机器学习和深度学习方法在网络流原始时空域空间中的分析。因此, 寻找可观测性强、可分离度高的网络流变换域, 在变换域上对网络流作进一步分析, 是 SSL/TLS 加密网络流检测的公开问题之一。

2 流谱理论

光学频谱(光谱)、声音频谱(声谱)等都是对信号在频域中的观测表达, 是分析复杂信号的一种方法, 将复杂的信号表征成分离度更高、观测性更强的形式。在实际网络空间中, 原始网络流由一系列数据包组成, 往往呈现出复杂性、耦合性, 且由于攻击方式日益复杂多样, 难以从原始网络流中形成对威胁行为全面、系统、深刻的认识。基于机器学习和深度学习的网络流检测方法主要在网络流原始时空域空间中进行分析。流量数据在时空域分布空间的分离性和表征性, 会决定模型检测的上限。因此, 本文借鉴光谱、声谱的思想, 提出流谱理论。

流谱理论通过将网络空间中的复杂原始网络流按某种时域到某变换域的映射方法, 形成可分离、可观测的特征表示集合, 实现对网络流的高效分析。具体到网络空间中的威胁行为映射, 则具象为“势变谱”, 威胁行为从原始时空域空间映射到变换域空间的过程叫作“势变”。

流谱理论对原始威胁行为网络流的变换映射过程如图 1 所示。定义网络流的原域空间为 F , 流谱域空间 S 为原域空间在某种映射下的变换域。考虑原域空间下 t 时刻的网络流为 $f(t)$, 根据五元组(源 IP, 目的 IP, 源端口, 目的端口, 传输层协议)对网络流进行切分, 同一五元组的

双向网络流组成一个会话网络流。对会话网络流进行原域空间下的行为特征提取得到原域下的行为特征矩阵 F , 给定变换算子 $\odot$ 与流谱势变基底矩阵 W , 则流谱域空间下的势变谱矩阵 S 为

$$S = W \odot F \quad (1)$$

流谱理论在实际网络空间威胁行为检测中的应用关键是在给定变换算子的情况下, 针对特定威胁网络流找到势变基底矩阵 W 。

3 基于流谱理论的 SSL/TLS 攻击检测

SSL/TLS 协议在握手阶段存在强时序关系与状态转移过程, 同时部分 SSL/TLS 攻击间存在相似性, 因此对于 SSL/TLS 攻击的检测不仅需要考虑时序上下文信息, 还需要考虑对 SSL/TLS 网络流的高分离度的表示。本文基于流谱理论, 采用威胁模板思想提取势变基底, 使用基于长短时记忆单元的势变基底映射将 SSL/TLS 攻击网络流映射到流谱域空间得到可观测、可分离的势变谱, 实现对 SSL/TLS 攻击网络流的高效分析。

3.1 基于长短时记忆单元的网络流变换

本文采用长短时记忆(LSTM, long short-term memory)单元^[17]作为变换算子实现网络流变换。长短期记忆网络是一种特殊的循环神经网络, 能够学习长期时序依赖关系。由于其特殊的推理结构, 现在被广泛应用于处理时序数据。

LSTM 单元的结构如图 2 所示, 整体由遗忘门(蓝色方块)、更新门(红色方块)和输出门(紫色方块)组成。

t 时刻遗忘门的输出为

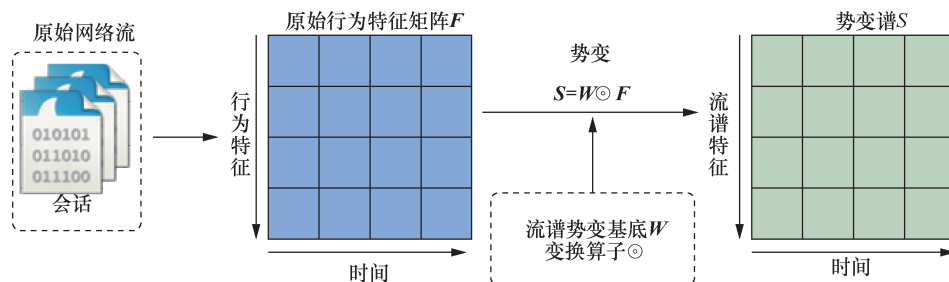


图 1 流谱理论对网络流的变换过程

Figure 1 The transformation process of flow spectrum theory on network flow

$$\Gamma_f = \sigma(W_f[a_{t-1}, L_t] + b_f) \quad (2)$$

其中, W_f 和 b_f 为训练变量, $\sigma(x) = \frac{1}{1+e^{-x}}$ 为 sigmoid 函数。

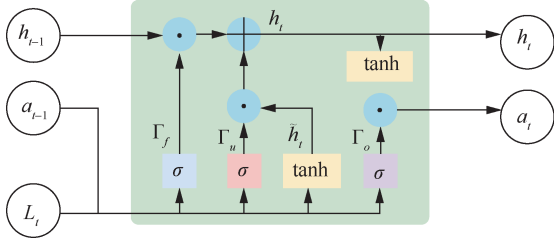


图 2 LSTM 单元的结构
Figure 2 Architecture of an LSTM cell

t 时刻更新门的输出为

$$\Gamma_u = \sigma(W_u[a_{t-1}, L_t] + b_u) \quad (3)$$

其中, W_u 和 b_u 为需要学习的变量。

t 时刻输出门的输出为

$$\Gamma_o = \sigma(W_o[a_{t-1}, L_t] + b_o) \quad (4)$$

其中, W_o 和 b_o 为训练变量。

t 时刻的隐藏状态可以按式(5)更新

$$h_t = \Gamma_u \odot \tilde{h}_t + \Gamma_f \odot h_{t-1} \quad (5)$$

$\tilde{h}_t$ 可由式(6)计算。

$$\tilde{h}_t = \tanh(W_c[a_{t-1}, L_t] + b_c) \quad (6)$$

其中, W_c 和 b_c 为训练变量。

长时间记忆单元 t 时刻的输出为

$$a_t = \Gamma_o \odot \tanh(h_t) \quad (7)$$

从式(2)~式(7), 可以对 LSTM 单元的隐藏状态 h_t 进行更新, 并得到时间步 t 上的 LSTM 输出。对原域特征矩阵 F 中每个时间步的特征向量进行上述 LSTM 变换, 则可得到流谱域下势变谱矩阵 S 对应时间步的特征向量。

3.2 基于威胁模板的势变基底提取

在实际网络空间中, 威胁行为繁多复杂。但对于每种威胁行为, 其背后存在固定的威胁行为模式, 称之为威胁行为的模板。如果对于威胁行为, 能够在变换域中找到其模板, 那么针对其攻击过程的网络流量, 通过流谱势变进行映射, 便可以在变换域中计算其与模板的距离, 从而判断并识别攻击。性质良好的势变基底应该能使同一

类威胁行为网络流在变换后离威胁模板近, 不同类威胁行为网络流在变换后离威胁模板远。

本文提出一种基于威胁模板的势变基底提取算法, 其流程如图 3 所示。

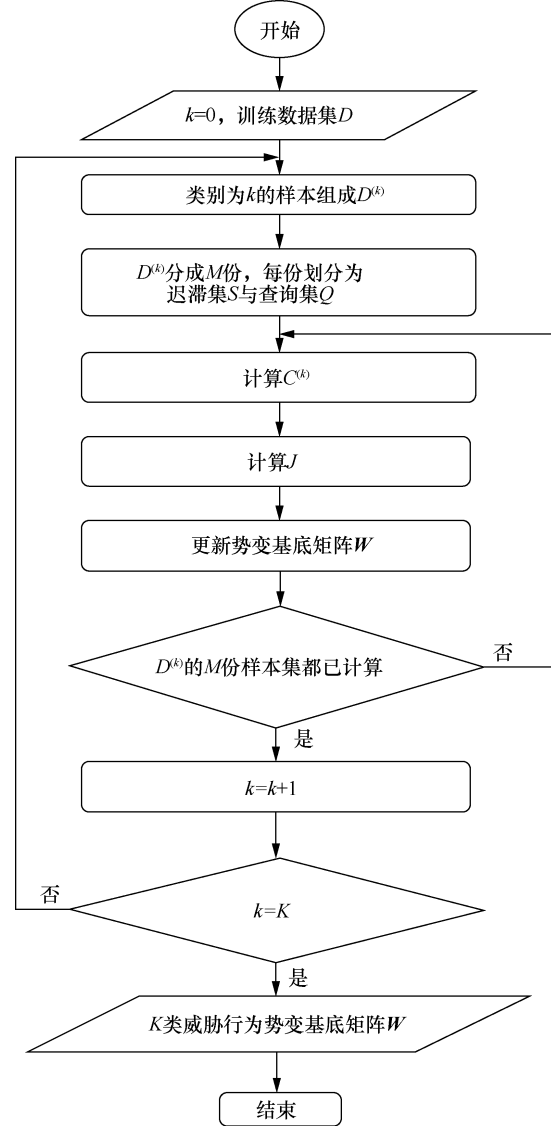


图 3 基于威胁模板的势变基底提取算法流程
Figure 3 Algorithm flow of behavior base extraction based on threat template

具体算法步骤如下。

算法 1 基于威胁模板的势变基底提取算法

输入 含 K 类威胁行为的训练样本数据集 D

输出 K 类威胁行为独立的势变基底矩阵 W

1) 初始 $k = 0$ 。

2) 从训练数据集 D 中选出类别为 k 的训练样本组成集合 $D^{(k)}$ 。

3) 将 $D^{(k)}$ 分成 M 份, 每一份选 N_s 个样本组成支持集 S , 剩余 N_Q 个样本组成查询集 Q 。

4) 对于支持集 S 中的样本 (x_i, y_i) , 计算 $C^{(k)} \leftarrow \frac{1}{N_s} \sum_{(x_i, y_i) \in S} W \odot x_i$ 。

5) 初始 $J=0$, 对于查询集 Q 中的样本 (x_i, y_i) , 计算 $J \leftarrow J + \frac{1}{N_Q} d(W \odot x_i, C^{(k)})$ 。

6) 根据 J , 利用梯度下降法更新势变基底矩阵 W 。

7) 对于 $D^{(k)}$ 的每一份样本集执行步骤 3)~6)。

8) $k = k + 1$, 重复执行步骤 2)~7), 直到 $k = K$ 。

其中, d 为变换后的网络流特征矩阵与模板间的距离度量函数。由于欧几里得距离具备更好的鲁棒性^[18], 因此本文选用欧几里得距离作为距离度量函数 d 。

$$d(x_1, x_2) = \sqrt{\sum_{i=1}^P (x_{1i} - x_{2i})^2} \quad (8)$$

以上算法完成后, 可以得到每种威胁行为的势变基底, 从而可以对威胁行为网络流进行势变映射, 转化为流谱域下的势变谱, 实现对网络流可分离、可观测的高效分析。

3.3 基于距离计算的威胁谱系分类

在得到每种威胁行为的势变基底与模板后, 可以对威胁进行分类, 实现威胁行为网络流的可分离。

定义 $S^{(i)} = [s_1^{(i)}, s_2^{(i)}, \dots, s_T^{(i)}]$, 其中 $s_t^{(i)}$, $1 \leq t \leq T$ 为第 i 个势变谱在 t 时刻的列向量。定义 $C^{(i)} = [c_1^{(i)}, c_2^{(i)}, \dots, c_T^{(i)}]$, 其中 $c_t^{(i)}$, $1 \leq t \leq T$ 为 t 时刻威胁 i 的模板向量。通过计算威胁行为势变谱与各威胁模板之间的距离, 选取距离最小的威胁模板对应的类型作为威胁类型, 即

$$\hat{y} = \arg \min_i d(S^{(i)}, C^{(i)}) \quad (9)$$

在得到各威胁模板后, 还可以对威胁行为间的距离进行计算。威胁行为 i, j 之间的距离定义为威胁模板之间的距离:

$$d_{ij} = d(C^{(i)}, C^{(j)}) \quad (10)$$

计算两两威胁之间的距离, 可以得到威胁谱系图的邻接矩阵 D , 从而可以绘制威胁谱系图。

根据势变谱矩阵 $S^{(i)}$ 与威胁模板 $C^{(i)}$, 可以对各威胁行为的特征重要性进行排序。

针对威胁行为 i , 计算势变谱第 k 个特征输出与威胁模板 i 的第 k 个分量的距离, 并与其他威胁模板的第 k 个分量的距离相比, 差值越大, 则该分量对最终分类结果的贡献越大, 该特征越重要。这是由于分类所依赖的势变谱与威胁模板的距离是所有分量距离的求和, 因此如果某分量与各威胁模板的对应分量在距离上有显著区分度, 则该特征对威胁行为的分类有重要意义。具体地, 威胁行为 i 第 k 个特征的重要性 $FI(i, k)$ 由式(11)计算。

$$FI(i, k) = \frac{\sum_j \sum_t (d(a_{k,t}^{(j)}, c_{k,t}^{(j)}) - d(a_{k,t}^{(i)}, c_{k,t}^{(i)}))}{\sum_k \sum_j \sum_t (d(a_{k,t}^{(j)}, c_{k,t}^{(j)}) - d(a_{k,t}^{(i)}, c_{k,t}^{(i)}))} \quad (11)$$

其中, $a_{k,t}^{(i)}$ 为势变谱 i 第 k 个分量在 t 时刻的值, $c_{k,t}^{(i)}$ 为威胁模板 i 第 k 个分量在 t 时刻的值。

4 实验评估

4.1 实验准备

本文针对目前缺乏公共 SSL/TLS 攻击网络流数据集的问题, 通过搭建 SSL/TLS 攻击网络流采集环境, 构建了包含 4 种典型 SSL/TLS 攻击网络流与正常网络流的数据集。4 种典型攻击包括 POODLE 攻击、BREACH 攻击、RC4NOMORE 攻击和 THC-SSL-DoS 攻击。图 4 是 SSL/TLS 攻击的整体示意, 包含 3 部分: 存在漏洞的服务器、受害客户端和中间人代理。



图 4 SSL/TLS 攻击整体示意
Figure 4 Schematic diagram of the attack scenario

对于 POODLE 攻击、BREACH 攻击与 RC4NOMORE 攻击, 攻击过程大致如下。

步骤 1 攻击者建立一个中间人代理, 劫持客户端与服务器间的通信。

步骤 2 攻击者将恶意代码注入客户端并通过跨站脚本攻击等手段运行恶意代码。

步骤 3 攻击者通过分析中间人代理捕获的网络流数据, 从密文中恢复明文。

对于 THC-SSL-DoS 攻击, 不需要劫持客户

端与服务器间的通信,只需要在客户端上运行攻击工具即可对服务器发起攻击。

对于 BREACH 攻击,本文使用 rupure (一种发起 BREACH 攻击与其他基于压缩算法攻击的框架)发起攻击。对于 THC-SSL-DoS 攻击,本文使用 Kali Linux 上的 THC-SSL-DoS 攻击工具发起攻击。对于 POODLE 攻击与 RC4NOMORE 攻击,没有现有工具可以使用,本文使用 JavaScript 脚本与 shell 脚本实现了这两种攻击。

除了攻击网络流,本文通过使用自动化框架 selenium^[20]模仿正常用户行为采集了正常网络流。具体过程为解析页面上的所有链接,每间隔一段随机时间,随机选取某个链接进行访问。

实验在本地搭建配置了含有 SSL/TLS 漏洞的服务器,通过编写脚本、使用现有工具发起攻击并捕获网络流。本文使用 tshark^[21]工具捕获网络流,生成 pcap 格式数据包捕获文件,每个 pcap 是一个样本,包含一次客户端与服务器间的完整会话过程。

本文采集的 SSL/TLS 攻击数据集样本数如表 1 所示。

表 1 采集的 SSL/TLS 攻击数据集样本数
Table 1 Number of samples in collected dataset of SSL/TLS attacks

网络流类型	采集样本数
POODLE 攻击	10 738
BREACH 攻击	10 726
RC4NOMORE 攻击	11 083
THC-SSL-DoS 攻击	10 049
正常网络流	25 797

实验采用的原始行为特征为数据包的协议字段,具体如表 2 所示。

为了避免实验偶然性,本文采用十折交叉验证方法,将数据集分成 10 份,轮流选取其中 9 份作为训练数据,剩余 1 份作为测试数据,最终评估时取平均值作为结果。

实验使用的计算机配置为 Intel Xeon CPU E5-2678 v3 @ 2.50 GHz, 64 GBRAM, 安装有 Ubuntu 18.04 LTS。

实验使用的时间序列长度 T 为 32,学习率为 0.001。代码采用 PyTorch^[22]1.10 与 scikit-learn^[23]1.0.1 来编写。

表 2 原始行为特征使用的协议字段
Table 2 Protocol fields used by the original behavior feature

SSL/TLS 协议报文	协议字段
ClientHello	
ServerHello	内容类型
Certificate	
ServerHelloDone	
ClientKeyExchange	长度
HandshakeMessage	
ApplicationData	版本
ClientHello	
ServerHello	
Certificate	握手类型
ServerHelloDone	
ClientKeyExchange	
ClientHello	密码套件长度
ServerHello	压缩类型
Certificate	证书长度
	证书个数

4.2 评估指标

实验的评估指标主要为分类指标,分类指标中的相关参数定义如表 3 所示。由于本文的威胁行为分类为多分类问题,因此在具体关注某一类的分类指标时,该类即为正例,其他类则为负例。总体的分类指标则定义为各类分类指标的样本数加权平均。

表 3 分类指标相关参数定义
Table 3 Definition of parameters of classification metrics

指标参数	参数含义
TP (true positive)	被正确预测为正例的样本数
TN (true negative)	被正确预测为负例的样本数
FP (false positive)	被错误预测为正例的样本数
FN (false negative)	被错误预测为负例的样本数

根据表 3,定义准确率 (Accuracy) 为

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (12)$$

精确率 (Precision) 和召回率 (Recall) 定义为

表 4 原始行为特征矩阵与势变谱的分类结果对比

Table 4 Comparison of classification results between original behavior feature matrix and potential spectrum

网络流类型	原始 LSTM				本文方法			
	准确率	精确率	召回率	F1 值	准确率	精确率	召回率	F1 值
POODLE	87.45%	85.22%	87.45%	86.32%	97.65%	97.32%	97.65%	97.48%
BREACH	89.98%	85.68%	89.98%	87.78%	97.11%	96.72%	97.11%	96.91%
RC4NOMORE	86.44%	90.84%	86.44%	88.59%	92.74%	98.58%	92.74%	95.57%
THC-SSL-DoS	92.23%	88.35%	92.23%	90.25%	98.74%	97.56%	98.54%	98.15%
正常网络流	92.24%	96.78%	92.24%	94.46%	99.25%	99.30%	99.25%	99.27%
总体	90.19%	91.02%	90.19%	90.56%	97.72%	98.37%	97.72%	98.03%

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (13)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (14)$$

定义精确率和召回率的调和平均为 $F1$ 值。

$$F1 \text{ 值} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (15)$$

4.3 威胁可分离性评估

对变换前的原始行为特征矩阵与变换后的势变谱矩阵进行可视化，观察势变基底变换对网络流可分离性的影响。由于原始行为特征矩阵与势变谱矩阵均处于高维空间中，无法直接进行可视化展示，因此使用 t -SNE^[19]降维方法对矩阵进行降维处理，转化到二维平面进行可视化展示，结果如图 5 所示。

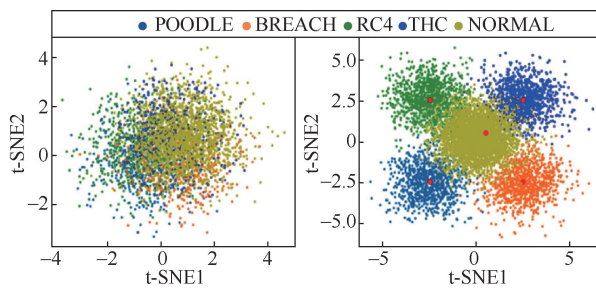


图 5 原始行为特征矩阵（左）与势变谱（右） t -SNE 降维可视化结果
Figure 5 Original behavior feature matrix (left) and potential spectrum (right) t -SNE dimensionality reduction visualization results

从图 5 可以看出，通过流谱势变基底变换后，在原域空间中耦合在一起的网络流被分离开，且聚集在各威胁行为的模板（图中红点）周围。

原始行为特征矩阵与势变谱的分类结果对比

如表 4 所示，表中对比了直接在原始行为特征矩阵上使用 LSTM 进行威胁行为分类与使用势变谱进行威胁行为分类的结果。

从表 4 可以看到，本文提出的流谱理论能够提高网络流分类的准确率、精确率、召回率和 $F1$ 值，相比直接在原始行为特征矩阵上使用 LSTM 进行威胁行为分类，使用势变谱分类在准确率、精确率、召回率和 $F1$ 值上各有 7% 左右的提升。因此，通过利用势变基底将原始行为特征矩阵映射到势变谱，提高了网络流的可分离性，从而能够实现对网络流的高效分析。

4.4 威胁特征权重评估

对于 4 种 SSL/TLS 威胁行为，根据式(11)的特征重要性计算方法，对每一类威胁行为分别计算特征重要性，取每一类行为前 5 重要的特征绘制特征重要性排序图，如图 6 所示。

从图 6 可以看到，4 种 SSL/TLS 威胁行为的特征重要性排序各不相同。例如，对于 THC-SSL-DoS 攻击行为，其前 5 最重要的特征分别为 ClientKeyExchange : Version ; ClientHello : Version ; HandshakeMessage : Version ; ServerHello : Version ; Certificate : Version，说明对 THC-SSL-DoS 威胁行为更关注 ClientKeyExchange、HandshakeMessage 报文特征，这符合 THC-SSL-DoS 攻击行为的模式，其正是利用 SSL/TLS 握手协商阶段密钥计算验证过程，产生大量的重协商报文，要求服务器不断进行密钥计算验证，从而消耗服务器的资源。

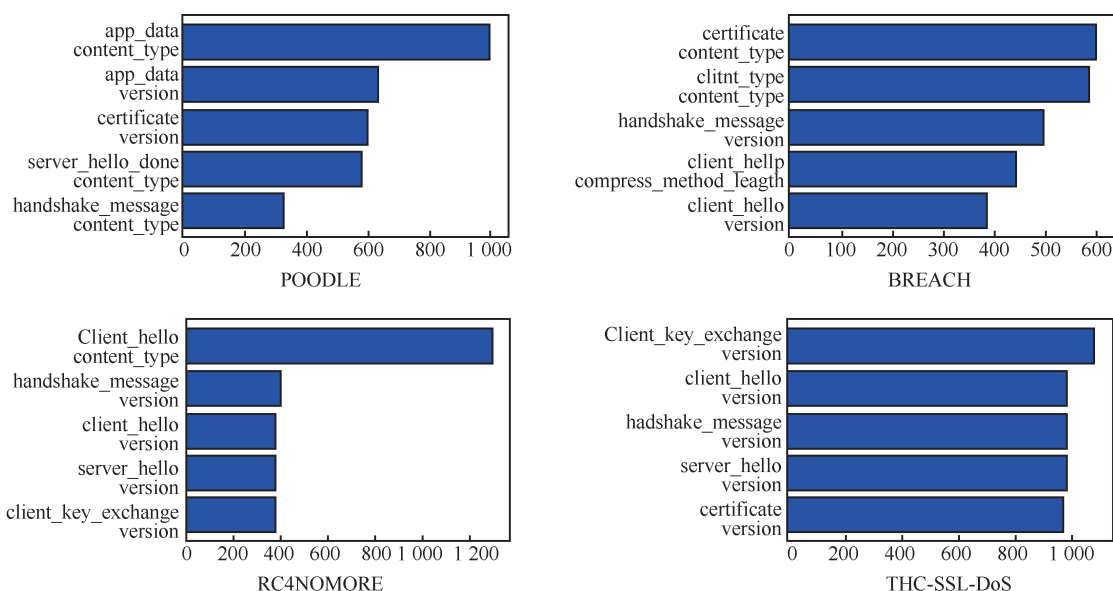


图 6 4 种 SSL/TLS 威胁行为前 5 特征重要性
Figure 6 The importance of the top 5 features of the 4 SSL/TLS attacks

4.5 威胁谱系划分评估

对于 4 种 SSL/TLS 威胁行为与正常行为网络流，两两计算网络流模板之间的距离，可以得到威胁谱系图的邻接矩阵 D ，并绘制威胁谱系图，如图 7 所示。

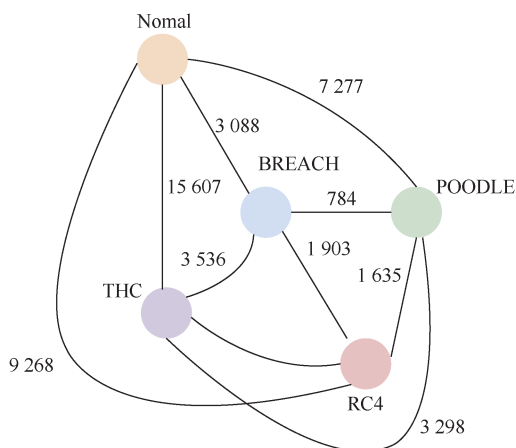


图 7 4 种 SSL/TLS 攻击行为与正常网络流间的谱系图
Figure 7 Genealogy diagram between 4 SSL/TLS attack behaviors and normal traffic

从图 7 可以看到，POODLE 攻击与 BREACH 攻击间的距离较近，这主要因为 POODLE 攻击与 BREACH 攻击都是利用 SSL/TLS 会话用户数据加密、压缩中的漏洞达到窃取用户会话数据的目的。

对 4 种 SSL/TLS 威胁行为的势变基底矩阵进

行可视化展示，其结果如图 8 所示。

从图 8 可以看到，不同威胁行为其势变基底矩阵各不相同。图中颜色较深区域说明该处的绝对值较大，对输入的敏感程度更强，在一定程度上反映了不同威胁的行为特征。

5 结束语

相比于常见的攻击行为网络流检测，本文重点关注 SSL/TLS 攻击网络流的检测识别，通过搭建网络流采集环境，构建了包含 4 种 SSL/TLS 攻击网络流与正常网络流的数据集。针对基于机器学习和深度学习的网络流检测方法可观测性有限、原始网络流时空域的分异性有限问题，提出了流谱理论，通过将网络空间中的复杂原始网络流按某种时域到某变换域的映射方法，形成可观测、可分离的特征表示集合，实现对网络流的高效分析。本文以 LSTM 作为变换算子，基于威胁模板的思想提取势变基底变换矩阵，在自建 SSL/TLS 攻击网络流数据集上进行了流谱理论的实验验证，说明了流谱理论具有较好的可观测性与可分离性，为威胁行为网络流分析提供了一种新视角。

参考文献：

- [1] GURUBARAN S. Cisco encrypted traffic analytics white paper [EB].

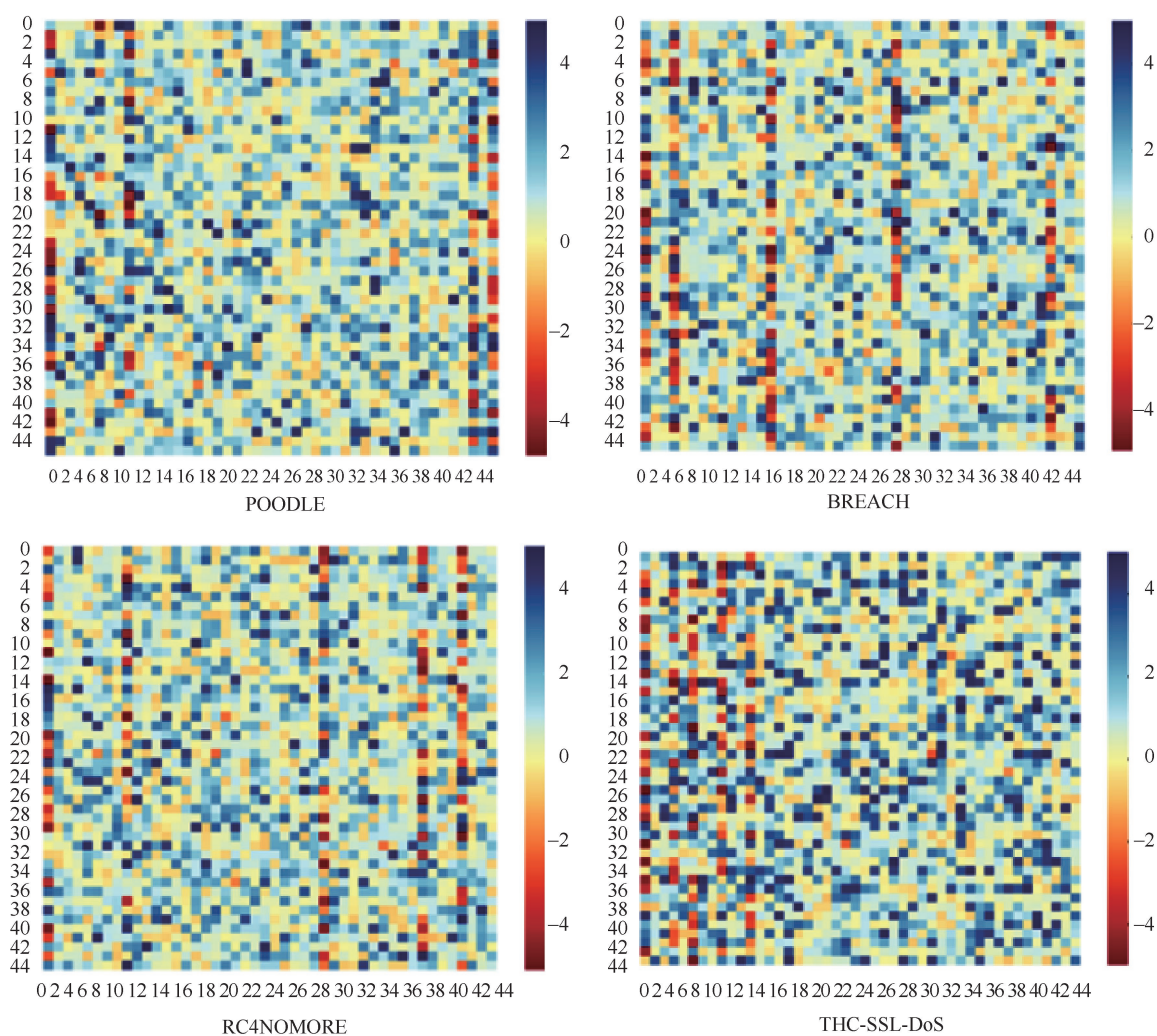


图8 4种SSL/TLS威胁行为势变基底矩阵
Figure 8 The potential base matrix of 4 SSL/TLS attacks

- [2] SHEFFER Y, HOLZ R, SAINT-ANDRE P. Summarizing known attacks on transport layer security (TLS) and datagram TLS (DTLS)[J]. Internet Engineering Task Force Request for Comments, 2015, 7457.
- [3] MCPHERSON J, MA K L, KRYSOSK P, et al. Portvis: a tool for port-based detection of security events[C]//Proceedings of the 2004 ACM workshop on Visualization and Data Mining for Computer Security. 2004: 73-81.
- [4] FINSTERBUSCH M, RICHTER C, ROCHA E, et al. A survey of payload-based traffic classification approaches[J]. IEEE Communications Surveys & Tutorials, 2013, 16(2): 1135-1156.
- [5] CAO Z, XIONG G, ZHAO Y, et al. A survey on encrypted traffic classification[C]//International Conference on Applications and Techniques in Information Security. 2014: 73-81.
- [6] FREIER A, KARLTON P, KOCHER P. The secure sockets layer (SSL) protocol version 3.0[R]. RFC 6101, 2011.
- [7] RESCORLA E, DIERKS T. The transport layer security (TLS) protocol version 1.3[J]. 2018.
- [8] MÖLLER B, DUONG T, KOTOWICZ K. This POODLE bites: exploiting the SSL 3.0 fallback[J]. Security Advisory, 2014, 21: 34-58.
- [9] GLUCK Y, HARRIS N, PRADO A. BREACH: reviving the CRIME attack[J]. Unpublished manuscript, 2013.
- [10] VANHOEF M, PIESENS F. All your biases belong to us: Breaking RC4 in WPA-TKIP and TLS[C]//24th USENIX Security Symposium {USENIX} Security. 2015: 97-112.
- [11] KORCZYŃSKI M, DUDA A. Markov chain fingerprinting to classify encrypted traffic[C]//IEEE INFOCOM 2014-IEEE Conference on Computer Communications. 2014: 781-789.
- [12] SHEN M, WEI M, ZHU L, et al. Classification of encrypted traffic with second-order markov chains and application attribute bigrams[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(8): 1830-1843.
- [13] LIU C, HE L, XIONG G, et al. Fs-net: a flow sequence network for encrypted traffic classification[C]//IEEE INFOCOM 2019-IEEE Conference on Computer Communications. 2019: 1171-1179.
- [14] RADFORD B J, APOLONIO L M, Trias A J, et al. Network traffic anomaly detection using recurrent neural networks[J]. arXiv pre-

print arXiv:1803.10769, 2018.

- [15] MIRSKY Y, DOITSHMAN T, ELOVICI Y, et al. Kitsune: an ensemble of autoencoders for online network intrusion detection[J]. arXiv preprint arXiv:1802.09089, 2018.
- [16] FU C, LI Q, SHEN M, et al. Realtime robust malicious traffic detection via frequency domain analysis[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 3431-3446.
- [17] HOCHREITER S, SCHMIDHUBER J. Long short-term memory[J]. Neural Computation, 1997, 9(8): 1735-1780.
- [18] SNELL J, SWERSKY K, ZEMEL R. Prototypical networks for few-shot learning[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. 2017: 4080-4090.
- [19] VAN DER MAATEN L, HINTON G. Visualizing data using t-SNE[J]. Journal of Machine Learning Research, 2008, 9(11).
- [20] HOLMES A, KELLOGG M. Automating functional tests using selenium[C]//AGILE 2006 (AGILE'06). 2006.
- [21] MERINO B. Instant traffic analysis with Tshark how-to[M]. Packt Publishing Ltd, 2013.
- [22] PASZKE A, GROSS S, MASSA F, et al. Pytorch: an imperative style, high-performance deep learning library[J]. Advances in neural Information Processing Systems, 2019, 32: 8026-8037.
- [23] PEDREGOSA F, VAROQUAUX G, GRAMFORT A, et al. Scikit-learn: machine learning in Python[J]. The Journal of Machine Learning Research, 2011, 12: 2825-2830.

[作者简介]



郭世泽（1969-），男，河北石家庄人，浙江大学教授，主要研究方向为网络空间安全。



张帆（1978-），男，浙江杭州人，浙江大学教授、博士生导师，主要研究方向为网络安全、硬件安全、系统安全。



宋卓学（1998-），男，浙江衢州人，浙江大学硕士生，主要研究方向为网络空间安全。



赵子鸣（1998-），男，河北邢台人，浙江大学博士生，主要研究方向为网络空间安全。



赵新杰（1986-），男，河南开封人，浙江大学高级工程师，主要研究方向为网络与信息安全。



王小娟（1985-），女，河北保定人，北京邮电大学副教授，主要研究方向为计算机网络安全。



罗向阳（1978-），男，湖北钟祥人，信息工程大学教授、博士生导师，主要研究方向为网络与信息安全。