# 一种基于扩展攻击链和循环神经网络的高级持续性威胁检测方法

廖铎烽

（广州市香江中学国际部，广东 广州 511340）

**摘 要** 随着信息系统智能化的发展，高级持续性威胁带来的危害愈加严重。如何对各类传统安全设备产生的海量日志进行关联分析，从而对此新型网络威胁进行有效的检测显得愈加重要。本文在分析高级持续性威胁的原理和特点的基础上，提出了基于扩展攻击链模型结合长短期记忆网络模型对网络行为进行广泛关联的智能威胁检测方法，为检测高级持续性威胁的应用和实践提供了一种新的思路。

**关键词** 高级持续性威胁 入侵检测 网络攻击链 循环神经网络

**中图分类号**：TP31 **文献标识码**：A **文章编号**：1007-0745(2022)01-0010-04

## 1 前言

近年高级可持续威胁（Advanced Persistent Threat，APT）逐渐引起人们的关注。APT 攻击也称为定向攻击，通常是具有高水平专业知识和丰富资源的组织对特定重要对象开展的持续的网络攻击活动，相较于传统的网络攻击模式更加难以防范，造成的危害更加严重[1]。

传统的防御方法，如入侵检测、防火墙等，主要适用于应对模式固定的网络攻击。APT 攻击往往具有“多步骤”和“低姿态”的特点，在一个很长的时间段内，运用钓鱼邮件、系统漏洞、社会工程学等各种手段，绕过边界防护潜伏在系统中。如何有效地检测 APT 攻击过程中相关的异常事件仍然是比较困难的问题。

为了应对这种复杂的网络攻击手段，本文对 APT 攻击原理和防护技术进行研究，提出一种基于网络攻击链模型和循环神经网络的检测方法，在时间和空间上对 APT 攻击链条中相关的网络行为进行关联，提高对 APT 攻击的识别能力。

## 2 相关工作

国内外学者围绕 APT 检测已开展了广泛的研究和实践，其成果主要集中于入侵检测技术方面。入侵检测技术可分为特征检测和异常检测，前者使用基于规则库的入侵检测系统等安全设备对计算机网络中的事件进行分析，与规则相匹配的网络行为则被检测为攻击[2-4]；后者采用统计机器学习的方法，通过收集正常数据训练行为模型，当网络中出现偏离该模型限值的情况时会被认为是网络攻击行为[5-6]。从实际应用情况来看，上述研究成果对于改善 APT 攻击的检测水平起到了重要作用，但是也存在一些问题。一方面，现有的入侵检测系统缺乏对安全威胁特征代码库中尚未签名的未知威胁的实时有效的安全防护能力[7]；另一方面，基于常规机器学习模型的检测方法，对于时间跨度大、攻击行为不明显的 APT 攻击的效果相对有限[8]。

## 3 APT 检测关键技术

### 3.1 经典攻击链模型

APT 攻击行为不仅是直接的破坏行为，其攻击的各阶段是混杂交织的，需要引入更细粒度的模型来指导防御[9]。经典网络攻击链（Cyber Attack Chain，CAC）模型是美国洛克希德 - 马丁公司于 2011 年提出的从攻击者角度描述的一种有针对性的分阶段攻击的网络安全模型。该模型协助安全人员识别潜在攻击每个阶段的可疑活动，如未能在某一步中发现攻击迹象，也可以在后续阶段中找到线索，以期尽早发现并阻止攻击行为，使防御效果最大化。通过 CAC 模型侧写出恶意攻击的逻辑关系，为网络安全事件追踪溯源、关系抽取和攻击预测提供了先决条件。

如图 1 所示，CAC 模型包含 7 个攻击阶段：侦查跟踪通常通过充分利用社会工程学了解目标系统和网络信息；武器构建主要是指制作定向攻击工具，例如带有恶意代码的 PDF 文件或 Office 文件；载荷投递将输送攻击工具到目标系统上，常用的手法包括邮件的附件、网站（挂马）、U 盘等；攻击利用是利用目标系统的应用或操作系统漏洞，在目标系统触发已制作的攻击工具使其运行；安装植入与互联网控制器服务器建立一个命令与控制信道；通信控制是指执行所需要

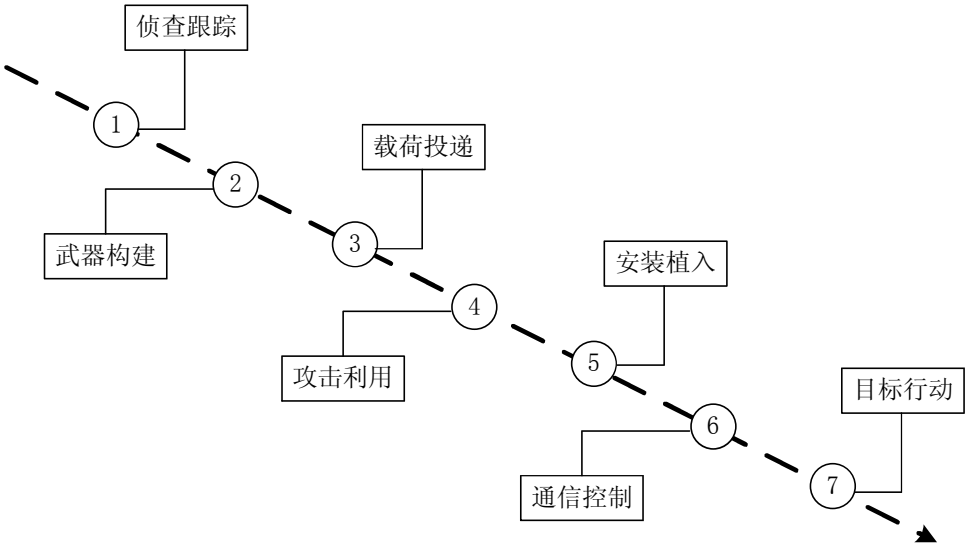


图 1 经典攻击链模型

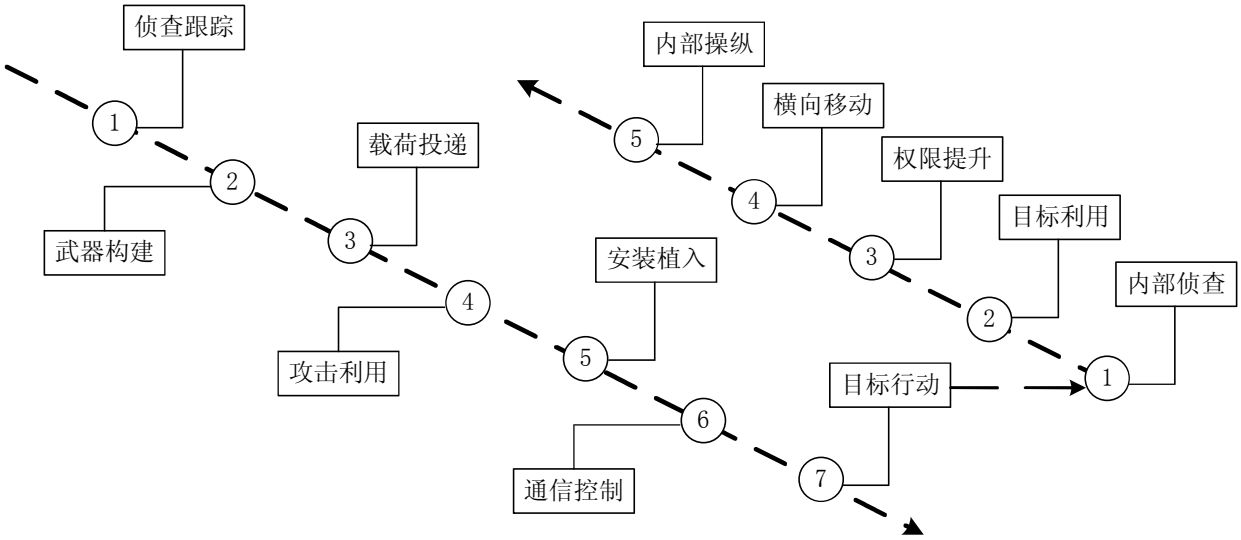


图 2 扩展攻击链模型

的攻击行为，例如偷取信息、篡改信息等；最后目标行动阶段创建攻击据点，并持续潜伏扩大攻击战果。

3.2 循环神经网络

与传统神经网络不同，循环神经网络（Recurrent Neural Network，RNN）内置循环的网络，允许信息持续存在，从而能够对输入时间点前后的事件进行关联。

神经单元 A 接收输入 X 并输出一个值 h，循环允许信息从网络的一个步骤传递到下一个步骤。可以将循环神经网络视为同一网络的在不同时刻的复制，每个复制都将消息传递给下一个时刻，因此理论上来看，循环神经网络能够处理“长期依赖性”问题。

## 4 基于扩展 CAC 及 LSTM 的 APT 检测方法

4.1 扩展攻击链模型

前面所述的经典攻击链模型仅适合建模外部攻击，不适用于内部威胁[10]。在 APT 攻击中，大量攻击行为都是在获得了内部系统权限后进行的，所以需要对经典攻击链模型进行扩展，扩展后的攻击链模型如图 2 所示。相对于经典攻击链，扩展 CAC 细分了内部行为，在达成目标阶段中增加了内部攻击链。内部攻击链是为了获得对目标系统的访问，包含内部侦察、目标利用、

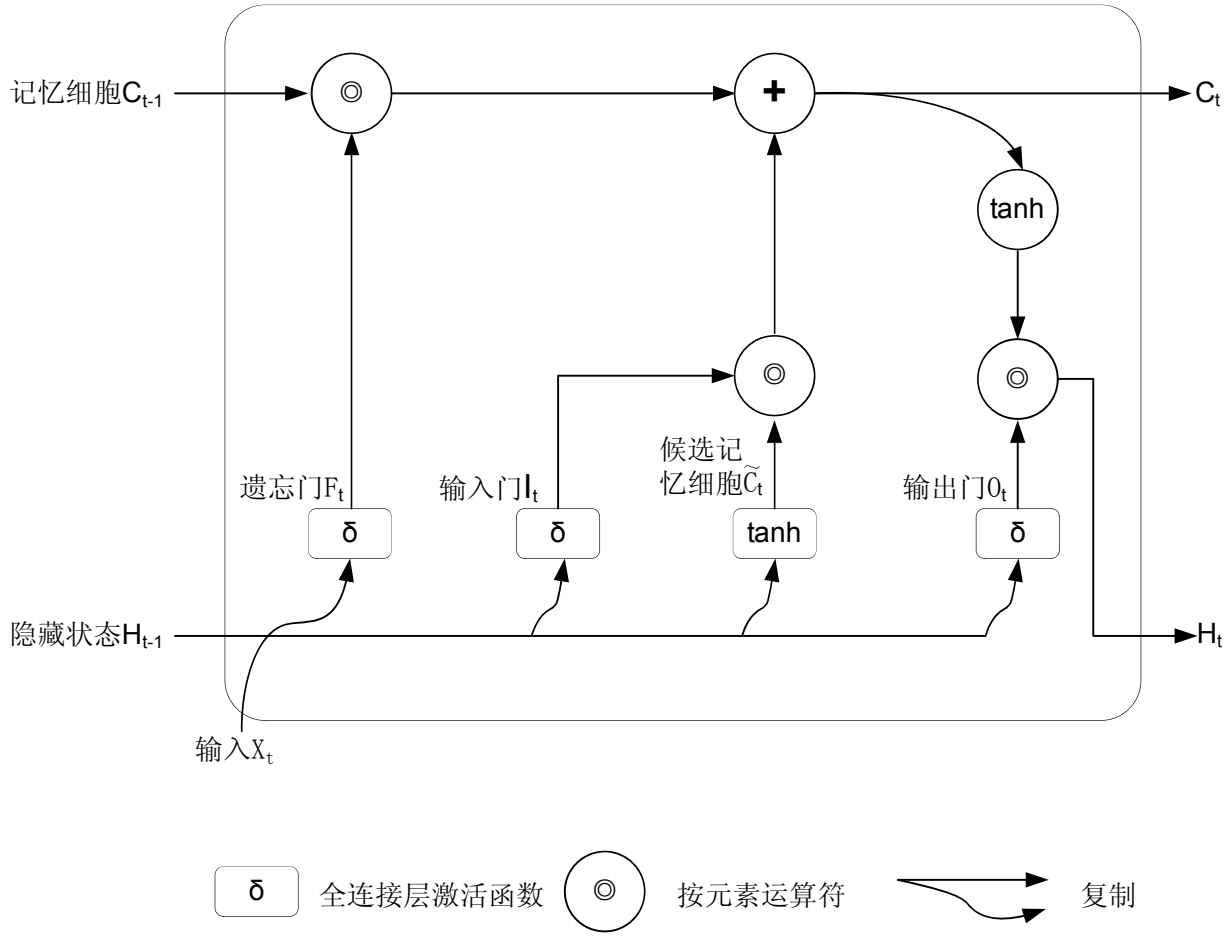


图 3 长短期记忆网络单元

权限提升、横向移动和内部目标操纵。

4.2 长短期记忆网络

在实践中 RNN 模型对于学习“长期依赖”的能力仍然存在不足，并且会有梯度消失的问题存在，因此一种特殊结构的 RNN，即长短期记忆网络（Long-Short Term Memory，LSTM）被提出[11]。LSTM 对 RNN 中的神经单元进行了扩展，引入了三个门，即输入门、遗忘门和输出门，以及记录额外的信息的记忆细胞（见图 3）。

具体来说，令隐藏单元个数为 h，给定时间步为 t，输入为 $X_t$，上一时间步隐藏状态 $H_{t-1}$，时间步 t 的输入门 $I_t$、遗忘门 $F_t$ 和输出门 $O_t$ 分别计算如下：

$I_t=\sigma(X_tW_{xi}+H_{t-1}W_{hi}+b_i)$；

$F_t=\sigma(X_tW_{xf}+H_{t-1}W_{hf}+b_f)$；

$O_t=\sigma(X_tW_{xo}+H_{t-1}W_{ho}+b_o)$；

其中的 $W_{xi}$，$W_{xf}$，$W_{xo}$ 和 $W_{hi}$，$W_{hf}$，$W_{ho}$ 是对应的权重参数，$b_i$，$b_f$，$b_o$ 是对应的偏差参数。

4.3 基于扩展攻击链和 LSTM 的 APT 检测

结合以上定义，基于扩展攻击链和 LSTM 的 APT 检测方法的总体框架，具体可以分为以下四个步骤：

1. 扩展攻击链映射。将宽度为 j 的窗口内的网络事件序列 ei-j，…ei-1，ei 输入至 LSTM，与此同时，对事件与扩展攻击链模型进行映射。

2. 事件权重更新。根据攻击链映射的结果获得各个事件 ei 的权重 wi，并将其更新至“1”已输入至 LSTM 模型的事件序列中。

3. 事件序列表示学习。使用 LSTM 模型来结合不同时刻事件的信息提取事件的变化特征，并进行表示向量的学习，将该窗口内的整个事件序列表示成一维的向量。

4. 流数据的异常检测。使用成熟的数据流上的异常检测算法 RRCF[12] 给出异常分数。为了确定异常事件

（下转第 108 页）

在一些班级进行试验，教学效果得到明显改善。

## 7 教学效果

当学生学习完 Java 程序设计后，制作了阅卷调查，一共按照计划收集了 20 级软件技术 2、3、4、9、10、11、12、13 班共 8 个班的《阅卷调查》报告，共计近 300 份，其中 9、10、11、12、13 班因为是勤工助学班，大部分学生外出实习，留在本班学习的学生较少，平均只有 10 几个，整体阅卷调查覆盖整个年级大部分班级（学生掌握知识的情况如表 3 所示）。

学生普遍反映，Java 程序设计知识点本身有点枯燥，但由于老师采用了以上各种教学方法，使学生能够跟上老师的节奏，调动了学生学习的积极性。学生通过对比法，逐渐掌握到了 Java 的基础知识，了解到了 Java 语言的魅力；通过案例法，学生从知识点逐渐过渡实际生活的案例，以点到面，逐渐形成利用 Java 语法解决问题的习惯，达到知识点的深刻理解；通过项目法，学生开始总结每章所学习的知识点，以一个小组共同完成一个小项目，尽管在编程的过程中遇到了不少问题和麻烦，但最终可以单独做出一个项目，整体能力有了不小的提升，收获颇丰。

## 8 结语

Java 程序设计是计算机系软件技术等相关专业的一门专业课程，传统的教学模式，是以老师一人授课，学生听的模式，但学生的基础薄弱，理解基础知识点困难，课堂上跟不上老师的步骤。本文通过采取案例法、对比法、项目法等教学方法进行教学，取得了一定的教学效果，使学生的兴趣得到了一定的提高，并感受到了 Java 语言的魅力，为后续 JavaWeb、JavaEE 等课程打下了扎实的基础。

## 参考文献：

[1] 刘萍，陈东东．高职 Java 程序设计课程教学设计与实践 [J]. 计算机教育 ,2016,150(02):150-152.
[2] 李韦红．高职院校 Java 程序设计课程教学改革与探索研究 [J]. 电脑知识与技术 ,2018(14):147-148.
[3] 王树宝．以创课为载体助推《Java 程序设计》课程教学改革 [J]. 计算机教育 ,2021,42(02):178-179.
[4] 宋艳．超星学习通在 Java 程序设计课程教学中的应用 [J]. 福建电脑 ,2020,36(11):137-138.
[5] 熊风光，张元，况立群．面向对象程序设计课程教学改革 [J]. 计算机教育 ,2021(09):86-88.

（上接第 12 页）

序列，可以设定一个阈值并认为该分数超过阈值的序列存在异常。

## 5 结语

现有网络攻击防御措施主要侧重于检测固定模式的网络攻击行为，对 APT 攻击检测效果不佳。本文在分析 APT 攻击原理和攻击特点的基础上，提出了一种新的 APT 检测方法。在经典网络攻击链模型基础上，考虑内部威胁部分，提出了扩展攻击链模型，并结合 LSTM 神经网络模型对网络行为进行广泛关联，为 APT 攻击检测的应用实践提供了一种新的思路。

## 参考文献：

[1] 孙增．高级持续性威胁 (APT) 的攻防技术研究 [D]. 上海：上海交通大学 ,2015.
[2] 陶晓玲，周理胜，龚昱鸣．基于角标随机读取的 Snort 报警数据聚合方法 .CNKI:SUN:GLDZ.0.2019-04-008[P].2019.
[3] Karim I,Vien Q T.Snort-based intrusion detection system for practical computer networks: implementation and comparative study[J].2017.
[4] More S,Matthews M,Joshi A,et al. A Knowledge-Based Approach to Intrusion Detection Modeling[M].2012.
[5] 王竹晓，张彭彭，李为，等．基于深度 Q 网络的电力工控网络异常检测系统 [J]. 计算机与现代化 ,2019(12):114-118.
[6] 张蕾，崔勇，刘静，等．机器学习在网络空间安全研究中的应用 [J]. 计算机学报 ,2018,41(09):1943-1975.
[7] 高昆仑，辛耀中，李钊，等．智能电网调度控制系统安全防护技术及发展 [J]. 电力系统自动化 ,2015,39(01):48-52.
[8] 刘海波，武天博，沈晶，等．基于 GAN-LSTM 的 APT 攻击检测 [J]. 计算机科学 ,2020,47(01):287-292.
[9] Hutchins EM,Cloppert MJ,Amin RM.Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research.2011,01(01):80.
[10] 刘文彦，霍树民，陈扬，等．网络攻击链模型分析及研究 [J]. 通信学报 ,2018,39(S2):88-94.
[11] Gf A,Schmidhuber J,F Cummins.Learning to Forget:Continual Prediction with LSTM[C]//Istituto Dalle Molle Di Studi Sull Intelligenza Artificiale.Istituto Dalle Molle Di Studi Sull Intelligenza Artificiale,1999.
[12] Guha S, Mishra N, Roy G, et al. Robust random cut forest based anomaly detection on streams. In: Proc.of the Int'l Conf. on Machine Learning (ICML),2016:2712-2721.