计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.181102103

基于 GAN-LSTM 的 APT 攻击检测

刘海波　武天博　沈　晶　史长亭
哈尔滨工程大学计算机科学与技术学院　哈尔滨 150000
(liuhaibo@hrbeu.edu.cn)

摘　要　高级持续性威胁(Advanced Persistent Threat,APT)带来的危害日趋严重。传统的 APT 检测方法针对的攻击模式比较单一,处理的 APT 攻击的时间跨度相对较短,没有完全体现出 APT 攻击的时间序列性,因此当攻击数据样本较少、攻击持续时间较长时准确率很低。为了解决这个问题,文中提出了基于生成式对抗网络(Generative Adversarial Netwokrs,GAN)和长短期记忆网络(Long Short-term Memory,LSTM)的 APT 攻击检测方法。一方面,基于 GAN 模拟生成攻击数据,为判别模型生成大量攻击样本,从而提升模型的准确率;另一方面,基于 LSTM 模型的记忆单元和门结构保证了 APT 攻击序列中存在相关性且时间间距较大的序列片段之间的特征记忆。利用 Keras 开源框架进行模型的构建与训练,以准确率、误报率、ROC 曲线等技术指标,对攻击数据生成和 APT 攻击序列检测分别进行对比实验分析。通过生成式模型生成模拟攻击数据进而优化判别式模型,使得原有判别模型的准确率提升了 2.84%,与基于循环神经网络(Recurrent Neural Network,RNN)的 APT 攻击序列检测方法相比,文中方法在检测准确率上提高了 0.99 个百分点。实验结果充分说明了基于 GAN-LSTM 的 APT 攻击检测算法可以通过引入生成式模型来提升样本容量,从而提高判别模型的准确率并减少误报率;同时,相较于其他时序结构,利用 LSTM 模型检测 APT 攻击序列有更好的准确率和更低的误报率,从而验证了所提方法的可行性和有效性。

关键词:网络安全;博弈论;高级持续性威胁;生成式对抗网络;长短期记忆网络
中图法分类号　TP393

Advanced Persistent Threat Detection Based on Generative Adversarial Networks and Long Short-term Memory

LIU Hai-bo,WU Tian-bo,SHEN Jing and SHI Chang-ting
College of Computer Science and Technology,Harbin Engineering University,Harbin 150000,China

Abstract　Advanced persistent threat (APT) brings more and more serious harm. Traditional APT detection methods have a lower accuracy when the attack data samples are fewer and the attack duration is longer. To solve this problem,an ATP attack detection method based on generative adversarial networks (GAN) and long short-term memory (LSTM) was proposed. On the one hand,this method generates attack data based on GAN simulation,generates a large number of attack samples for discriminant model,and improves the accuracy of the model. On the other hand,the memory unit and gate structure based on LSTM model guarantee the feature memory among the sequence fragments which have correlation and large time interval in APT attack sequence. Keras open source framework was used to construct and train the model,and Accuracy,FPR,ROC curve were used as metric to compare,test and analyze the methods of attack data generation and APT attack sequence detection. By generating simulated attack data and optimizing the discriminant model,the accuracy of the original discriminant model is improved by 2.84%,and the accuracy of APT attack sequence detection is improved by 0.99% comparing with the recurrent neural network (RNN) model. The experimental results fully show that APT attack detection algorithm based on GAN-LSTM can improve the accuracy of discriminant model and reduce false alarm rate by introducing generative model to increase sample size,and the detection of APT attack sequence using LSTM model has better accuracy and lower false alarm rate than other temporal structures,which shows the feasibility and validity of the proposed method.

Keywords　Network security,Game theory,Advanced persistent threat,Generative adversarial networks,Long short-term memory

到稿日期:2018-11-15　返修日期:2019-05-04　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:黑龙江省自然科学基金(F2018011);中央高校基本科研业务费专项资金(HEUCFP201808,HEUCFP201838)
This work was supported by the Natural Science Foundation of Heilongjiang Province of China (F2018011),Fundamental Research Funds for the Central Universities of Ministry of Education of China (HEUCFP201808,HEUCFP201838).
通信作者:沈晶(shenjing@hrbeu.edu.cn)

近年来，高级持续性威胁越来越多，APT 是网络攻击中最难以防范的攻击手段之一。这类攻击往往带有十分明显的目的性，攻击者通过几乎不可抵挡的复杂入侵方式，隐蔽且长期地潜伏在目标系统之内，最终实施破坏或窃取核心资料。

目前常用的与 APT 相关的检测方法有基于沙箱的恶意代码检测、基于异常流量检测、全包捕获与分析、主机恶意代码检测、社交网络安全事件挖掘等[1-2]。基于沙箱的恶意代码检测方法通过在容器(模拟执行环境)中运行可疑应用程序并监控其异常行为实现对恶意攻击代码的检测。基于异常流量检测的方法首先建立正常流量模式基准，通过网络流量的细微变化来检测网络攻击事件。全包捕获与分析方法通过抓取网络中特定场合下的全数据报文，利用大数据分析技术检测是否存在攻击。主机恶意代码检测方法通过特征码或启发式规则检测恶意代码。社交网络安全事件挖掘方法从社交网络的海量数据中学习用户在网络中的行为模式并挖掘用户的社交关系网等社会属性，为 APT 攻击检测提供指导和依据。

上述方法主要应对攻击模式固定、时间跨度较短的 APT 攻击，但是由于 APT 攻击规模庞大且攻击持续时间较长，导致数据采集成本较大，攻击样本往往较少，因此传统方法的检测效果往往不佳。鉴于此，本文提出了基于 GAN 和 LSTM 的 APT 攻击检测方法。一方面，基于 GAN 模拟生成大量攻击数据，解决了攻击数据固化单一、攻击数据样本不足的问题；另一方面，利用 GAN 中训练得到的判别器进行 APT 检测，同时，利用 LSTM 处理 APT 攻击序列，以解决攻击时间跨度大导致的判别器记忆缺失问题。本文的方法提高了对 APT 攻击的检测能力。

1 基于博弈论的 APT 网络攻防

APT 攻击在长期持续的攻击过程中综合利用了多种攻击[3]手段，理想状态下被攻击的系统会在 APT 攻击过程中不断提升自我防御能力，当 APT 攻击过程中的攻击被检测系统发现后，系统会提升防范能力以防止攻击方的下一次攻击。若攻击者的攻击能力不变，那么其对防御能力有所提升的系统的攻击成效将降低。因此，攻击方需要提升自己的攻击能力，以应对系统防御能力的增强。但是，这种攻击能力的提升不是盲目的，而是要根据攻击防御系统后带来的反馈有针对性地提升攻击能力。同样地，防御系统也需要不断提升自己的防御能力以应对攻击方攻击能力的增强，这种防御能力的提升也不是盲目的，而是要根据攻击方对防御系统的攻击效果的反馈有针对性地提升防御能力。因此，可以将攻防过程看作攻击者和防护者之间的一场博弈，博弈的双方都根据自身对网络环境和对方的动作估计自己的动作。在此博弈过程中，双方的信息都是不完备的，随着攻防过程的进行，双方都可以获取更多关于对方的信息。

定义 1(APT 网络攻防博弈) APT 网络攻防中，标准形式的博弈可定义为 $G=\{S_a, S_d, u_a, u_d\}$。其中，$S_a=\{S_{a1}, S_{a2}, \cdots, S_{am}\}$ 代表攻击方的策略和工具所组成的空间；$S_d=\{S_{d1}, S_{d2}, \cdots, S_{dn}\}$ 代表防护方的防御策略和防御系统所组成的空间；u_a 表示攻击者的效用函数；u_d 为防护者的效用函数。

根据行为的时间序列性，将博弈论分为两类：静态博弈和动态博弈。静态博弈是指在博弈中，参与人同时选择，或虽非同时选择但后行动者并不知道先行动者采取了什么具体行动；动态博弈是指在博弈中，参与人的行动有先后顺序，且后行动者能够观察到先行动者所选择的行动。攻防双方交替进行并根据对方的反馈来优化自我，因此网络攻防的过程属于动态博弈。攻击方和防御方的博弈过程在理想情况下最终只会出现两种结局：防御方抵御住攻击方的进攻，或攻击方攻破了防御方的防御。因此，APT 网络攻防的博弈过程属于零和博弈，即攻防双方收益的总和为某个常数。

定义 2(APT 网络攻防中的纳什均衡，Nash Equilibrium) 在 APT 攻防对抗的过程中，经过对抗双方的一次或若干次决策选择，得到双方都不愿或不会单独改变自己策略的策略组合，这种攻防双方都不愿改变自己策略的策略组称为纳什均衡。APT 网络攻防中的纳什均衡可表示为：在博弈 $G=\{S_a, S_d, u_a, u_d\}$ 中，如果策略组 $\{s_a^*, s_d^*\}$ $(s_a^* \in S_a, s_d^* \in S_d)$ 中任一策略都是对对手策略的最佳策略，即对任一策略 $s_a' \in S_a$ 和策略 $s_d' \in S_d$，总有收益 $(s_a', s_d^*) \leqslant$ 收益 $(s_a^*, s_d^*) \geqslant$ 收益 (s_a^*, s_d')，则策略组 $\{s_a^*, s_b^*\}$ 称为 APT 网络攻防中的一个纳什均衡。

为了让系统具有更好的 APT 攻击检测能力，向 APT 攻击检测系统中加入一个与自身进行动态博弈的 APT 攻击者，这样通过二者的零和博弈，最终达到纳什均衡点，此时攻击方和防御方的策略组合达到最优，而后再利用这个攻击者来优化 APT 攻击检测系统的能力。

2 基于 GAN-LSTM 的 APT 检测算法

2.1 基于 GAN 的 APT 攻击数据生成方法

近年来，深度学习的兴起与大数据、云计算的飞速发展密不可分。这些数据相关技术的发展，为模型提供了更多的样本量，随着样本量的提升，模型的准确率逐步攀升。APT 攻击由于规模庞大且攻击持续时间较长，导致数据采集成本过大，攻击样本往往较少，因此攻击样本量的提升会提高 APT 攻击检测的准确率。

APT 攻防过程包括 APT 攻击者和 APT 防御者，攻击和防御处于动态变化的博弈过程，因此，攻击能力的提升会动态地提升防御的能力，向模型中加入攻击能力不断增强的攻击者会反向增强防御模型的防御能力，因此本文采用 GAN 模拟攻防体系。

GAN[4]由生成式模型和判别式模型共同组成，生成式模型用来生成攻击数据，判别式模型用来判别样本数据和生成式模型产生的数据是否为攻击数据。GAN 利用了博弈论的相关理论[5]。整个博弈过程中，判别式模型不断调整权值参数以分辨出真实数据和生成数据，生成式模型不断调整权值参数以生成判别器无法准确分辨的生成数据[6]，当 GAN 达

到纳什均衡状态后，GAN 达到收敛状态[7]，此时生成式模型可以生成模拟真实攻击样本的数据。

APT 的攻击和防御存在着博弈关系，其中判别式模型作为 APT 的防御者，生成式模型作为 APT 的攻击者。整个 GAN 训练的目标函数[8]定义为：

$$\min_G \max_D V(D,G)=E_{x\sim p_{\text{data}}(x)}[\log D(x)]+E_{z\sim p_{\text{data}}(z)}[\log(1-D(G(z)))] \quad (1)$$

其中，x 表示真实的网络攻击样本，z 表示输入生成式模型 G 的高斯随机噪声[9]变量，$G(z)$表示 G 网络生成的模拟攻击数据。$D(x)$表示判别式模型 D 判断真实样本 x 是真实攻击数据的概率，$D(G(z))$是判别式模型 D 判断生成式模型 G 生成的数据是真实攻击数据的概率。对于 G，期望 $D(G(z))$趋近于 1。若 $D(x)$趋近于 0，此时 $V(D,G)$趋向于某个极小数；对于 D，期望 $D(x)$趋近于 1。若 $D(G(x))$趋近于 0，此时 $V(D,G)$会趋向于某个极大数。当 GAN 达到纳什均衡时，D 已经无法区分出输入数据是真实攻击样本数据还是生成式模型生成的模拟攻击数据，此时 $D(G(z))=D(x)=1/2$，目标函数收敛于 $-\log 4$[10]，生成式模型已经可以生成模拟样本的攻击数据。

当生成式模型训练完毕后，利用生成式模型模拟生成大量的模拟攻击数据，为新生成的攻击数据标记对应的标签后将其与原始攻击数据共同作为判别式模型的样本。此方法能够极大地提升样本容量，从而提升判别模型的准确率。

2.2 基于 LSTM 的 APT 时序处理方法

APT 的长期持续性，导致当前时刻和与之产生关联性的先前时间之间可能存在较大的时间跨度，因此本文采用 LSTM 模型来处理 APT 的时间序列。

LSTM[11]模型是基于循环神经网络[12]（Recurrent Neural Network，RNN），为了解决梯度消失[13]问题并处理更长序列的一种改进模型。LSTM 的内部结构如图 1 所示，其在 RNN 基础上增加了遗忘门、更新门、输出门。其中，$x^{\langle t\rangle}$ 表示 APT 攻击序列 x 在 t 时刻的序列片段[14]；$a^{\langle t-1\rangle}$ 是 t 时刻网络隐层的输出信息，会传递给 t 时刻的网络；$c^{\langle t-1\rangle}$ 是 $t-1$ 时刻网络记忆的信息，也会传递到 t 时刻的网络。用 Γ_f 表示遗忘门，Γ_u 表示更新门，Γ_o 表示输出门，$\tilde{c}^{\langle t\rangle}$ 是 t 时刻新的候选记忆信息，相关计算公式分别如下：

$$\Gamma_f=\sigma(W_f\times[a^{\langle t-1\rangle},x^{\langle t\rangle}]+b_f) \quad (2)$$

$$\Gamma_u=\sigma(W_u\times[a^{\langle t-1\rangle},x^{\langle t\rangle}]+b_u) \quad (3)$$

$$\Gamma_u=\sigma(W_o\times[a^{\langle t-1\rangle},x^{\langle t\rangle}]+b_o) \quad (4)$$

$$\tilde{c}^{\langle t\rangle}=\tanh(W_c\times[a^{\langle t-1\rangle},x^{\langle t\rangle}]+b_c) \quad (5)$$

$a^{\langle t-1\rangle}$ 和 $x^{\langle t\rangle}$ 共同经过对应门的权值以及偏置计算，再经过对应激活函数得到对应输出。$c^{\langle t\rangle}$ 的计算公式为：

$$c^{\langle t\rangle}=\Gamma_u\times c^{\langle t\rangle}+\Gamma_f\times c^{\langle t-1\rangle} \quad (6)$$

$c^{\langle t\rangle}$ 由当前时刻记忆单元经过更新门的更新部分和上一时刻记忆单元经过遗忘门的遗忘部分共同决定。$a^{\langle t\rangle}$ 由当前记忆单元激活后经过输出门得到，其计算公式为：

$$a^{\langle t\rangle}=\Gamma_o\times\tanh c^{\langle t\rangle} \quad (7)$$

$y^{\langle t\rangle}$ 是模型在 t 时刻的输出，输出的是到 t 时刻为止输入的序列中是否包含 APT 攻击。

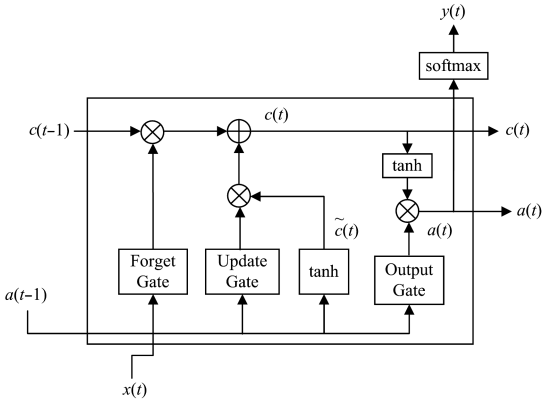


图 1 LSTM 的内部结构

Fig. 1 Internal structure of Long short-term memory

2.3 APT 攻击检测算法

APT 攻击检测算法包括 3 个模块，分别为 APT 攻击数据生成模块、APT 攻击数据判别模块、APT 时序处理模块，其基本结构如图 2 所示。APT 攻击数据生成模块利用 GAN 生成 4 种攻击标签的模拟攻击数据，其输入为原始攻击样本 x 和高斯随机噪声 z，输出为生成的攻击数据。APT 攻击数据判别模块负责对攻击数据进行多分类，其输入为原始攻击样本 x 以及生成数据 $G(z)$，输出为对应的分类标签。APT 时序处理模块采用 LSTM 结构对 APT 进行时序处理，其输入为向量化后的攻击标签，输出为布尔量 y，y 代表当前序列在当前位置之前的序列是否为 APT 攻击序列。

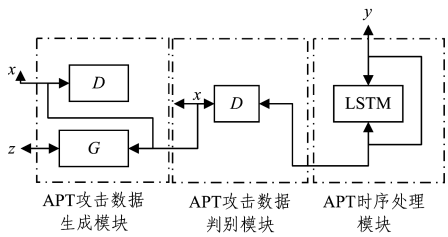


图 2 模型的基本架构

Fig. 2 Basic structure of model

模型的训练过程如下：首先根据 APT 攻击数据生成模块，利用 GAN 原理构建生成 NUM 个攻击标签的攻击数据生成器，具体步骤如下。

1）对每个生成模型做 PRE 次迭代的预训练，使得生成模型有一定的判别能力，记预训练后的模型为 $D_{pre\text{-}1}$，$D_{pre\text{-}2}$，…，$D_{pre\text{-}NUM}$。

2）构造 GAN 模型，将 $D_{pre\text{-}i}$ 作为 GAN 中的初始化 D_{NUM} 模型，该网络经过 N 次对抗训练达到收敛。由此，得到生成模型 D_1，D_2，…，D_{NUM}。

训练完 NUM 个生成器后，利用生成数据优化训练 APT 攻击数据判别模块的判别式模型 D，具体步骤如下。

1）用纳什均衡状态下 GAN 中的判别式模型的权值初始化 APT 攻击数据判别模块的判别式模型 D。

2)利用生成器 $D_1, D_2, \cdots, D_{NUM}$ 生成 C 条模拟样本数据，并根据生成器的类别对生成数据标签进行处理。

3)将生成的数据和原始样本数据共同作为样本输入模型 D，直到算法收敛。由此得 APT 攻击多分类判别式模型 D。

训练完判别式模型 D 后，利用 APT 时序处理模块对 APT 攻击序列进行训练，具体步骤如下。

1)根据标签的种类和数目，将模型 D 的输出标签进行向量化处理。

2)将长度为 SEQ 的 APT 攻击序列 x 作为样本数据，依次将 x 在 t 时刻的词向量输入时序处理模型，模型经过 L 次训练达到收敛状态。

时序模型训练完毕后，整个模型框架完成。时序处理模块无限接收 APT 攻击数据判别模块向量化后的输出，直至检测到当前序列属于 APT 攻击序列。APT 检测算法的伪代码如算法 1 所示。

算法 1 APT 攻击检测算法

输入：t 时刻的网络数据报文 $IP_{(t)}$

输出：当前时刻存在 APT 攻击威胁的概率 $P_{(seq(t)=APT)}$

```
1. while TRUE do
2.    对报文进行特征提取，x(t) = f(IP(t))
3.    将 x(t) 输入到攻击检测模型 D，x(t) -> D
4.    得到对应的标签 Label(t)，Label(t) = D(x(t))
5.    if Label(t) == NORMAL then
6.       continue
7.    else
8.       将 Label(t) 进行词向量替换，L(t) = WordDic(Label(t))
9.       将 L(t) 输入到时序模型 LSTM，L(t) -> LSTM
10.      计算当前序列属于 APT 攻击的概率，即 P(seq(t)=APT) = LSTM(L(t))
11.      end if
12. end while
```

对于长度为 n 的网络报文序列，APT 攻击检测算法首先对每条报文进行标签判别，处理时间复杂度为 O(1)；然后，将该标签连同先前的标签扩展至时序模型训练时每一轮中的最大迭代次数 m，再输入到时序模型得到当前序列属于 APT 攻击序列的概率，处理时间复杂度为 O(mn)。因此，算法的总体复杂度为 O(mn)。

3 实验与分析

3.1 实验环境及模型构建

实验环境基于 Linux 操作系统，开发语言使用 shell 脚本语言和 python 语言，网络模型的开发基于 Keras 开源框架。APT 攻击数据生成模块使用的训练数据集为 KDD99，其由美国国防部高级规划署在林肯实验室通过建立模拟美国空军局域网的网络环境并收集 9 周的网络连接和系统审计数据组成，共约 50 万条，包含 4 大类攻击类型，39 小类具体攻击类别。每条数据包含 41 个特征值，其中 TCP 连接的基本特征 9 种、TCP 连接的内容特征 13 种、基于时间的网络流量统计特征 9 种、基于主机的网络流量统计特征 10 种。取其中 40 个特征作为样本输入特征，利用 shell 脚本将每条数据标签替换为 5 类标签，分别为 ATTACK, UP, FILEOP, PROBING, NORMAL，依次代表攻击、提升权限、进行文件操作、监听动作、正常数据。APT 时序处理模块数据集根据 APT 攻击特性，构造正则表达式 $((N|P|A)^*U)^*(A^*F^*)^*$（可以利用 shell 脚本模拟生成），其中 N, P, A, U, F 分别代表 NORMAL, PROBING, ATTACK, UP, FILEOP 这 5 类标签。攻击序列样本由标签 N, P, A, U, F 组成，再经过向量化处理将每条序列转化为对应的向量，其中，[1,0,0,0,0] 代表 A，[0,1,0,0,0] 代表 U，[0,0,1,0,0] 代表 F，[0,0,0,1,0] 代表 P，[0,0,0,0,1] 代表 N。

APT 攻击数据生成模块中的判别式模型 D 采用 CNN 结构模型，输入样本共有 40 个特征值，分为 TCP 连接的基本特征、TCP 连接的内容特征、基于时间的网络流量统计特征、基于主机的网络流量统计特征 4 类，每类特征有一定相关性。类似于灰度图像[15]被分为水平的 4 条光带，输入数据也被转换为 4×10 的矩阵。CNN 包含 4 个卷积池化层、2 个全连接层和 1 个 sigmoid 激活层，其中，第 1 个卷积池化层包含 5 个 3×3 卷积层和 1 个最大池化层，第 2 个卷积池化层包含 3 个 3×3 卷积层和 1 个最大池化层，第 3 个卷积池化层包含 1 个 3×3 卷积层和 1 个最大池化层，第 4 个卷积池化层包含 1 个卷积层和 1 个最大池化层。最后，经过 sigmoid 激活层输出的是输入数据属于当前标签类别的概率。

生成式模型 G 采用 10 层深度神经网络模型实现，其输入为 100×1 维高斯随机噪声向量，隐层权值和输出均为 40×1 维向量。G 的输出结果转化为与判别式模型 D 输入维度相同的 4×10 的矩阵作为判别式模型 D 的输入。4 种攻击 ATTACK, UP, FILEOP, PROBING 的网络结构一致，超参数相同，只需要分别根据不同标签对应的真实样本训练 4 次并保存对应类别的权值参数，即可得到 4 种攻击类别的生成式模型。

APT 攻击数据判别模块的判别模型 D 采用 CNN 结构，该模型与 APT 攻击数据生成模块的判别式模型 D 结构相似，不同之处在于最后一层由原来的 sigmoid 二分类层变为 softmax 多分类层。其输出为输入数据所属的 5 类标签（4 类攻击标签和 1 类正常标签）。

APT 时序处理模块采用 LSTM 结构模型[16]，每一时刻的输入 $x_{(t)}$ 为 APT 攻击数据判别模块的输出标签向量化[17]后的 1×5 维向量[18]，记忆传递单元 $a^{(t)}$ 为 10×5 的矩阵，记忆单元 $c^{(t)}$ 为 10×5 的矩阵，遗忘门参数 W_f 为 10×11 的矩阵，更新门参数 W_u 为 10×11 的矩阵，输出门参数 W_o 为 10×11 的矩阵。

3.2 实验结果的对比分析

实验中数据集的分布如表 1 和表 2 所列，整个数据集分为 3 部分：80%的数据作为训练集，用于训练网络模型；交叉验证集占 10%，用于调整模型结构；剩余 10%作为测试集，用

于测试模型的实际效果。用来训练生成模型的数据集分为 4 部分，分别对应 4 类攻击标签 ATTACK，PROBING，UP，FILEOP，各占各自标签对应样本数据的 50%。

表 1 整体数据集的分布情况

Table 1 Distribution of total data set

集合类别	百分比/%
训练集	80
交叉验证集合	10
测试集	10

表 2 生成数据集分布情况

Table 2 Distribution of generating data set

生成数据类别	百分比/%
ATTACK	50
PROBING	50
UP	50
FILEOP	50

目前由于完整的 APT 攻击流程持续时间较长且数据采集成本较高，因此并没有 APT 检测与深度学习相结合的具体实验，大多数实验都是基于入侵检测数据集，这些数据无法完全反映出 APT 的具体攻击流程和 APT 攻击的时间性、序列性的特点。因此，为了验证实验效果，采用两组对比实验：攻击数据生成实验和 APT 攻击序列检测实验。

攻击数据生成实验采用控制变量法，分别对比没有生成模型和引入生成模型的网络的检测准确率和误报率。实验中，首先去掉 APT 攻击数据生成模块，只保留 APT 攻击数据检测模块，直接使用原始数据样本训练 APT 攻击数据判别模型，经训练后对测试集数据进行测试，准确率达 82.12%。然后，为了验证 GAN 对现有网络的影响，向原模型系统中加入 APT 攻击数据生成模块，依次构建 4 种标签 ATTACK，UP，PROBING，FILEOP 对应的生成模型，训练完毕后生成对应标签的模拟攻击数据，再将这些数据与原始样本数据共同作为输入样本训练 APT 攻击数据判别模型，实验结果如表 3 所列。可以看出，加入 ATTACK 生成器后，准确率提高到 83.22%；加入 UP 生成器后，准确率提高到 83.73%；加入 PROBING 生成器后，准确率提高到 84.24%；加入 FILEOP 生成器后，准确率提高到 84.96%。总体上，准确率提升了 2.84%。随着生成器的不断加入，各类标签的样本数据逐渐增多，模型的准确率逐渐上升，误报率和漏报率都有所降低。选取不同阈值，分别绘制 5 组实验情况下的 ROC 曲线，结果如图 3 所示。根据 ROC 曲线特性，曲线越靠近左上角说明模型效果越好。随着生成模型的加入，曲线越来越靠近(0,1)坐标点，通过计算得出 5 条曲线的 *auc* 值分别为：0.755，0.784，0.812，0.846，0.865，这说明随着生成器的依次加入，模型的识别效果越来越好。由此可见，在迭代次数和测试数据集都相同的情况下，向 GAN 中加入生成模型后，测试集判别的准确率得到了提高，误报率和漏报率都有所下降；而且增加对应攻击类别的生成模型后，各类指标都在原有基础上得到了提升，这说明利用 GAN 构建 APT 攻击数据生成模型能够通过扩充样本容量提升判别模型的准确率，并降低误报率和漏报率。

表 3 生成模型的性能对比

Table 3 Performance comparison of generating model

(单位：%)

模型	准确率	误报率	漏报率
无生成器模型	82.12	4.78	5.22
加入 ATTACK 生成器	83.22	4.36	5.19
加入 UP 生成器	83.73	4.07	5.13
加入 PROBING 生成器	84.24	3.85	5.07
加入 FILEOP 生成器	84.96	3.82	4.82

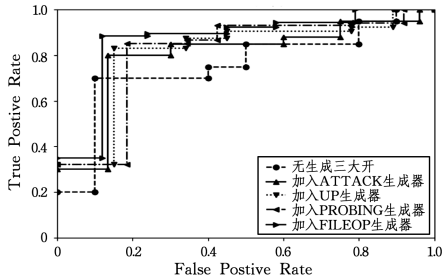


图 3 攻击数据生成实验的 ROC 曲线

Fig. 3 ROC curve of attack data generation experimental

APT 攻击序列检测实验采用控制变量法，分别采用基本 RNN 网络结构/GRU 网络结构、LSTM 网络结构进行对比实验。为了验证实验效果，将测试集中的序列按照长度范围进行分类，实验结果如表 4 所列。可以看出，序列长度较短时，3 种模型的准确率基本持平，随着长度的增加，相同序列长度范围下 LSTM 模型的准确率要略高于 GRU，且明显高于 RNN 模型。随着序列长度范围的增加，3 种模型的准确率都有所降低，但是 RNN 的准确率的降低幅度要大于另外两种模型。LSTM 的最终准确率最高，高出 RNN 0.99 个百分点，误报率最低。根据不同的阈值，分别绘制 3 种模型的 ROC 曲线，结果如图 4 所示。可以看出，LSTM 模型的效果略好于 GRU 模型，明显优于 RNN 模型；LSTM 模型的 ROC 曲线更靠近(0,1)坐标点。通过计算得出 3 条曲线的 *auc* 值分别为 0.828，0.853，0.859，这说明 LSTM 模型的效果相对更好，相较于其他网络结构，在序列长度范围相同的情况下准确率更高、误报率更低，因此使用 LSTM 模型检测 APT 攻击序列具有较好的效果。

表 4 序列模型的性能对比

Table 4 Performance comparison of sequence model

(单位：%)

序列长度范围	RNN	GRU	LSTM
1～1000	99.31	99.32	99.31
1000～5000	98.82	99.30	99.26
5000～10000	96.88	98.37	98.56
10000 以上	95.36	97.15	97.21
测试集准确率	97.83	98.76	98.82
测试集误报率	2.72	2.31	2.25

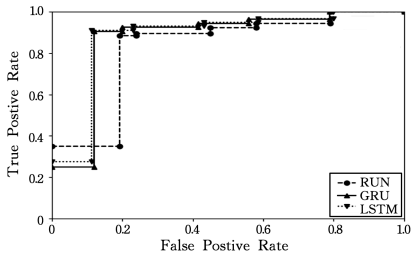


图 4 APT 攻击序列检测实验的 ROC 曲线

Fig. 4 ROC curve of APT attack sequence detection

结束语 现有 APT 的攻击检测技术主要着眼于小规模、模式较为单一的 APT 攻击，在 APT 攻击数据较少、攻击持续时间较长时效果不佳。本文从深度学习的角度出发，分别使用基于 GAN 的 APT 攻击数据生成方法和基于 LSTM 的 APT 时序处理方法生成大量的攻击数据，处理 APT 时序序列。实验结果表明，基于 GAN 和 LSTM 的 APT 检测方法，一方面通过模拟生成攻击数据极大地增加了样本数据量，提高了判别模型的准确率，降低了误报率；另一方面，针对 APT 攻击的长期持续性，通过 LSTM 的记忆单元和门结构保证了对较长时序序列的特征记忆，在针对持续性较长的 APT 攻击序列时保证了一定的准确率和误报率。将 GAN 和 LSTM 应用于 APT 攻击检测中，为解决 APT 攻击检测问题提供了一种新的思路。

虽然本文提出的方法针对 APT 攻击样本较少、攻击持续时间较长的问题进行了相应改进，但是仍有不足之处，当序列过长时虽然能保证一定的准确率，但效果仍需进一步提高。GAN 在后续的工作中，我们将寻找解决这些问题的方法。

参 考 文 献

[1] ZENG W L, LI G H, CHEN J W. A Model of Network Security Protection System Based on APT Intrusion and Its Key Technologies[J]. Journal of Modern Electronics Technology, 2013, 36(17): 78-80.

[2] LIU X. APT Attack Detection and Defense in Data Context [J]. Network and Information Engineering, 2014, 30(2): 80-81.

[3] LI F H. Research on Anti-APT Attack Scheme of High-level Security Network [J]. Information Network Security, 2014(9): 109-114.

[4] GOODFELLOW I J. Generative Adversarial Nets[C]// Advances in Neural Information Processing Systems. 2014: 2672-2680.

[5] SALIMANS T, GOODFELLOW I. Improved Techniques for Training GANs [J]. arXiv: 1606.03498.

[6] RADFORD A. Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks [J]. arXiv: 1511.06434.

[7] MIRZA M. Conditional Generative Adversarial Nets[J]. arXiv: 1411.1784v1.

[8] GOODFELLOW I. NIPS 2016 Tutorial: Generative Adversarial Networks[J]. arXiv: 1701.00160.

[9] ARORA S, GE R, LIANG Y Y, et al. Generalization and Equilibrium in Generative Adversarial Nets[J]. arXiv: 1703.00573.

[10] GULRAJANI I, AHMED F, ARJOVSKY M, et al. Improved Training of Wasserstein GANs[J]. arXiv: 1704.00028v3.

[11] HOCHREITER S, SCHMIDHUBER J. Long short-term memory[J]. Springer Berlin Heidelberg, 2012, 8(8): 1735-1780.

[12] SOCHER R, PERELYGIN A, WU J Y, et al. Recursive deep models for semantic composotionality over a sentiment treebank [C]// Proc of the Conference on Empirical Methods in Natural Language Processing. Seattle, USA: ACL, 2013: 1631-1642.

[13] LECUN Y, BENGIO Y, HINTON G. Deep learning[J]. Nature, 2015, 521(7553): 436-444.

[14] CHO K, VAN MERRIENBOER B, BAHDANAU D, et al. On the properties of neural machine translation: encoderdecoder approaches[J]. arXiv: 1409.1259v2.

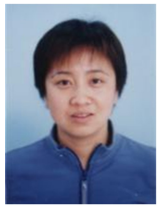
[15] DONG C, CHEN C L, HE K, et al. Image super-resolution using deep convolutional networks[J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2016, 38(2): 295-307.

[16] MNIH V, HEESS N, GRAVES A. Recurrent models of visual attention[M]// Advances in Neural Information Processing Systems. Massachusetts: MIT Press, 2014: 2204-2212.

[17] BAHDANAU D, CHO K, BENGIO Y. Neural machine translation by jointly learning to align and translate[J]. arXiv: 1409.0473.

[18] MIKOLOV T, CHEN K, CORRADO G, et al. Efficient estimation of word representations in vector space[J]. arXiv: 1301.3781.

LIU Hai-bo, born in 1976, Ph. D, associate professor, is a member of China Computer Federation (CCF). His research interests include intelligence computing and information security.



SHEN Jing, born in 1969, Ph. D, associate professor, is member of China Computer Federation (CCF). Her research interests include machine learning.