计算机科学
COMPUTER SCIENCE

基于动态贝叶斯博弈的工业控制网络恶意接入检测研究

刘浩含，陈泽茂

引用本文

刘浩含，陈泽茂. 基于动态贝叶斯博弈的工业控制网络恶意接入检测研究[J]. 计算机科学，2025，52(1)：383-392.

LIU Haohan, CHEN Zemao. Study on Malicious Access Detection in Industrial Control Networks Based on Dynamic BayesianGames [J]. Computer Science, 2025, 52(1): 383-392.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231200083

基于动态贝叶斯博弈的工业控制网络恶意接入检测研究

刘浩含　陈泽茂
武汉大学国家网络安全学院　武汉 430040
(liuhaohan@whu.edu.cn)

摘　要　针对工业控制网络(Industrial Control Network,ICN)远程接入场景下未经授权访问、拒绝服务攻击、欺骗攻击以及信息披露等安全问题,通过STRIDE威胁建模方法对该场景下的潜在威胁进行分析,提出一种基于动态贝叶斯博弈的接入检测框架。该方法能够将试图接入ICN的非法、恶意请求筛选出来并阻断,同时利用持续进行的多轮博弈迭代以及SDN灵活动态的特性对策略参数进行实时调整,以防止相同恶意接入源的再次访问。仿真实验结果表明,随着博弈轮数的增加,相比于现有的两类恶意接入防御方法,该框架的检测准确性提升了3%以上,假阳性比例下降了1.2%以上,检测效率提升了14.7%以上,且具有较好的鲁棒性。

关键词:工业控制网络;软件定义网络;动态贝叶斯博弈;恶意接入检测
中图分类号　TP393

Study on Malicious Access Detection in Industrial Control Networks Based on Dynamic Bayesian Games

LIU Haohan and CHEN Zemao
School of Cyber Science and Engineering,Wuhan University,Wuhan 430040,China

Abstract　In view of security issues such as unauthorized access,denial of service attacks,spoofing attacks and information disclosure in the remote access scenario of industrial control network(ICN),the STRIDE threat modeling method is used to analyze the potential threats in this scenario. An access detection framework based on dynamic Bayesian game is proposed. This method can screen and block illegal and malicious requests trying to access the ICN. At the same time,it uses the continuous multiple rounds of game iterations and the flexible and dynamic characteristics of SDN to adjust the policy parameters in real time to prevent the same malicious access source from being accessing again. Simulation experimental results show that as the number of game rounds increases,compared with the existing two types of malicious access defense methods,the detection accuracy of this framework increases by more than 3%,the false positive rate decreases by more than 1.2%,the detection efficiency has improved by more than 14.7%,and it has good robustness.

Keywords　Industrial control network,Software-defined network,Dynamic Bayesian game,Malicious access detection

1　引言

工业控制网络作为关键的基础设施,其安全性至关重要。恶意接入是工控网络中常见的攻击行为,其中包括未授权访问、拒绝服务攻击以及欺诈访问等。恶意接入通常作为攻击工控网络的第一步,可以为后续攻击提供有利条件,从而进一步导致严重的后果,如系统瘫痪、数据泄露和生产中断。与大部分传统企业网络不同,工业控制网络通常对实时性、可靠性要求较高,大多需要不间断运行,因此难以进行离线检测;同时,工控网络中流量较大、协议种类多样,增大了研究人员实施恶意接入检测时的困难程度。因此,提出一种准确高效、实时动态的恶意流量检测机制对于工控网络安全至关重要。

最近有研究者提出基于机器学习的工业控制网络(ICN)入侵检测方法[1-3],用于识别进入ICN的异常、非法流量。这些方法都需要大量样本数据进行建模。Ouyang等[4]提出了一种只需少量学习样本的入侵检测模型(FS-IDS),其适用于只有少量攻击示例时的入侵检测场景。此外,有研究人员将机器学习与SDN技术相结合[5-7],灵活调整网络的防御策略以应对威胁。但是,这些方法因延迟较大,并不适用于工ICN。Fausto等[8]将基于机器学习的IDS与SDN相结合,以增加软硬件复杂度为代价,减少了通信延迟。但该方法需要消耗大量的计算资源,且无法有效面对0Day攻击。除机器学习方法外,还有研究者提出基于行为信息的ICN入侵检测方法[9-10],以区分恶意接入和正常接入行为。但这些方法

到稿日期:2023-12-12　返修日期:2024-04-19
基金项目:国家重点研发计划(2022YFC3102805)
This work was supported by the National Key Research and Development Program of China(2022YFC3102805).
通信作者:陈泽茂(chenzemao@whu.edu.cn)

无法有效应对仿冒、欺骗攻击。Liu 等[11]提出了一种基于弱信号处理技术的针对未授权物理接入的检测方法，以防止仿冒设备接入 ICN。但该方法针对物理接入，并不适用于远程接入的场景。有研究者提出混合的 IDS 方案[12-14]，这些方法资源消耗较大，需要付出较高的维护成本，且无法对策略进行动态调整和更新，从而无法应对持续变化的威胁情境[15]。

为了保护工控网络免受恶意远程接入请求的侵害，克服大部分机器学习方法在计算资源、学习资料等方面要求较高，以及传统基于行为的检测方法难以应对实时变化威胁情境的困难，本文提出一种基于动态贝叶斯博弈(Dynamic Bayesian Games，DBG)的边界恶意行为检测框架(Boundary Malicious Behavior Detection Framework Based on Dynamic Bayesian Game，BMD-DG)。DBG 用于描述多方参与者在不确定环境中做决策和协作的情境。每个参与者通过贝叶斯推理来更新对环境状态和其他参与者策略的信任度分布，并基于该信任度分布采取不同策略和行动。DBG 通常涉及参与者的学习和适应过程，随着时间的推移，参与者通过观察和互动逐渐改进他们的策略，以适应不断变化的环境。BMD-DG 是基于 DBG 的，同时结合了 SDN 架构，通过充分发挥 SDN 对网络流量的全局可见性和灵活的流量控制能力，更加精确地观察和分析 ICS 接入流量，检测恶意接入行为。

本文的主要贡献如下：

1)提出了一种基于动态贝叶斯博弈的恶意接入识别框架 BMD-DG，该框架能够在用户认证之前分析进入网络的流量数据，识别并阻断恶意接入流量。

2)对工业控制网络远程接入场景中的各类异常行为进行了数学建模，并构建了该场景下的动态贝叶斯博弈模型，通过该博弈模型能够区分恶意流量和合法流量。

3)通过仿真实验将 BMD-DG 与现有的防御手段进行横向对比，验证了 BMD-DG 在工业控制网络远程接入场景下具有准确性高、性能开销低的优点。

2 工控网络接入威胁分析

本文所研究的工控接入场景如图 1 所示。工控网络与访问者分处异地，访问者通过非安全的网络信道接入工控网络，对其中的资源进行访问，并对设备进行远程控制。

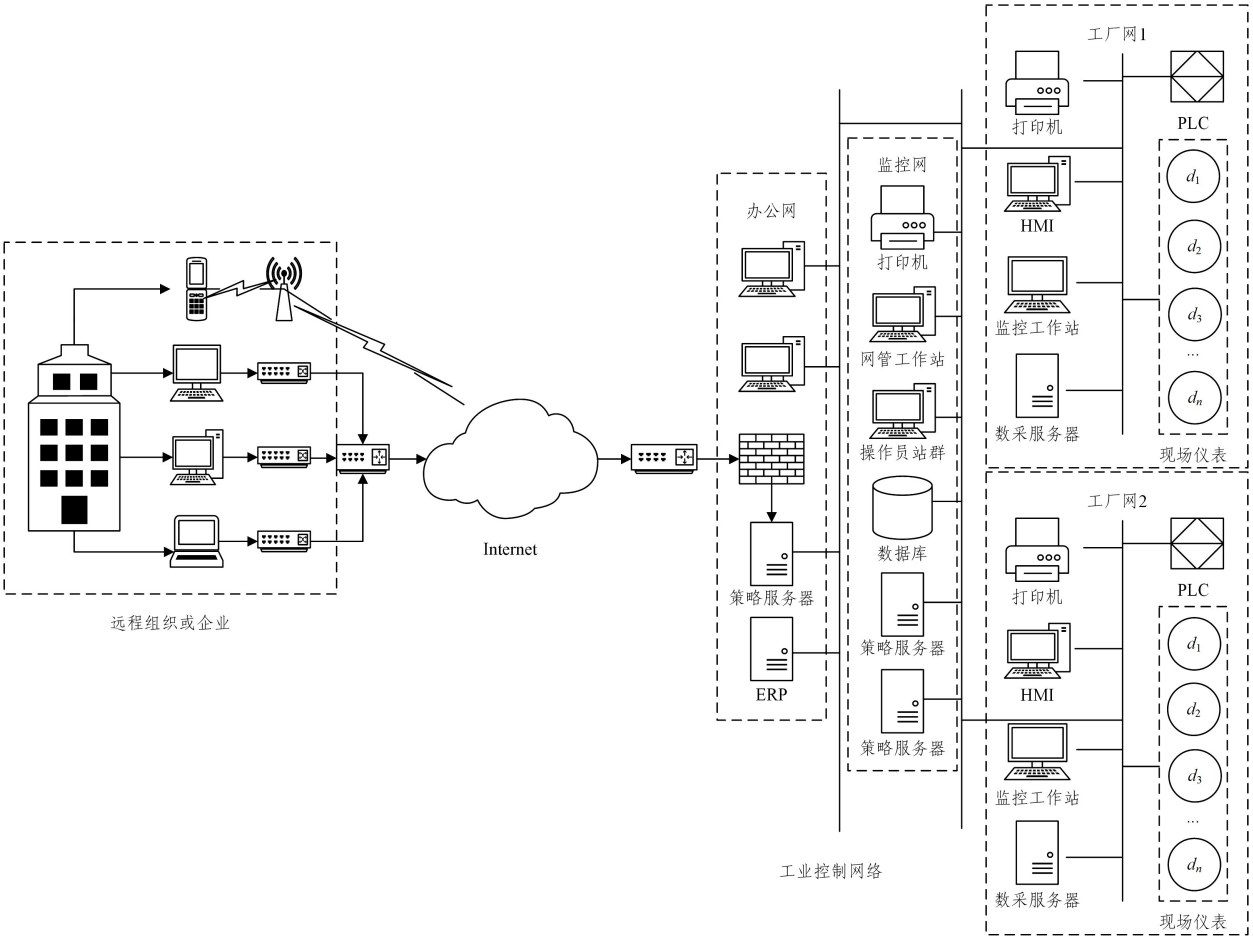


图 1 远程接入场景示意图

Fig. 1 Schematic diagram of remote access scenario

本文采用 STRIDE 威胁建模方法，分析工控网络所面临的接入安全威胁。STRIDE 模型从欺骗(Spoofing)、篡改(Tampering)、否认(Repudiation)、信息披露(Information Disclosure)、拒绝服务(Denial of Service)以及特权提升(Elevation of Privilege)这 6 类攻击的维度，提供了一个系统性、全面性的框架，帮助安全研究者在系统设计阶段更加全面地理解潜在的威胁并进行威胁分析，从而减轻这些威胁。

基于 STRIDE 分析方法，本文的工控网络接入场景所面临的威胁如表 1 所列。

表 1 工控网络远程接入 STRIDE 威胁模型

Table 1 Industrial control network remote access STRIDE threat model

威胁	定义	攻击方式
欺骗 (Spoofing)	冒充有效系统用户或资源以访问工控网络	恶意接入者通过使用虚假 IP 地址或用户信息来隐藏自己的流量来源和身份，从而误导工业控制网络边界防御设施
篡改 (Tampering)	在被发现或未被发现的情况下修改系统或用户数据	未经授权的攻击者修改工业控制网络边界防御设施的规则、策略和访问列表等
否认 (Repudiation)	用户的非法操作因无法被追踪而导致用户可以否认自己的错误行为	该攻击通过身份认证即可抵御，不在本文研究范畴
信息披露 (Information Disclosure)	对敏感信息进行披露	攻击者尝试从恶意接入的回显中获取工控网络中的敏感信息，如登录账号的合法结构、中间件版本号
拒绝服务 (Denial of Service)	使系统暂时不可用或无法使用	攻击者通过向工控网络发送大量接入数据包，致使工控网络边界防御设施瘫痪
特权提升 (Elevation of Privilege)	无对应权限的用户获得特权，从而能够执行特权操作	该攻击发生在用户认证之后，对此本研究不做过多讨论

3 工业控制网络边界接入行为建模

为了方便后续博弈模型的构建以及恶意接入行为检测，本节采用数学建模方法，从接入者的设备行为和网络访问行为等方面构建工控网络边界接入行为模型。将所有行为分为可疑行为和有害行为两类：前者表示可疑但暂时不会危害系统安全的行为，用于确定接入者第 t 次尝试接入时的可疑数值σ_t；后者表示会对系统造成实质性危害的行为，用于确定接入者第 t 次尝试接入时的有害数值τ_t。

表 2 列出了本研究所使用的全部符号及其含义。

表 2 本文所使用符号

Table 2 Symbols used in this paper

符号	含义
τ_t	接入者第 t 次尝试接入时的“有害”数值
σ_t	接入者第 t 次尝试接入时的“可疑”数值
UB_i	编号为 i 的可疑行为
HB_i	编号为 i 的有害行为
t_L	用户接入的时刻
t_R	用户下班的时刻
t_W	用户上班的时刻
Cer_t	证书颁发时间
Cer_v	证书有效期
$Curr\_time$	当前系统时间
F^i_{ip}	源 IP 在同一网段内的数据流
F^i_{mac}	源 MAC 相同的数据流
L_j	某用户第 j 次接入时请求数据包的大小
L_s	接入请求数据包大小的标准值
L_l	上一次接入成功时请求数据包的大小
p_k	凭证验证比率的阈值
o_k	一次性凭证验证比率的阈值

3.1 可疑行为建模

可疑行为是指那些具有反常特征但暂时没有对系统安全构成危害的行为。本文从网络流量中提取和整合可疑行为特征，分别用UB_i表示。对于二值的UB_i指标，其值为 1 时表示存在该行为，为 0 时表示不存在；对于连续型的UB_i指标，其值越大，表示该行为越明显。具体包含以下几类：

1)接入地点非法。根据数据流的源 IP 确定该指标。

2)证书频繁更新。该指标由式(1)确定。

$$UB_2=\max\left(\frac{Cer_t+Cer_v-Curr\_time}{Cer_v},0\right) \tag{1}$$

对于具有初始证书的合法入网设备，我们规定UB_2为 0。频繁更新证书的行为可能意味着攻击者正在尝试滥用盗取得到的证书，他们为了降低被检测到的风险而频繁更新证书，以换取新的有效凭证。

3)证书过期。

4)接入时间可疑。指标由t_L，t_R以及t_W确定，如式(2)所示。

$$UB_4=s*A+2*\min\left[0.5,(1-s)\frac{t_L-t_R}{t_W-t_R}\right] \tag{2}$$

其中，s 表示该用户在下班时刻是否依旧保持登录状态，s 为 1 表示是，s 为 0 表示否。A 表示该用户是否在非工作段内进行了接入行为，A 为 1 表示是，A 为 0 表示否。式(2)通过 s 和 A 综合考虑工作人员在非工作期间进行加班的特殊情况，下班时注销账号的用户在非工作时间段接入是可疑的。

5)一次性密码验证方式改变。一次性密码验证方式由身份认证系统进行实时反馈。

6)使用非加密传输协议。

7)已登录账号重复登录。BMD-DG 会在接入者每次成功接入时从身份认证系统获取反馈回来的用户信息，用于在处理下次接入请求时判断用户是否发生重复登录。重复登录行为可能预示着攻击者在对已登录的合法用户进行密码爆破。

8)更换设备登录。

9)数据流非相关。将一定时间内具有一定关联性的所有数据包组成的集合称为数据流，这可以帮助我们按照源头对流量进行初步分类。将源 IP 在同一网段内的数据流称为数据流F^i_{ip}；类似地，定义了源 MAC 相同的数据流F^i_{mac}。$F^i_{\text{ip}}=F^i_{\text{mac}}$时$UB_9$为 0，否则为 1。

为了方便第 4 章的展开，表 3 列出了所有建模后的可疑行为。

表 3 可疑行为

Table 3 Suspicious behaviors

序号	可疑行为名称	符号	取值范围
1	接入地点非法	UB_1	0 或 1
2	证书频繁更新	UB_2	[0,1]
3	证书过期	UB_3	0 或 1
4	接入时间可疑	UB_4	[0,1]
5	一次性密码验证方式改变	UB_5	0 或 1
6	使用非加密传输协议	UB_6	0 或 1
7	已登录账号重复登录	UB_7	0 或 1
8	更换设备登录	UB_8	0 或 1
9	数据流非相关	UB_9	0 或 1

3.2 有害行为建模

有害行为指那些会直接造成实际危害的反常行为，用HB_i表示，且指标值为 1 时表示对应行为存在，为 0 时表示不存在。有害行为包括：

1)证书缺失。

2)凭证验证次数过多。HB_2 由凭证验证比率 $Ratio\_PVT$ 确定,如式(3)所示。

$$HB_2=\begin{cases}1, & Ratio\_PVT>p_k\\ 0, & Ratio\_PVT\leqslant p_k\end{cases} \tag{3}$$

其中,$Ratio\_PVT$ 由式(4)确定。

$$Ratio\_PVT=\min\left(\frac{\sum_1^T i}{\sum_1^5 j},1\right) \tag{4}$$

其中,T 表示同源请求凭证验证次数,凭证验证次数的上限为5,达到上限时 $Ratio\_PVT$ 达到最大值1。

3)一次性密码验证次数过多。HB_3 由一次性凭证验证次数比率 $Ratio\_OVT$ 确定,如式(5)所示。

$$HB_3=\begin{cases}1, & Ratio\_OVT>o_k\\ 0, & Ratio\_OVT\leqslant o_k\end{cases} \tag{5}$$

其中,$Ratio\_OVT$ 的计算方式如式(6)所示。

$$Ratio\_OVT=\min\left(\frac{\sum_1^{T_o} i}{\sum_1^5 j},1\right) \tag{6}$$

其中,T_o 表示一次性密码验证次数,其上限为5,达到上限时 $Ratio\_OVT$ 达到最大值1。

4)接入请求访问其他端口。访问非法端口的接入请求有可能是攻击者的端口扫描行为。

5)接入过程使用白名单之外的加密传输协议。

6)单数据包长度异常。如果某个接入请求的数据包过长或过短都是可疑的,这很有可能暗示着某些攻击行为,例如未经授权访问、恶意文件上传、DDoS攻击或隐蔽通信等。HB_6 由数据包大小与应有值的偏离 L 确定,如式(7)所示。

$$HB_6=\begin{cases}1, & L>L_k\\ 0, & L\leqslant L_k\end{cases} \tag{7}$$

其中,L_k 为阈值,L 则由式(8)确定。

$$L=\min\left(\frac{\beta|L_j-L_l|}{L_l},1\right)+\min\left(\frac{(1-\beta)|L_j-L_s|}{L_s},1\right) \tag{8}$$

其中,$\beta=0$ 时表示相同设备之前没有接入成功的记录,此时比较数据包大小与标准值L_s的距离,若 $\beta=1$,表示该设备之前存在接入成功的记录,此时比较数据包大小与历史接入成功的请求数据包大小L_l。

7)单一来源数据包量过大。HB_7 由数据包数量差距 F 来确定,如式(9)所示。

$$HB_7=\begin{cases}1, & F>F_k\\ 0, & F\leqslant F_k\end{cases} \tag{9}$$

其中,$F=\min(1,\max(0,\frac{f_i-f}{f}))$,$f_i$表示一定时间内数据流 i 包含的数据包数量,F_k表示阈值。

8)数据流内数据包访问端口不同。

有害行为的表示与取值范围如表4所列。

表4 有害行为

Table 4 Harmful Behaviors

序号	有害行为名称	符号	取值范围
1	证书缺失	HB_1	0或1
2	凭证验证次数过多	HB_2	0或1
3	一次性密码验证次数过多	HB_3	0或1
4	接入请求访问其他端口	HB_4	0或1
5	使用白名单外加密传输协议	HB_5	0或1
6	单数据包长度异常	HB_6	0或1
7	单一来源数据包量过大	HB_7	0或1
8	数据流内数据包访问端口不同	HB_8	0或1

4 基于动态贝叶斯博弈的ICN恶意接入行为检测

本章讨论BMD-DG博弈模型以及恶意接入行为检测方法。在本文研究的情景中,接入者分为合法用户和攻击者两类,他们都有可能进行合法或非法的操作,即他们都存在两种选择。基于此原则,我们使用信号博弈来构建BMD-DG博弈模型。定义第 t 次尝试接入时的有害数值为τ_t,其由3.2节中的各类有害行为联合确定,如式(10)所示。

$$\tau_t=HB_1\,|\,HB_2\,|\cdots|\,HB_n \tag{10}$$

信号 $Signal$ 是否有害由τ_t确定,如式(11)所示。

$$Signal=\begin{cases}\text{无害}, & \tau_t=0\\ \text{有害}, & \tau_t=1\end{cases} \tag{11}$$

在进行接入时,BMD-DG对接入者的确切身份并不知情,因此该博弈为不完全信息博弈。通过Harsanyi转换,我们将其转化为一个完全信息的不完美博弈,得到了如图2所示的博弈树。博弈树中的 BA 和 BD 分别表示接入者和BMD-DG的收益,同时用角标 A 和 U 分别表示攻击者和合法用户两类接入者,角标 L 和 S 分别表示接入者的无害接入行为和有害接入行为。防御系统对于接入请求的放行和丢弃分别用 A 和 D 表示。

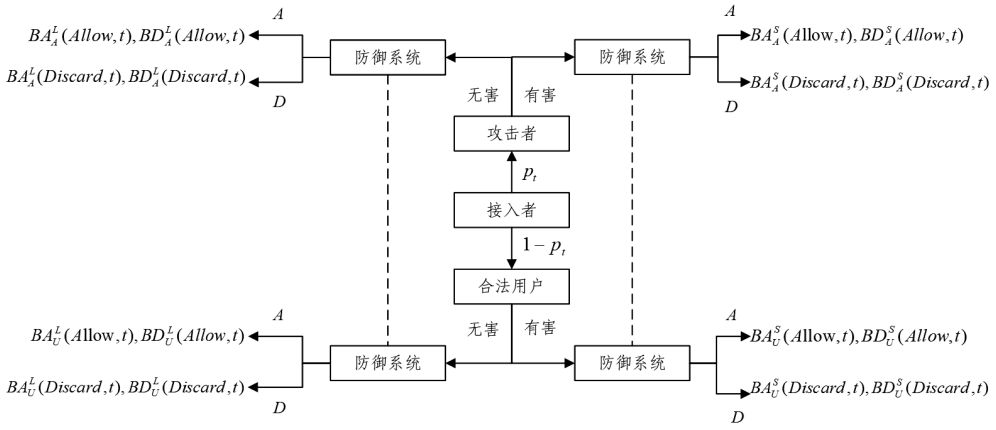


图2 BMD-DG博弈树(1)

Fig. 2 BMD-DG game tree(1)

4.1 博弈信任度模型

本节中讨论 BMD-DG 如何确定两类接入者的信任度。考虑到仅针对单个接入请求进行检测，会因为无法分析整个流的行为而降低检测率，且很难确定博弈的周期，我们针对每个博弈周期 T 内的所有接入请求进行检测，用 t 来表示博弈周期的序号。

将第 t 个博弈周期内接入行为的可疑数值定义为σ_t，其由 3.1 节中的各类可疑行为进行联合确定，如式(12)所示。

$$\sigma_t=\min\left(1,\frac{e^{\sum_1^n UB_i/N_{ub}}}{e^{0.5}}\right) \tag{12}$$

其中，N_{ub} 表示 3.1 节中讨论的可疑行为的总数量。考虑到用户失误操作的偶发性以及小范围性，此处 $\sum_1^n UB_i$ 的值为 N_{ub} 的一半及其以上时将不再存在用户失误操作的可能性。

BMD-DG 在第 t 次博弈中对接入者的信任度为 $(p_t,1-p_t)$，即 BMD-DG 接收到信号时，认为来源是攻击者的可能性为 p_t，是合法用户的可能性为 $1-p_t$。p_t 由可疑数值 σ_t 确定，如式(13)所示：

$$p_t=\lambda\sigma_t+\gamma,p_t\in(0,1] \tag{13}$$

其中，λ 和 γ 均不为 0，通过 λ 和 γ 调整 σ_t 对 p_t 的影响程度。

4.2 收益模型

本节讨论接入者和 BMD-DG 在第 t 次博弈中的收益情况。收益由增益和代价联合确定。

1)各类情况下用户接入的增益

攻击者发送有害信号并被 BMD-DG 放行的增益为 $G_A^S(Allow,t)$，由式(14)确定。

$$G_A^S(Allow,t)=P_t\frac{n}{N} \tag{14}$$

其中，N 代表攻击者采用某种攻击手段接入工业控制网络时需要获得的总进度。每次尝试获得的进度可能不同，因此 n 表示在本轮博弈中获得的平均进度而非具体进度。

接下来，考虑攻击者在第 t 轮博弈中能够推进攻击进度的概率。这个概率与过往累计的攻击进度呈正相关。首先考虑攻击者在第 1 轮博弈中成功接入的概率 P_1 与第 0 轮博弈中成功接入的概率 P_0 之间的关系，如式(15)所示：

$$P_1=P_0\left(k_1\frac{n}{N}+P_0\right)+(1-P_0)P_0=\left(1+k_1\frac{n}{N}\right)P_0 \tag{15}$$

其中，k_1 表示上一次尝试中获得的攻击进度能够为本次尝试提供帮助的大小。

令 $1+k_1\frac{n}{N}=\alpha$，得到在第 t 轮博弈中攻击者能够使攻击进度获得推进的概率 P_t，如式(16)所示：

$$P_t=P_0(1+\alpha+\alpha^2+\cdots+\alpha^t)=\frac{P_0(\alpha^{t+1}-1)}{k_1\frac{n}{N}} \tag{16}$$

进一步得到 $G_A^S(Allow,t)$ 关于初始概率 P_0 的表达，如式(17)所示：

$$G_A^S(Allow,t)=P_t\frac{n}{N}=\frac{P_0(\alpha^t-1)}{k_1} \tag{17}$$

此时对于 BMD-DG 来说，会得到 $-\frac{P_0(\alpha^t-1)}{k_1}$ 的增益。

攻击者发送无害信号并被 BMD-DG 放行的增益 $G_A^S(Allow,t)$ 如式(18)所示：

$$G_A^L(Allow,t)=g \tag{18}$$

其中，g 表示攻击者能够获得的部分信息，这些信息可能会对接下来的攻击产生帮助。此时，对于 BMD-DG 来说，会得到 $-g$ 的增益。

其他情况下，攻击者并不能获得实质上的收益，因此 $G_A^L(Discard,t)=G_A^S(Discard,t)=0$。

对于合法用户来说，接入系统是符合预期的，这并不会对他们带来什么增益，因此：

$G_U^L(Allow,t)=G_U^L(Discard,t)=G_U^S(Allow,t)=G_U^S(Discard,t)=0$。

2)不同选择下的代价

用接入者进行此次操作直到下次操作之前需要耗费的时间表示此次接入操作的代价。用 C_L 来定义攻击者发出无害信号所需要的代价，用 C_s 来定义攻击者发出有害信号所需要的代价。攻击者若想表现得如同合法用户一样无害，需要花费一定时间做准备，因此 $C_L\geqslant C_s$。

t_r 表示合法用户在接入失败时的代价，即合法用户重新进行接入所花费的时间。

k_2t_m 表示 SDN 策略服务器更新流规则所需要的时间，其中 k_2 与有害流量的种类数相关。

将各部分增益与代价代入后的博弈树如图 3 所示。

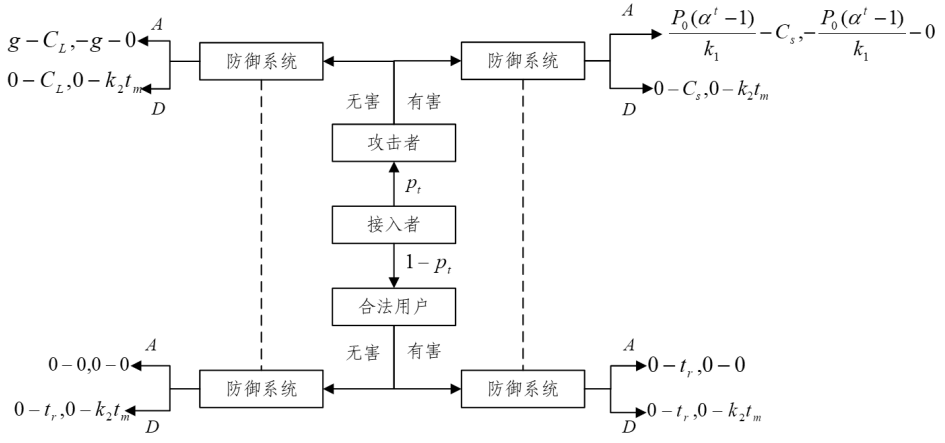


图 3 BMD-DG 博弈树(2)

Fig. 3 BMD-DG game tree(2)

4.3 BMD-DG 博弈分析

本节分析 BMD-DG 博弈模型的均衡条件。为了方便表述，用$[(S_1,S_2),(D_1,D_2)]$表示如下均衡：攻击发出信号 S_1，合法用户发出信号 S_2，对于信号 S_1 和 S_2，BMD-DG 分别做出决策 D_1 和 D_2。其中，接入者能够发出的信号包括有害信号和无害信号，分别用 H 和 U 表示；BMD-DG 能做出的决策包括丢弃和放行，分别用 D 和 A 表示。

定理 1 当满足以下条件时，本博弈达到仅有的唯一分离均衡$[(H,U),(D,A)]$。

①$P_0(\alpha^t-1)\geqslant k_1k_2t_m$

②$g\leqslant C_L-C_S$

证明：

1)BMD-DG 对于攻击者发送的可疑信号，做出放行和丢弃操作的收益分别如式(19)和式(20)所示。

$$u_d(allow)=-\frac{P_0(\alpha^t-1)}{k_1} \tag{19}$$

$$u_d(discard)=-k_2t_m \tag{20}$$

均衡条件下，BMD-DG 须满足$u_d(allow)\leqslant u_d(discard)$，即：

$$P_0(\alpha^t-1)\geqslant k_1k_2t_m \tag{21}$$

攻击者须满足：

$$g\leqslant C_L-C_S \tag{22}$$

2)BMD-DG 对于合法用户发送的合法信号，做出放行和丢弃操作的收益分别如式(23)和式(24)所示。

$$u_d(allow)=0 \tag{23}$$

$$u_d(discard)=-k_2t_m \tag{24}$$

此时，显然$u_d(allow)\geqslant u_d(discard)$，即对于 BMD-DG 已达到均衡条件。又因为合法用户发送有害信号时无论 BMD-DG 做何抉择，合法用户都会得到$-t_r$收益，该值小于(无害，放行)下的收益 0，所以此时攻击者也达到均衡条件。

简单可得，另一分离均衡$[(H,U),(A,D)]$不存在。因此，$P_0(\alpha^t-1)\geqslant k_1\ k_2t_m$且 $g\leqslant C_L-C_S$时，达到此博弈的唯一分离均衡$[(H,U),(D,A)]$。

定理 2 在满足条件③时，达到 BMD-DG 博弈的第一个混同均衡$[(H,H),(D,D),p]$。

$$③p\geqslant\frac{k_1k_2t_m}{P_0(\alpha^t-1)}\ \&\&\ \frac{p}{1-p}\geqslant\frac{k_2t_m}{g}$$

在满足条件④时，达到 BMD-DG 博弈的第二个混同均衡$[(U,U),(D,A),q]$。

$$④\frac{k_2t_m}{g}\geqslant q\geqslant\frac{k_1k_2t_m}{P_0(\alpha^t-1)}$$

证明：

1)证明混同均衡$[(H,H),(D,D),p]$

该情景下，BMD-DG 认为接入者只会发送有害信号，即$\tau_t=1$，此时考虑 BMD-DG 的最优决策，选择放行和丢弃操作的期望收益分别如式(25)和式(26)所示：

$$u_d(allow)=p*\left[-\frac{P_0(\alpha^t-1)}{k_1}\right]+(1-p)*0 \tag{25}$$

$$\begin{aligned}u_d(discard)&=p*[-k_2t_m]+(1-p)*(-k_2t_m)\\&=-k_2t_m\end{aligned} \tag{26}$$

为达到均衡，须$u_d(allow)\leqslant u_d(discard)$，即：

$$k_2t_m\leqslant p*\left[\frac{P_0(\alpha^t-1)}{k_1}\right] \tag{27}$$

此时由于收益信息为公共知识，因此接入者在知道此时 BMD-DG 的最优决策为丢弃的情况下应满足发送有害信号的收益大于无害信号的收益。此时，考虑以下两种情形。

(1)如果 BMD-DG 对合法者的反应为放行，则：

$$g-C_L\leqslant 0-C_s \tag{28}$$

$$0\leqslant 0-t_r(\text{显然不成立}) \tag{29}$$

(2)如果 BMD-DG 对合法者的反应为丢弃，则：

$$0-C_L\leqslant 0-C_s(\text{显然成立}) \tag{30}$$

$$0-t_r\leqslant 0-t_r(\text{显然成立}) \tag{31}$$

要使得(H,H)为均衡，BMD-DG 对合法者的决策必须是丢弃，即均衡下 BMD-DG 的策略为(D,D)。此时在对接入者发送合法信号时，BMD-DG 选择放行和丢弃的收益分别如式(32)和式(33)所示：

$$u_d(allow)=p*(-g)+(1-p)*0 \tag{32}$$

$$\begin{aligned}u_d(discard)&=p*0+(1-p)*(-k_2t_m)\\&=(1-p)*(-k_2t_m)\end{aligned} \tag{33}$$

若 BMD-DG 达到均衡条件，须满足$u_d(allow)\leqslant u_d(discard)$，即：

$$\frac{p}{1-p}\geqslant\frac{k_2t_m}{g} \tag{34}$$

综上，当 $p\geqslant\frac{k_1k_2t_m}{P_0(\alpha^t-1)}$且$\frac{p}{1-p}\geqslant\frac{k_2t_m}{g}$时，达到混同均衡$[(H,H),(D,D),p]$。

2)证明混同均衡$[(U,U),(D,A),q]$

该情景下，BMD-DG 认为接入者只会发送无害信号，即$\tau_t=0$，具体的证明方式与混同均衡$[(H,H),(D,D),p]$的证明方式类似。

4.4 恶意接入行为检测方法

本节利用 BMD-DG 的均衡条件，将恶意接入请求与合法接入请求进行区分。

根据定理 1，当攻击者的尝试次数增大时，在某轮博弈中会满足$P_0(\alpha^t-1)>k_1k_2t_m$，此时若 $g\leqslant C_L-C_S$也成立，攻击者就只会发送有害信号，从而 BMD-DG 就能够将攻击者和合法用户区分开来。

根据定理 2，当接入者的可疑行为较少时，会有$\frac{p}{1-p}<\frac{k_2t_m}{g}$，即合法用户不满足条件③。相反，攻击者满足条件③，因为随着攻击尝试的增多，$P_0(\alpha^t-1)$部分会显著增大，且攻击者的可疑行为多于合法用户。因此，随着博弈周期数增大，即使在某轮博弈中两类接入者都发送有害信号，BMD-DG 也能够将攻击者和合法用户进行区分。

根据定理 2，当接入者的可疑行为较多时，会有 $q>\frac{k_2t_m}{g}$，不满足条件④。相反，合法用户满足条件④。因此，在某轮博弈中即使两类接入者都发送无害信号，随着博弈轮数增加，BMD-DG 也能够将攻击者和合法用户进行区分。

5 实验与评估

本章首先介绍 BMD-DG 框架的内部结构，然后通过控制

变量法对 BMD-DG 检测准确率、性能开销等方面进行了测试，并将其与现有的攻击防御模型进行横向比较，最后分析了比较结果。

5.1 实验环境

BMD-DG 结合 SDN 架构进行工作，如图 4 所示。

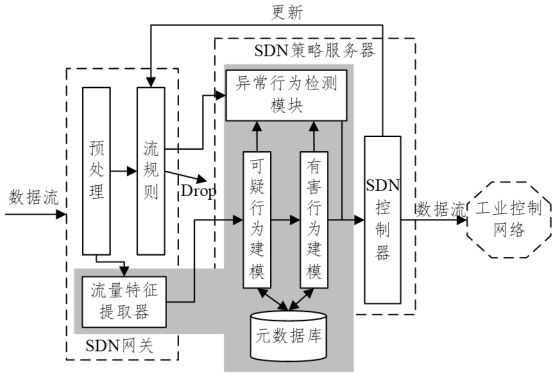


图 4 BMD-DG 架构图

Fig. 4 BMD-DG architecture diagram

BMD-DG 架构为图 4 中深色部分，由位于 SDN 网关的流量特征提取器，以及位于 SDN 策略服务器的 SDN 控制器、异常行为检测模块、可疑行为建模模块、有害行为建模模块和元数据库构成。其中，流量特征提取器提取防火墙监控到的网络层、MAC 层以及协议信息，同时将同源数据流进行归类记录后转发至可疑行为建模模块。

具体实验环境如表 5 所列。

表 5 实验环境

Table 5 Experimental environment

系统指标	版本或参数值
内存	16.0 GB
CPU	Intel(R) Core(TM) i5-10600KF CPU @ 4.10 GHz 4.10 GHz
GPU	NVIDIA GeForce RTX 2060
虚拟机	Ubuntu 18.04.6 LTS
SDN 控制器	OpenDayLight Argon-SR3

5.2 实验设计

本节通过仿真实验对 BMD-DG 框架的准确性、性能进行评估分析。考虑以下 3 种不同的条件。

1）启用现有的安全模型 IoT-IDM[16]；

2）启用现有的安全模型 Three-tier IDPS[17]；

3）启用本研究提出的 BMD-DG 博弈模型。

使用恶意接入检测的正确率、恶意接入流量比例、假阳性率以及防御机制时间开销 4 个指标来评估性能和实验结果。

1）恶意接入检测的正确率S_r如式(37)所示：

$$S_r=\frac{S_n}{S_n+U_n} \tag{37}$$

其中，S_n表示所有成功检测到的恶意接入请求数量，U_n表示未被检测到的恶意接入请求数量。

2）恶意接入流量占所有接入流量的比例HA_r如式(38)所示：

$$HA_r=\frac{HA_n}{HA_n+UA_n} \tag{38}$$

其中，HA_n表示恶意接入请求的总数量，UA_n表示合法接入请求的总数量。

3）恶意流量检测的假阳性率F_r如式(39)所示：

$$F_r=\frac{F_n}{F_n+S_n} \tag{39}$$

其中，F_n表示检测中误报的请求数量。

4）启用安全模型后造成的额外时间开销T_s，单位为 s。

通过分析不同HA_r下的S_r和F_r，可以判断恶意接入流量占比在很小、适中、较大时检测框架的有效性和准确度；通过分析不同接入请求数量下的S_r，F_r以及T_s，可以判断接入请求数量的增大是否会对检测框架的性能造成较大影响，以及性能较现有的安全机制 IoT-IDM 和 Three-tier IDPS 是否有提升。

在实验中，使用分布式互联网流量生成器 DITG[18]创建随机 TCP/IP 流量，并使用 PostMan 发送自定义 HTTPS 数据包模拟合法用户和攻击者的登录行为，从而实现研究中提到的针对工控网络接入场景的 STRIDE 威胁中的 STID4 类攻击。R 类攻击可以通过身份认证机制进行抵御，E 类攻击在身份认证之后发生，因此 R 和 E 两类攻击在此不做讨论。

根据现实中工控网络远程接入场景，以及第 2 章中描述的工控网络接入威胁模型，在 Mininet[19]上构建了包含合法远程接入系统、非法仿冒系统以及工业控制网络的网络拓扑图，如图 5 所示。通过在 Mininet 虚拟主机上运行 python 脚本，模拟了工控网络数据交互行为。其中，c_0表示 OpenDayLight 控制器[20]，同时在 h_5 主机上运行了具有登录认证业务的 web 服务。

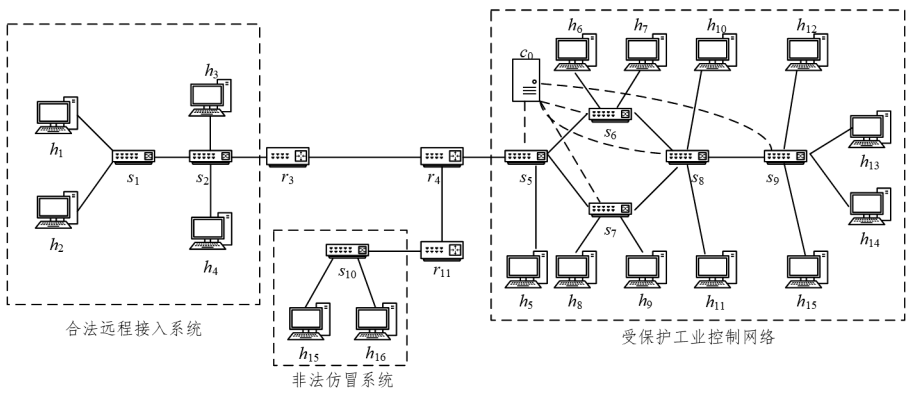


图 5 实验拓扑图

Fig. 5 Experimental topology diagram

持续的仿真实验结果表明，在选取不同参数值的情况下，防御机制在时间达 4 min 之后的检测效果达到平衡状态，因此选取 5 min 作为仿真时间指标的取值，并进行多次仿真实验，选取检测效果最好的博弈参数初始值，如表 6 所列。

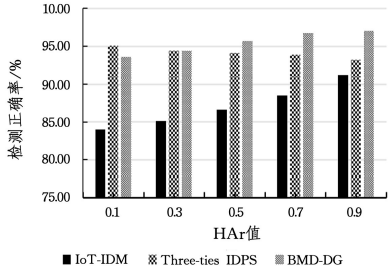
表 6 博弈参数初始值

Table 6 Initial values of game parameters

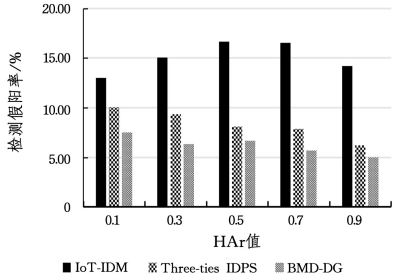
参数	值
λ	0.8
γ	0.2
T	1 200 ms
p_k	0.4
o_k	0.4
k_1	0.1
k_2	0.3
F_k	0.1
L_k	0.1
g	0.2
C_L	0.25
C_s	0.05

5.3 实验结果与分析

本节通过比较 BMD-DG 与 IoT-IDM，Three-tier IDPS 在 3 种场景下的S_r，F_r以及T_s指标，对 BMD-DG 的准确度、性能进行分析。



(a)S_r随HA_r的变化



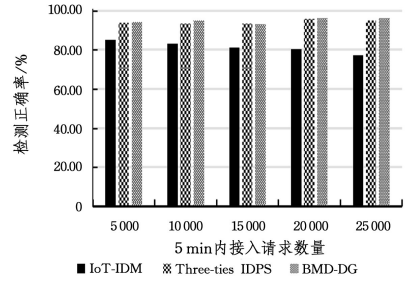
(b)F_r随HA_r的变化

图 6 S_r和F_r随HA_r的变化

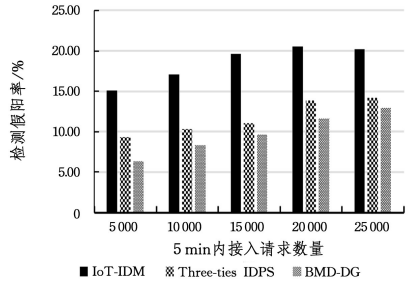
Fig. 6 S_r and F_r change with HA_r

首先，控制仿真阶段内数据包总数为 10 000，改变HA_r，得到的S_r和F_r分别如图 6 所示。结果表明，除了当 Three-tier IDPS 检测正确率最高时($HA_r=0.1$)BMD-DG 的检测正确率比 Three-tier IDPS 低 1.5%，其他情况下 BMD-DG 的检测正确率显著高于其他两个防御机制。随着HA_r的增大，Three-tier IDPS 的检测正确率逐渐下降，在$HA_r=0.9$时 BMD-DG 的检测正确率相比 IoT-IDM 提升了 5.8%，相比 Three-tier IDPS 提升了 3.8%。BMD-DG 的误报率也低于其他两个防御机制，相较于 IoT-IDM 误报率最低的情况($HA_r=0.1$)，BMD-DG 的误报率下降了 5.5%；相较于 Three-tier IDPS 误报率最低的情况($HA_r=0.9$)，BMD-DG 的误报率下降了 1.2%。

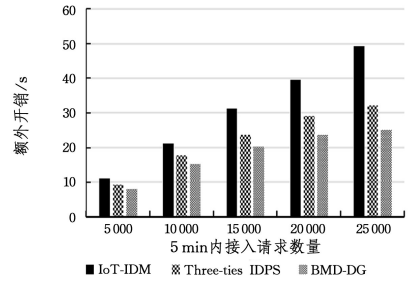
其次，为了观察接入请求数量的增加是否会影响 BMD-DG 的防御效果，控制HA_r为 0.3，通过改变仿真阶段内数据包总数，得到S_r，F_r以及T_s，如图 7 所示。



(a)S_r随接入请求数量的变化



(b)F_r随接入请求数量的变化



(c)T_s随接入请求数量的变化

图 7 S_r，F_r和T_s随接入请求数量的变化

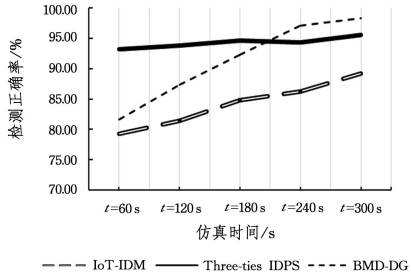
Fig. 7 S_r, F_r and T_s change with the number of access requests

实验结果表明，除了接入请求数量为 15 000 时 BMD-DG 的检测正确率比 Three-tier IDPS 低 0.4%，其他情况下 BMD-DG 的正确率均高于 Three-tier IDPS，且在 IoT-IDM 表现最好的情况(接入请求数量为 5 000)下仍然有 9.1%的优势。BMD-DG 的检测假阳率在不同接入请求的情况下均低于其他两个防御机制，相较于 IoT-IDM 假阳率下降了 7.1%以上，相较于 Three-tier IDPS 假阳率下降了 1.2%以上。检测效率方面，随着接入请求数量的增加，BMD-DG 的额外开销涨幅逐渐减小，这是因为 BMD-DG 能够借助 SDN 控制器对流表进行实时更新来避免处理来源相似的恶意请求，从而降低了接入请求数量暴增对防御效果的影响。BMD-DG 相较于 Three-tier IDPS 的额外时间开销下降了 27.4%以上，相较于 Three-tier IDPS 的额外时间开销下降了 14.7%以上。

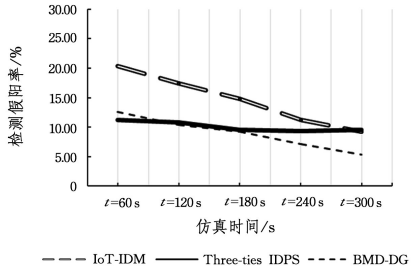
最后，为了检验多轮迭代是否能够提高博弈效果，控制HA_r指标为 0.3，仿真阶段内数据包总数为 10 000，观测S_r和

F_r随观测时间变化的结果，如图 8 所示。

实验结果表明，随着博弈轮数的增加，BMD-DG 的检测效果越来越好，在 240s 之后检测正确率能稳定在 95%以上，相较于 IoT-IDM 提升了 10.9%，相较于 Three-tier IDPS 提升了 2.8%；并且误报率随着博弈轮数的增加也显著降低。这是因为每一轮博弈都会为下一轮博弈提供参考信息，从而在一定程度上修正博弈参数，使得博弈更加适应恶意情境。



(a)S_r随观测时间的变化



(b)F_r随观测时间的变化

图 8 S_r和F_r随观测时间的变化

Fig. 8 S_r and F_r change with observation time

综上，相比于 IoT-IDM 和 Three-tier IDPS，BMD-DG 在检测准确率和性能方面表现出色，能够很好地适应工业控制网络远程接入过程中对高准确性、动态实时性和低延迟的要求。

结束语 本文提出了一种基于动态贝叶斯博弈的工业控制网络恶意接入识别框架，该框架能够在接入者进行用户认证之前，通过分析进入网络的流量数据，对恶意接入请求进行识别和阻断。在 Mininet 上对真实的网络拓扑进行了模拟，基于 OpenDayLight 控制器，使用 DITG，PostMan 和 Hydra 等工具对工控网络远程接入场景下的各类威胁进行了模拟，通过与现有的安全防御机制进行比较，证明了 BMD-DG 在检测准确率、检测效率方面具有较为明显的优势。

目前工作中仍存在一些不足点，包括行为建模和实验方案两方面。

1)可疑行为和有害行为建模部分涵盖的行为不够丰富，这可能会影响框架的检测效果。

2)实验设计部分采用单一仿真方案进行，而未使用其他实验方法进行对照，可能对实验结果的准确性产生一定影响。

在未来的研究工作中会将重心放在丰富各类可疑、有害行为的建模和分析上，并将该框架实施在不同的真实工控网络场景中以验证和完善其功能。

参 考 文 献

[1] DORASWAMY B，KRISHNA K L. A Deep Learning Approach for Anomaly Detection in Industrial Control Systems[C]// 2022 International Conference on Augmented Intelligence and Sustainable Systems(ICAISS). IEEE，2022：442-448.

[2] MUBARAK S，HABAEBI M H，ISLAM M R，et al. ICS cyber attack detection with ensemble machine learning and dpi using cyber-kit datasets[C]// 2021 8th International Conference on Computer and Communication Engineering (ICCCE). IEEE，2021：349-354.

[3] YOUM S，KIM Y K，SHIN K S，et al. An authorized access attack detection method for realtime intrusion detection system [C]// 2020 IEEE 17th Annual Consumer Communications & Networking Conference(CCNC). IEEE，2020：1-6.

[4] OUYANG Y，LI B，KONG Q，et al. FS-IDS：a novel few-shot learning based intrusion detection system for scada networks [C]// IEEE International Conference on Communications. IEEE，2021：1-6.

[5] FERDIANA R. Performance of Intrusion Detection System Using Bagging Ensemble with SDN-BaseClassifier[C]// 2022 IEEE 7th International Conference on Information Technology and Digital Applications(ICITDA). IEEE，2022：1-7.

[6] SEBOPELO R，ISONG B，GASELA N，et al. A review of intrusion detection techniques in the SDN environment[C]// 2021 3rd International Multidisciplinary Information Technology and Engineering Conference(IMITEC). IEEE，2021：1-9.

[7] FERDIANA R. New Approach of Ensemble Method to Improve Performance of IDS using S-SDN Classifier[C]// 2022 IEEE International Conference on Communication，Networks and Satellite(COMNETSAT). IEEE，2022：463-468.

[8] FAUSTO A，GAGGERO G，PATRONE F，et al. Reduction of the Delays Within an Intrusion Detection System(IDS) Based on Software Defined Networking (SDN)[J]. IEEE Access，2022，10：109850-109862.

[9] BURCH Z C. Credential Theft Powered Unauthorized Login Detection through Spatial Augmentation[D]. Virginia Tech，2018.

[10] KUNIMOTO M，OKUBO T. Analysis and Consideration of Detection Methods to Prevent Fraudulent Access by Utilizing Attribute Information and the Access Log History[J]. Journal of Information Processing，2023，31：602-608.

[11] LIU P，LIU Y，WANG X，et al. Channel-state-based fingerprinting against physical access attack in industrial field bus network [J]. IEEE Internet of Things Journal，2021，9(12)：9557-9573.

[12] PASHAEI A，AKBARI M E，LIGHVAN M Z，et al. Improving the IDS performance through early detection approach in local area networks using industrial control systems of honeypot [C]// 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe). IEEE，2020：1-5.

[13] CHAVEZ A，LAI C，JACOBS N，et al. Hybrid intrusion detection system design for distributed energy resource systems [C]// 2019 IEEE CyberPELS(CyberPELS). IEEE，2019：1-6.

[14] ZHANG Z X，ZONG X J，HE K，et al. Research on Abnormal

Traffic Detection in Industrial Control Network Based on CVAE-CatBoost[J]. Computer Engineering, 2023, 49(5): 173-180.

[15] LI S M, ZHANG Y H, WANG Y H, et al. Semi-quantitative Information Industry Control Heterogeneous Network Security Assessment[J]. Journal of Chinese Computer Systems, 2024, 45(5): 1218-1227.

[16] NOBAKHT M, SIVARAMAN V, BORELI R. A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow[C]// 2016 11th International Conference on Availability, Reliability and Security(ARES). IEEE, 2016: 147-156.

[17] ALI A, YOUSAF M M. Novel three-tier intrusion detection and prevention system in software defined network[J]. IEEE Access, 2020, 8: 109662-109676.

[18] SALAM R, BHATTACHARYA A. Performance evaluation of SDN architecture through D-ITG platform for distributed controller over single controller[C]// 2021 12th International Conference on Computing Communication and Networking Technologies(ICCCNT). IEEE, 2021: 1-6.

[19] KAUR K, SINGH J, GHUMMAN N S. Mininet as software defined networking testing platform[C]// International Conference on Communication, Computing & Systems(ICCCS). 2014: 139-142.

[20] BADOTRA S, SINGH J. Open Daylight as a Controller for Software Defined Networking[J]. International Journal of Advanced Research in Computer Science, 2017, 8(5): 1105-1111.

LIU Haohan, born in 1998, postgraduate. His main research interest is Internet of Things security.

CHEN Zemao, born in 1975, Ph.D, professor. His main research interests include information system security, trusted computing and equipment information security.

(责任编辑:柯颖)