文章编号:1671-251X(2018)11-0075-05 DOI:10.13272/j.issn.1671-251x.2018050036

煤矿企业工业控制系统入侵检测算法

吴开兴[1,2], 王文鼎[1,2], 李丽宏[1]

(1.河北工程大学 信息与电气工程学院,河北 邯郸 056000;
2.煤矿综合信息化河北省工程实验室,河北 邯郸 056000)

摘要:针对现有煤矿企业工业控制系统入侵检测算法未考虑防御因素影响、实现复杂等问题,从攻击进程和防御体系 2 个方面,提出了一种基于攻防树模型的煤矿企业工业控制系统入侵检测算法。首先,通过对攻击叶节点的攻击属性进行量化并构建指标体系得到攻击叶节点被攻击概率,进而得出攻击路径的入侵成功率,并结合攻击路径的入侵回报率得到攻击路径的入侵概率;然后,引入基于漏报率和误报率的入侵报警率,得到被动防御概率,通过漏洞发现率和漏洞修复率得到主动防御概率;最后,根据攻击路径的入侵概率、被动防御概率和主动防御概率,得出攻击路径最终入侵概率。实例结果表明,该算法能有效检测煤矿企业工业控制系统入侵概率,提高入侵检测的准确性。

关键词:煤矿网络安全;工业控制系统;入侵检测;攻防树模型;攻击进程;防御体系
中图分类号:TD67 文献标志码:A
网络出版地址:http://kns.cnki.net/kcms/detail/32.1627.TP.20181026.1500.009.html

Intrusion detection algorithm for industrial control system of coal mine enterprise

WU Kaixing[1,2], WANG Wending[1,2], LI Lihong[1]

(1.School of Information and Electrical Engineering, Hebei University of Engineering, Handan 056000, China; 2.Hebei Engineering Laboratory of Coal Mine Comprehensive Informatization, Handan 056000, China)

Abstract: In view of problems that existing intrusion detection algorithms for industrial control system (ICS) of coal mine enterprise failed to consider impact of defense factors and complexity of implementation, from two aspects of attack process and defense system, an intrusion detection algorithm for ICS of coal mine enterprise based on attack-defense tree model was proposed. Firstly, probability of attack leaf node being attacked is obtained by quantifying attack attribute of the attack leaf node and constructing index system, then intrusion success rate of attack path can be obtained, and intrusion probability of the attack path is obtained by combining the intrusion success rate and intrusion return rate of the attack path. Then, intrusion alarm rate based on false negative rate and false positive rate is introduced to obtain passive defense probability. Active defense probability is obtained through bug discovery rate and bug repair rate. Finally, final intrusion probability of the attack path is obtained according to the intrusion probability of the attack path, the passive defense probability and the active defense probability. The example results show that the algorithm can effectively detect ICS intrusion

收稿日期:2018-05-11;**修回日期**:2018-10-08;**责任编辑**:盛男。
基金项目:河北省自然科学基金资助项目(F2015402150)。
作者简介:吴开兴(1962—),男,陕西渭南人,教授,硕士,主要研究方向为信息安全、煤矿综合信息化,E-mail:1527110726@qq.com。通信作者:王文鼎(1992—),男,河北邯郸人,硕士研究生,主要研究方向为工业信息安全,E-mail:920176189@qq.com。
引用格式:吴开兴,王文鼎,李丽宏.煤矿企业工业控制系统入侵检测算法[J].工矿自动化,2018,44(11):75-79.
WU Kaixing, WANG Wending, LI Lihong. Intrusion detection algorithm for industrial control system of coal mine enterprise[J]. Industry and Mine Automation, 2018, 44(11): 75-79.

probability of coal mine enterprise with higher accuracy of intrusion detection.

Key words: coal mine network security; industrial control system; intrusion detection; attack-defense tree model; attack process; defense system

0 引言

煤矿企业工业控制系统(Industrial Control System,ICS)发生的入侵事件逐年增加,准确地检测入侵是煤矿企业 ICS 安全运行的重要前提和保障[1-3]。Ru Yeqi 等[4]通过攻击树模型模拟攻击进程,得出攻击进程中的入侵概率,但未考虑防御因素的影响;Chen Ying 等[5]提出了一种基于马尔科夫决策过程模型的 ICS 入侵检测算法,但存在模型构建复杂的缺点。攻防树模型由攻击树模型和防御树模型改进而来[6-7],具有实现简单的特点。因此,本文提出了一种基于攻防树模型的煤矿企业 ICS 入侵检测算法,该算法从攻击进程和防御体系 2 个方面来考虑,能提高入侵检测的准确性。

1 攻防树模型

攻防树模型中包含根节点、中间节点、攻击叶节点和防御叶节点 4 类节点[8]。该模型分为攻击进程和防御体系 2 个部分:攻击进程是利用逻辑门的"或"门和"与"门进行连接,"与"表示同层攻击叶节点或中间节点必须全部被攻破才能向根节点移动 1 层,"或"表示同层攻击叶节点或中间节点中只要有 1 个攻击叶节点或中间节点被攻破,便可向根节点移动 1 层;防御体系是指当攻击叶节点被攻击时,对应的防御叶节点采取相应的解决对策。

2 基于攻防树模型的 ICS 入侵检测算法

基于攻防树模型的 ICS 入侵检测算法流程如图 1 所示。

2.1 攻击进程

2.1.1 攻击叶节点攻击属性指标体系

常见的攻击属性[9]主要分为攻击者水平、攻击被检测到的概率和攻击频率。

(1) 攻击者水平。攻击者水平的高低取决于攻击者窃取 ICS 权限的大小,被窃取的权限越大,说明攻击者水平越高。参考文献[10]中的评判标准,被窃取的权限从小到大依次为无权限、非授权访问权限、普通用户权限、管理员权限和超级管理员权限 5 个级别,分别对应攻击者水平很低、低、一般、高、很高 5 个等级。

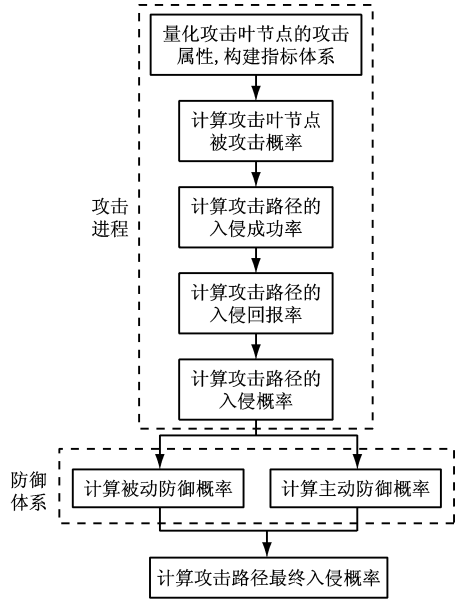

图 1 基于攻防树模型的 ICS 入侵检测算法流程

Fig. 1 Flow of ICS intrusion detection algorithm based on attack-defense tree model

(2) 攻击被检测到的概率。攻击被检测到的概率与 ICS 中部署的防护措施(如防火墙等)有关。工业防火墙技术由数据包过滤技术、状态包检测技术、代理服务技术和应用网管技术组成。当攻击分别被 4,3,2,1 种技术检测出来或没有被任何一种技术检测出来时,攻击被检测到的概率分别设定为很容易、容易、一般、难、很难。

(3) 攻击频率。参考文献[11]中的评判标准,当攻击者对 ICS 发动攻击次数分别为平均每周、每月、每半年、每年至少 1 次或攻击者 1 a 都未对 ICS 发动攻击,攻击频率分别设定为很高、高、一般、低、很低。

依据 3 种常见的攻击属性并结合德尔菲法[12],得出量化的攻击叶节点攻击属性。其指标体系见表 1。

2.1.2 攻击叶节点被攻击概率

采用多属性效用理论将攻击叶节点攻击属性转换为效用值,则攻击叶节点 N 被攻击概率为

$$P(N) = w_z U(z) + w_d U(d) + w_r U(r) \quad (1)$$

式中:w_z,w_d,w_r 分别为攻击者水平、攻击被检测到的概率和攻击频率 3 种攻击属性的加权系数,$w_z + w_d + w_r = 1$[4];$U(z)$,$U(d)$,$U(r)$分别为 3 种攻击属性的效用值;z为攻击攻击叶节点N的攻击者水

表 1　攻击叶节点攻击属性指标体系

Table 1　Attack attribute index system of attack leaf node

攻击者水平		攻击被检测到的概率		攻击频率	
选项	等级	选项	等级	选项	等级
很高	5	很容易	5	很高	5
高	4	容易	4	高	4
一般	3	一般	3	一般	3
低	2	难	2	低	2
很低	1	很难	1	很低	1

平;d 为攻击攻击叶节点 N 被检测到的概率;r 为攻击叶节点 N 被攻击次数。

2.1.3　攻击路径的入侵成功率

攻击路径是指向根节点攻击进程中一系列攻击叶节点 $N_1,N_2,\cdots,N_n$ 的有序集合,攻击路径的入侵成功率为

$$P_{\text{suc}} = P(N_1)P(N_2)\cdots P(N_n) \tag{2}$$

式中 $P(N_1),P(N_2),P(N_n)$ 分别为攻击叶节点 $N_1,N_2,\cdots,N_n$ 被攻击的概率。

2.1.4　攻击路径的入侵回报率

入侵回报率可表示为

$$P_{\text{ret}} = \frac{\sum_{q=1}^{m} R_q - \sum_{q=1}^{m} C_q}{\sum_{q=1}^{m} R_q} \times 100\% \tag{3}$$

式中:$R_q(q=1,2,\cdots,m,m$ 为攻击路径数量)为入侵收益,即攻击者通过攻击 ICS 获得的收益,本文设定每条攻击路径的入侵收益为 1;C_q 为入侵成本,即发动 1 次入侵所需成本,不同入侵类型[10]的入侵成本见表 2。

表 2　不同入侵类型的入侵成本

Table 2　Intrusion cost of different intrusion types

入侵类型	描述	入侵成本
Root	获取管理员权限	1.00
User	获取普通用户权限	0.50
Data	非授权访问或读写数据	0.30
Dos	拒绝服务攻击	0.20
Probe	扫描	0.05

2.1.5　攻击路径的入侵概率

根据式(2)和式(3),可得攻击路径的入侵概率为

$$P_{\text{att}} = P_{\text{suc}}P_{\text{ret}} \tag{4}$$

2.2　防御体系

当 ICS 受到攻击或存在潜在威胁时,ICS 会做出相应的防御措施,分为被动防御和主动防御。

2.2.1　被动防御概率

被动防御是指当攻击者破解 ICS 中漏洞时,根据防御者收集的信息进行及时修补。被动防御概率为

$$P_{\text{pass}} = \alpha_{\text{D}}P(I|A) \tag{5}$$

式中:α_{D} 为防御者动作,$\alpha_{\text{D}}=0$ 时未采取动作,$\alpha_{\text{D}}=1$ 时采取动作;$P(I|A)$为入侵报警率。

$$P(I|A) = \frac{P(I)P(A|I)}{P(I)P(A|I)+P(\bar{I})P(A|\bar{I})+P(I)P(\bar{A}|I)} \tag{6}$$

式中:I,A 分别为入侵事件和报警事件;$P(I)$为发生入侵事件的概率;$P(A|I)$为发生入侵事件时发生报警事件的条件概率;$P(\bar{I})$为未发生入侵事件的概率,$P(\bar{I})=1-P(I)$;$P(A|\bar{I})$为误报率,即未发生入侵事件时发生报警事件的概率;$P(\bar{A}|I)$为漏报率,即发生入侵事件时未发生报警事件的概率。

2.2.2　主动防御概率

主动防御就是在入侵行为对 ICS 发生影响之前,能够及时精准预警。主动防御概率为

$$P_{\text{act}} = P_{\text{I}}P_{\text{II}} \tag{7}$$

式中 $P_{\text{I}},P_{\text{II}}$分别为漏洞发现率和漏洞修复率。

$$P_{\text{I}} = \frac{H_{\text{v}}-H_{\text{j}}}{H_{\text{cv}}-H_{\text{j}}} \tag{8}$$

$$P_{\text{II}} = \alpha_{\text{D}}\exp(P_{\Delta t}) \tag{9}$$

式中:H_{v} 为 ICS 中存在的漏洞数;H_{j} 为攻击者发现的漏洞数;H_{cv}为公共漏洞数;$P_{\Delta t}$为防御者在 Δt 时间内修复漏洞的概率。

2.3　攻击路径最终入侵概率

攻击路径最终入侵概率[13]为

$$P_{\text{fin}} = P_{\text{att}} + P_{\text{act}} + P_{\text{pass}} \tag{10}$$

3　案例分析

根据某煤矿企业 ICS 构建攻防树模型,如图 2 所示,其中节点属性见表 3。

对攻击叶节点的攻击属性进行量化和归一化处理(设加权系数 $w_z=0.6,w_d=0.3,w_r=0.1$),得出攻击叶节点攻击属性指标体系和被攻击概率,见表 4。

依据表 4 和式(2)—式(4)可计算出攻击路径的入侵成功率、入侵回报率、入侵概率,见表 5。

煤矿企业 ICS 近 3 000 条报警事件中,误报事件 54 件,漏报事件 421 件,通过式(5)、式(6)得出被动防御概率,见表 6。

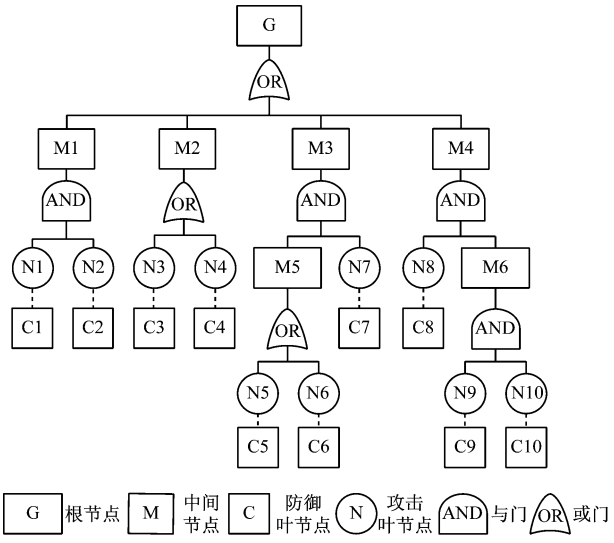

图 2 煤矿企业 ICS 攻防树模型

Fig. 2 Attack-defense tree model of coal mine enterprise ICS

表 3 节点属性

Table 3 Node attribute

节点	属性	节点	属性
G	通过攻击发送错误信息，使 ICS 瘫痪	N8	截取测量或状态数据包
M1	通过前端发送信号	N9	在网络中窃听信息
M2	在 ICS 中可以访问人机界面	N10	破解消息的加密算法
M3	获得身份信息认证	C1	传统 IT 防火墙
M4	影响状态估计模块	C2	专业的工业防火墙
M5	连接数据库服务器	C3	部署严密的网络监控
M6	注入虚假数据	C4	隔离工程师站、先控站
N1	扫描控制中心历史服务器	C5	隔离工程师站、先控站
N2	获得控制中心应用服务器	C6	隔离工程师站、先控站
N3	ICS 共享服务器	C7	隔离工程师站、先控站
N4	本地 ICS 访问权限	C8	部署严密的网络监控
N5	Web 服务器访问权限	C9	部署严密的网络监控
N6	FTP 服务器访问权限	C10	系统安全测试
N7	数据库服务器访问权限		

依据煤矿企业 ICS 实际情况，设定 $H_v=200$，$H_j=30$，$H_{cv}=6\ 787$，$P_{\Delta t}=0.004$。将数据代入式(7)—式(9)，可得主动防御概率 $P_{act}\approx0.044$。

根据式(10)，得出攻击路径最终入侵概率，见表 7。

将表 7 数据用曲线形式表示，并与文献[4]中基于攻击树模型的入侵检测算法得到的入侵概率和实际的入侵概率进行对比，如图 3 所示。可看出本文算法更接近实际的入侵概率，与文献[4]算法相比，提高了入侵检测准确性。

表 4 攻击叶节点攻击属性指标体系和被攻击概率

Table 4 Attack attribute index system and being attacked probability of attack leaf node

攻击叶节点	攻击者水平	攻击被检测到的概率	攻击频率	被攻击概率/%
N1	4	5	3	21.30
N2	5	5	3	18.00
N3	3	3	5	29.50
N4	4	3	4	27.50
N5	2	2	4	47.50
N6	3	2	4	37.50
N7	4	2	4	32.50
N8	3	4	2	32.50
N9	2	2	3	48.30
N10	2	3	1	50.00

表 5 攻击路径的入侵成功率、入侵回报率和入侵概率

Table 5 Intrusion success rate, intrusion return rate and intrusion probability of attack path

序号	攻击路径	入侵成功率/%	入侵成本	入侵收益	入侵回报率/%	入侵概率/%
1	N1N2	6.0	0.35	1	65	3.90
2	N3	32.7	0.30	1	70	22.90
3	N4	28.8	0.50	1	50	14.40
4	N5N7	15.9	0.80	1	20	3.18
5	N6N7	14.7	0.80	1	20	2.90
6	N8N9N10	8.1	0.90	1	10	0.81

表 6 被动防御概率

Table 6 Passive defense probability

序号	攻击路径	被动防御概率/%
1	N1N2	2.30
2	N3	18.50
3	N4	11.40
4	N5N7	1.78
5	N6N7	2.30
6	N8N9N10	0.06

4 结语

提出了一种基于攻防树模型的煤矿企业 ICS 入侵检测算法。首先，通过对攻击叶节点的攻击属

表 7　攻击路径最终入侵概率

Table 7　Final intrusion probability of attack path

序号	攻击路径	最终入侵概率/%
1	N1N2	10.60
2	N3	45.80
3	N4	30.20
4	N5N7	9.36
5	N6N7	9.60
6	N8N9N10	1.31

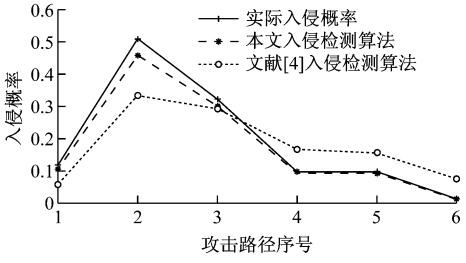

图 3　不同算法下入侵概率对比

Fig. 3　Comparison of intrusion probability under different algorithms

性进行量化并构建指标体系得到攻击叶节点被攻击的概率,进而得出攻击路径的入侵成功率,并结合攻击路径的入侵回报率得到攻击路径的入侵概率;然后,引入基于漏报率和误报率的入侵报警率,得到被动防御概率,通过漏洞发现率和漏洞修复率得到主动防御概率;最后,根据攻击路径的入侵概率、被动防御概率和主动防御概率,得出攻击路径最终入侵概率。结果表明,该算法能有效检测煤矿企业 ICS 入侵概率,具有较高的准确性。

参考文献(References):

[1] 潘瑜. 基于网络的煤矿信息系统安全研究[J]. 工矿自动化,2005,31(4):28-31.
PAN Yu. The security study of coal mine information system based on computer network[J]. Industry and Mine Automation,2005,31(4):28-31.

[2] 彭勇,江常青,谢丰,等. 工业控制系统信息安全研究进展[J]. 清华大学学报(自然科学版),2012,52(10):1396-1408.
PENG Yong, JIANG Changqing, XIE Feng, et al. Industrial control system cybersecurity research[J]. Journal of Tsinghua University (Science and Technology),2012,52(10):1396-1408.

[3] CHERDANTSEVA Y, BURNAP P, BLYTH A, et al. A review of cyber security risk assessment methods for SCADA systems[J]. Computers & Security,2016,56:1-27.

[4] RU Yeqi, WANG Yufei, LI June, et al. Risk assessment of cyber attacks in ECPS based on attack tree and AHP [C]//The 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, Changsha,2016:465-470.

[5] CHEN Ying, HONG J, LIU C C. Modeling of intrusion and defense for assessment of cyber security at power substations[J]. IEEE Transactions on Smart Grid,2018,9(4):2541-2552.

[6] KORDY B, PIETRE L, SCHWEITZER P. DAG-based attack and defense modeling: don't miss the forest for the attack trees[J]. Computer Science Review,2014,13/14:1-38.

[7] ARGHAVANI A, ARGHAVANI M, AHMADI M, et al. Attacker-manager game tree (AMGT): a new framework for visualizing and analysing the interactions between attacker and network security manager[J]. Computer Networks,2018,133:42-58.

[8] 付钰,俞艺涵,陈永强,等. 基于攻防行为树的网络安全态势分析[J]. 工程科学与技术,2017,49(2):115-120.
FU Yu, YU Yihan, CHEN Yongqiang, et al. Network security analysis situation on attack-defense behavior tree[J]. Advanced Engineering Science,2017,49(2):115-120.

[9] 黄家辉,冯冬芹,王虹鉴. 基于攻击图的工控系统脆弱性量化方法[J]. 自动化学报,2016,42(5):792-798.
HUANG Jiahui, FENG Dongqin, WANG Hongjian. A method for quantifying vulnerability of industrial control system based on attack graph[J]. Acta Automatica Sinica,2016,42(5):792-798.

[10] 姜伟,方滨兴,田志宏,等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报,2009,32(4):817-827.
JIANG Wei, FANG Binxing, TIAN Zhihong, et al. Evaluating network security and optimal active defense based on attack - defense game model[J]. Chinese Journal of Computers,2009,32(4):817-827.

[11] GB/T 33009.3—2016 工业自动化和控制系统网络安全集散控制系统(DCS) 第 3 部分:评估指南[S].

[12] OKOLI C, PAWLOWSKI S D. The Delphi method as a research tool: an example, design considerations and applications[J]. Information & Management,2004,42(1):15-29.

[13] 刘菲菲. 流程工业数据驱动报警分析[D]. 北京:北京化工大学,2015.