基于 TLS 的变电站通信网络安全攻防策略生成方法*

陈　刚[1],李　岩[2],赵　轩[1],王文华[1],付同福[1],黄照厅[1],张礼波[1]
(1. 贵州电网六盘水供电局,贵州六盘水 553000;
2. 武汉映瑞电力科技有限公司,武汉 430074)

摘　要: 针对变电站通信网络受到攻击时,安全攻防策略生成时间较长、持续性较差的问题,为满足变电站通信网络安全需求,基于 TLS 研究变电站通信网络安全攻防策略生成方法。为了保障变电站通信网络中数据传输的安全性与完整性,设计符合变电站高实时性的安全传输层协议(TLS),以此为基础,分析变电站通信网络安全攻防竞争过程,构建攻防概率模型,以构建模型为依据模拟攻防双方的竞争过程,求解不同状态下攻防双方的最佳策略,从而实现了变电站通信网络安全攻防策略的生成。实验结果显示:在不同的攻击行为下,与对比方法相比较,提出方法的防御策略生成时间更短在 1.545 7 s 以下、有效时间更长最高达 28.43 s,安全攻防行为判断准确性在 93.8% 以上,充分验证了提出方法具备可行性。

关键词: TLS; 变电站; 通信网络; 安全; 攻防策略
中图分类号: TP29　　**文献标识码:** A　　DOI **编码:** 10.14016/j.cnki.1001-9227.2021.07.046

Generation method of substation communication network security attack and defense strategy based on TLS

CHEN Gang[1],LI Yan[2],ZHAO Xuan[1],WANG Wenhua[1],FU Tongfu[1],HUANG Zhaoting[1],ZHANG Libo[1]
(*1. Liupanshui Power Supply Bureau of Guizhou Power Grid Co. LTD,Liupanshui Guizhou 553000,China;*
2. Wuhan INRE Power Technology Co. LTD,Wuhan 430074,China)

Abstract: Aiming at the problem that the generation time of security attack and defense strategy is long and the persistence is poor when substation communication network is attacked,in order to meet the security requirements of substation communication network,the generation method of substation communication network security attack and defense strategy based on TLS is studied. In order to ensure the security and integrity of data transmission in substation communication network,a high real-time secure transport layer protocol (TLS) is designed. Based on this,the process of security attack and defense competition in substation communication network is analyzed,and construct the attack and defense probability model,Based on the model,the competition process of both sides is simulated,The optimal strategies of attack and defense parties in different states are solved,and the generation of security attack and defense strategies of substation communication network is realized. The experimental results show that: under different attack behaviors,compared with the comparison method,the generation time of the proposed method is shorter than that of the contrast method,and the effective time is longer,up to 28.43 s. The accuracy of the security attack and defense behavior judgment is more than 93.8%,which fully verifies the feasibility of the proposed method.

Key words: TLS; substation; communication network; security; attack and defense strategy;

0　引言

现今通信网络安全环境越来越复杂,国家电网监控过程中,基础通信网络设施普遍存在着一定程度的安全隐患[1]。近几年,在世界范围内,通信网络恶意攻击、恶意入侵事件频发,尤其是针对电力系统,电网通信网络安全问题逐渐受到人们的重视。目前电网未设计充足的访问控制机制,对用户访问、操作权限等行为进行审核。传统通信网络利用加密技术保护自身网络的安全,但电网通信技术要求具备高实时性,加密技术容易致使通信延迟,再加上支撑软件的运行,会加大通信网络安全的薄弱环节[2]。另外,电网稳定运行依靠大量的嵌入式设备,这也为其带来更大的通信网络安全威胁,限制了通信网络安全传输层协议的设计与实现。

Tong W,Gao J,Li Z 等人[3]对智能变电站通信网络中的数据流进行了分析,提出了一种基于消息识别和流量监控的网络攻击拥塞保护方法。该方法成功地识别和丢弃伪消息,避免了真实消息在拥塞期间传输过程中的超时和丢包。郝唯杰,杨强,李炜[4]在对变电站站控层网络流量行为特性进行分析的基础上,采用分形自回归积分滑动平均(FARIMA)模型对网络流量构建了阈值模型。针对变电站典型的网络攻击模式和流量异常特征,基于运行状态评估算法对某实际变电站站控层流量数据进行分析,实现变电站在网络攻击情形下的安全态势评价。宋佳翰,李婧娇,皮杰,等人[5]提出基于马尔可

收稿日期: 2021-01-20
* 基金项目: 贵州电网科技项目(No. GZKJXM20182241)
作者简介: 陈刚(1982-),男,重庆永川人,高级工程师,主要研究方向为继电保护、厂站自动化、智能电网。

夫决策过程的变电站网络攻/防策略建模方法。该方法综合考虑了目标变电站的关键特性,攻/防双方的技术能力,为攻/防双方在电力信息物理系统网络安全场景设计中的行为选择提供了理论依据。上述方法虽然在一定程度上完成了网络防御,但是生成方法存在攻防策略生成及时性与时效性较差的缺陷,无法满足目前变电站通信网络安全需求。

为解决上述问题提出基于 TLS 的变电站通信网络安全攻防策略生成方法研究。TLS 指的是安全传输层协议,应用在两个通信应用程序之间,保障数据的完整性与保密性。此研究希望通过设计 TLS 为变电站通信网络安全提供更加有效的保障。

1 变电站通信网络安全攻防策略生成方法研究

1.1 安全传输层协议(TLS) 设计

为了保障变电站通信网络中数据传输的安全性与完整性,设计符合变电站高实时性的安全传输层协议(TLS) ,具体设计过程如下所示:

TLS 实质上在公钥基础上,满足通信网络的身份认证、数据加密等服务,此研究设计的 TLS 还需要具备防止伪造、窃听、篡改等通信网络攻击行为[6]。

设计的安全传输层协议(TLS) 具体步骤如下:

步骤一: 建立基于传输控制协议的连接;

步骤二: 客户端发送消息。若消息为 Client Hello,则表明其支持压缩算法、密码算法列表与协议版本,同时发送后续使用的随机数;

步骤三: 服务器反馈消息,其消息主要包含 Server Hello,Certificate,Certificate request,Server key exchange 与 Server hello done;

步骤四: 客户端反馈消息,其消息主要包含 Certificate,Client key exchange,Certificate Verify 与 Finished;

步骤五: 服务器发送消息,其消息主要包含 Change cipher spec 与 Finished;

步骤六: 基于加密过的数据,进行变电站通信;

步骤七: 客户端发送消息 close_notify,显示与传输控制协议的关闭[7]。

安全传输层协议(TLS) 示意图如图 1 所示。

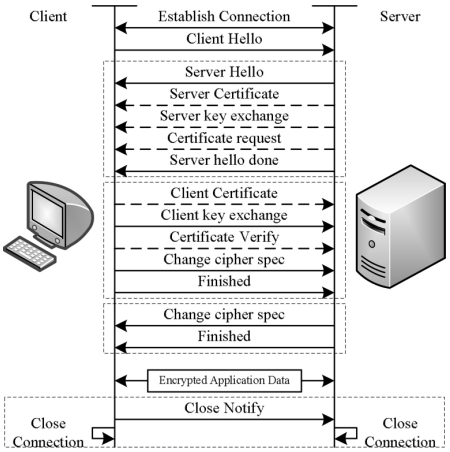

图 1 安全传输层协议(TLS) 示意图

1.2 攻防竞争过程分析

以上述设计的安全传输层协议(TLS) 为基础,分析变电站通信网络安全攻防竞争过程,为后续攻防概率模型构建提供帮助[8]。

常规情况下,一个完整的通信网络攻击行为主要分为 7 个时间段,在攻击过程中,访问与攻击行为产生的通信网络安全因子均存在着威胁性,为了对其进行深入的分析,给出通信网络攻击目标与位置标识,具体如表 1 所示。

表 1 通信网络攻击目标与位置标识表

攻击行为	攻击类型	攻击位置	攻击目标
访问行为	通信网络内	a1	通信网络
		a2	间隔层设备
		a3	用户交互界面
	通信网络外	a4	广域网
		a5	控制中心网络
		a6	邻接网络
		a7	企业网络
攻击行为	信息设备	c1-5	防火墙
		c6	远程访问点
		c7	时间同步
	物理设备	c8/9	过程层设备
		c10	控制中心服务器
		c11	控制中心用户交互界面

如表 1 所示,对通信网络攻击目标进行了分类,并对部分攻击位置进行标识,具体攻击位置如图 2 所示。

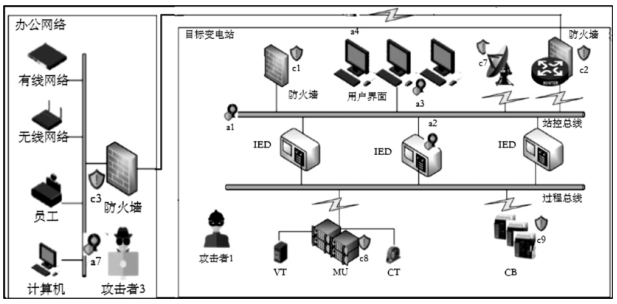

图 2 通信网络攻击位置标识图

如图 2 所示,此研究中设置一个通信网络攻击路径,产生若干个网络安全因子,构成一个网络安全事件,记为 a7-c3-a4-c2-a1-c8/c9[9]。

1.3 攻防概率模型构建

基于上述通信网络安全攻防竞争过程的分析结果,分别以攻击者与防御者视角出发,构建攻防概率模型,具体模型构建过程如下:

常规情况下,发动一个网络安全因子(CSF) 攻击后,结果只有两个,成功与失败,故其服从一个二项分布的离散事件[10]。设定网络安全因子之间是相互独立的,每个通信网络安全事件(CSE) 由若干个网络安全因子(CSF) 组成,则成功的通信网络安全事件包含的网络安全因子集合为 F,大小规格为 N_F,其服从泊松分布[11],记为 $N_F \sim P(\lambda_f)$,通信网络安全事件发生概率计算公式为

$$\begin{cases} P(N_F = n_f) = f(n_f, \lambda_f) = \dfrac{\lambda_f^{n_f} e^{-\lambda_f}}{n_f!} \\ P(N_F \leqslant n_f) = F(n_f, \lambda_f) = e^{-\lambda_f} \sum_{i=0}^{n_f} \dfrac{\lambda_f^i}{i!} \end{cases} \tag{1}$$

式(1)中，n_f 表示的是一个成功通信网络安全事件中包含的网络安全因子数量；λ_f 表示的是 N_F 的期望，反映变电站通信网络的安全级别；$f(n_f, \lambda_f)$ 表示的是一次成功的通信网络安全事件中攻击者触发 n_f 个网络安全因子的概率；$F(n_f, \lambda_f)$ 表示的是一次成功的通信网络安全事件需要触发的网络安全因子数量小于或等于 n_f 的概率。

当触发网络安全因子时，防御者主要是通过防火墙、安全传感器等抵御通信网络攻击。但是常规措施存在一定的局限性，因此，设置攻击者发动数个通信网络安全事件，形成多个日志，触发变电站通信网络监控系统发出警报[12]。依据贝叶斯原理可知，当通信网络监控系统警报响起时，通信网络攻击发生条件概率为

$$P(I/A) = \frac{P(I)\,P(A/I)}{P(I)\,P(A/I) + P(\neg I)\,P(A/\neg I)} \tag{2}$$

式(2)中，$P(I/A)$ 表示的是通信网络攻击发生条件概率。I 与 A 分别表示的是通信网络攻击与警报；$P(I)$ 表示的是通信网络攻击的概率；$P(A/I)$ 表示的是通信网络安全事件发生时，警报发生的条件概率；$P(\neg I)$ 表示的是没有通信网络安全事件发生的正常状态概率；$P(A/\neg I)$ 表示的是虚假警报发生概率。

通过研究可知，每个通信网络安全事件发生时，会产生正常日志数据与异常日志数据，分别采用 $\delta(f^k)$ 与 $\gamma(f^k)$ 表示，为常数。假设对于每个 CSF 而言，通过不断的模拟通信网络攻击事件，发现异常日志增量呈现逐渐下降的趋势[13]。因此，构建通信网络攻防概率模型计算公式为

$$P(I) = \frac{\sum_{k=1}^{n_f} [1 - F(k, \lambda_f)]\,\delta(f^k)}{\sum_{k=1}^{n_f} \{[1 - F(k, \lambda_f)]\,\delta(f^k) + \gamma(f^k)\}} \tag{3}$$

式(3)中，f^k 表示的是被攻击者成功发送的一组通信网络安全事件集合。

1.4　最佳攻防策略生成

以上述构建的攻防概率模型为依据，模拟变电站通信网络安全攻防双方的竞争过程，求解不同状态下攻防双方的最佳策略，为变电站通信网络安全提供更加有效的理论支撑[14]。

变电站通信网络安全最佳攻防策略 π 生成的目标为攻防各自期望累积收益最大化，表达式为

$$\begin{cases} \pi(s) = \arg\max_a \{P_a(s, s') [R_a(s, s') + \gamma V(s')]\} \\ V(s) = P_{\pi(s)}(s, s') [R_{\pi(s)}(s, s') + \gamma V(s)] \end{cases} \tag{4}$$

式(4)中，$\pi(s)$ 表示的是状态到动作选择的映射函数；$P_a(s, s')$ 表示的是从 t_r 时刻状态通过行动 a 转移到 t_{r+1} 时刻状态 s' 的概率；$R_a(s, s')$ 表示的是通信网络状态从 s 通过行动 a 转移到状态 s' 的即时收益；γ 表示的是策略生成过程中的收益权重因子，取值范围为(0,1)；$V(s)$ 与 $V(s')$ 分别表示的是状态 s 与状态 s' 的效用价值[15]。

假设 t_r 时刻变电站通信网络攻击相关状态为 $s = \{n_f, \lambda_f\}$，攻击者与防御者行动决策变量为 a_A 与 a_D。当 a_A 取值为 1 时，攻击者采取预备攻击行为；当 a_A 取值为 2 时，攻击者采取实质攻击行为；当 a_D 取值为 1 时，防御者采取主动防御行动；当 a_D 取值为 2 时，防御者采取被动防御行动[16]。

通过现有文献研究可知，变电站通信网络状态转移与攻防最佳策略的生成息息相关。当攻防动作分别为 $a_A = 1$ 与 $a_D = 1$ 时，变电站通信网络状态转移概率如表 2 所示。

表 2　通信网络状态转移概率表

s	s'	$P_a(s, s')$	攻防过程	决策时效性	模型通用性
$\{n_f, \lambda_f\}$	$\{+0, +0\}$	$(1-P_{-\lambda_f})(1-P_{+\lambda_f}) + P_{-\lambda_f} P_{+\lambda_f}$	时间连续	好	较好
	$\{+0, +1\}$	$P_{+\lambda_f}(1-P_{-\lambda_f})$			
	$\{+0, -1\}$	$P_{-\lambda_f}(1-P_{+\lambda_f})$			

依据表 2 显示的状态转移概率，针对不同通信网络攻击策略，实时给出最佳的防御策略，并达到攻防各自期望累积收益 $R_a(s, s')$ 的最大化[17]。

通过上述过程实现了变电站通信网络安全攻防最佳策略的生成，为变电站通信网络安全提供更加有效地保障。

2　实验与结果分析

为了验证提出方法与现有方法的攻防策略生成性能差异，采用 MATLAB 软件平台设计仿真对比实验，具体实验过程如下所示。

2.1　实验数据准备

实验在美国 MIT 攻防行为数据库选取强 A_H、中 A_M、弱 A_L 三种类型的攻击行为与防御行为，将其作为实验数据，如表 3 与表 4 所示。

表 3　攻击行为表

攻击类型	攻击名称	攻击强度
A_H	Remote buffer overflow	0.95
	Install Trojan	0.80
	Steal account and crack it	0.70
A_M	Send abnormal data to GIOP	0.50
	Shutdown Database server	0.45
	LPC to LSASS process	0.40
A_L	Oracle TNS Listener	0.35
	Ftp rhost attack	0.30
	Sr-Hard blood	0.25

表 4　防御行为表

攻击类型	攻击名称	攻击强度
A_H	Reinstall Listener program	0. 80
	Limit packets from ports	0. 80
	Install Oracle patches	0. 80
	Limit access to MDSYS. SDO_CS	0. 70
	Uninstall delete Trojam	0. 70
	Restart Database server	0. 60
	Renew root data	0. 60
A_L	Add physical resource	0. 50
	Limit SYN/ICMP packets	0. 50
	Correct homepage	0. 40
	Repair database	0. 40
	Redeploy firewall rule and filtrate malicious packets	0. 30
	Delete suspicious account	0. 30
	Patch SSH on Ftp Sever	0. 20

2. 2　最佳收益权重因子确定

通过现有文献研究可知,收益权重因子极大地影响着攻防策略的生成,故需要在实验进行前,确定最佳收益权重因子。收益权重因子变化曲线如图 3 所示。

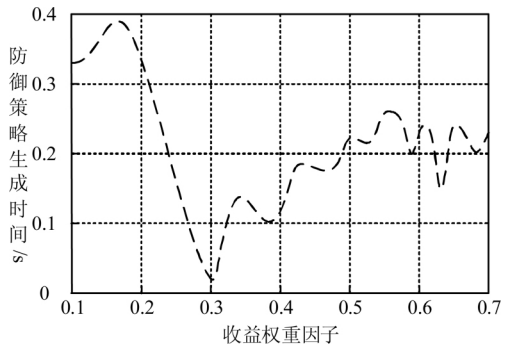

图 3　收益权重因子变化曲线图

如图 3 曲线显示,当收益权重因子为 0. 3 时,防御策略生成时间最短,可以更好地保障变电站通信网络的安全。故确定最佳收益权重因子为 0. 3。

2. 3　实验结果分析

依据上述选取的实验数据与确定的收益权重因子,采用对比方法与提出方法进行仿真对比实验,依据攻击强度从大到小将攻击行为进行排序,编号记为 1 ~ 9。分别对比本文方法与文献 [3] 基于消息识别和流量监控的网络攻击拥塞保护方法以及文献 [5] 基于马尔可夫决策过程的变电站网络安全攻防策略选取方法实验获得攻防策略生成及时性与时效性数据如表 5 所示。

表 5　实验数据表

(1) 攻防策略生成及时性数据

攻击编号	攻防御策略生成时间/s		
	提出方法	文献 [3] 方法	文献 [5] 方法
1	1. 247 2	2. 415 2	3. 422 2
2	1. 008	2. 215 8	3. 183
3	0. 982 4	2. 115	3. 157 4
4	1. 022 8	2. 063 5	3. 197 8
5	1. 021 1	2. 215 6	3. 196 1
6	1. 545 7	2. 915 8	3. 720 7
7	0. 980 5	1. 845 2	3. 155 5
8	0. 851 9	1. 883	3. 026 9
9	0. 848 2	2. 113 3	3. 023 2

(2) 攻防策略生成时效性数据

攻击编号	攻防御策略有效时间/min		
	提出方法	文献 [3] 方法	文献 [5] 方法
1	20. 18	15. 63	17. 04
2	23. 48	10. 73	20. 34
3	20. 22	10. 22	17. 08
4	24. 61	12. 56	21. 47
5	19. 59	12. 7	16. 45
6	25. 87	13. 75	22. 73
7	26. 52	15. 68	23. 38
8	27. 91	16. 46	24. 77
9	28. 43	12. 48	25. 29

如表 5 数据显示,本方法与文献 [3] 方法和文献 [5] 方法相比较,在不同攻击行为序号下,提出方法的防御策略生成时间更短、有效时间更长,表明提出方法具备更好的攻防策略生成及时性与时效性,这是由于本方法依据构建的攻防概率模型,模拟变电站通信网络安全攻防双方的竞争过程,求解不同状态下攻防双方的最佳策略,从而减少了生成策略的时间和延长了策略有效时间。为进一步验证提出方法具有更好的适用性与指导作用,分别利用上述三种方法判断变电站通信网络安全攻击行为与防御行为的准确性,实验结果如图 4 所示。

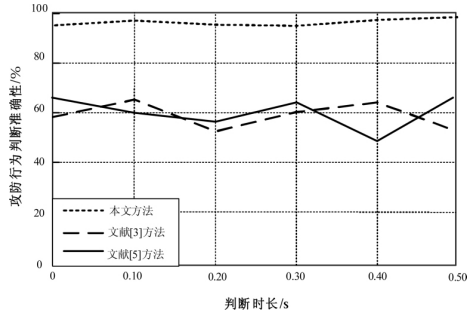

图 4　变电站通信网络安全攻防行为判断准确性

由图 4 可知,本方法与文献 [3] 方法和文献 [5] 方法相比较,安全攻防行为判断准确性更高,在 93. 8% 以上,这是由于本方法构建攻防概率模型,可以更高精度地识别攻防行为。

3　结束语

此研究在设计安全传输层协议(TLS) 下,提出了新的变电站通信网络安全攻防策略生成方法,通过实验证实了提出方法攻防策略生成的及时性与时效性,能够保障变电站通信网络遭受到攻击时,及时生成最佳防御策略,为变电站通信网络安全提供更加有效地保障,也为通信网络安全研究提供一定的参考。

(下转第 54 页)

按保护重要性由高到低的顺序对各保护进行检查，避免了传统的随机或顺序检查各保护的缺点，它对于提高电力系统安全稳定运行和可靠性具有重要意义。

但由于研究时间有限，目前的验证技术还存在一定的不足。由于电网规模不断扩大，为了满足实时检测的需要，有必要进一步研究提高在线检测计算速度的方法。

参考文献

[1] 魏巍. 定值在线校核系统在地铁供电领域的应用研究[J]. 城市轨道交通研究，2018，21(4)：153-156.

[2] 蒋航，刘进，熊俊，等. 基于线路二次设备实时信息的保护定值风险评估研究[J]. 电力系统保护与控制，2020，550(4)：103-109.

[3] Dawei L，Shuang S，Quan M A. Automatic test system of relay protection device for intelligent substation based on cloud strategy and MMS protocol[J]. Power System Protection and Control，2019，47(12)：159-164.

[4] Yufeng Q，Chenglong D，Guangzhong S. Application of Relay Protection Setting Value Intelligent Assistant Audit System Based on Expert Database[J]. Inner Mongolia Electric Power，2019，37(01)：1-5.

[5] 刘俊红，邓兆云，李泽科，等. 基于即插即用的智能变电站信息自动校核技术[J]. 电力系统保护与控制，2018，500(2)：137-143.

[6] 邓炼兴，巩俊强，姜云峰，等. 智能电网继电保护定值在线比对和固化系统[J]. 电网与清洁能源，2018，34(04)：36-41.

[7] 徐长宝，赵立进，高吉普，等. 基于灰色马尔科夫链的继电保护装置寿命研究[J]. 电力科学与技术学报，2019，34(3)：114-119.

[8] 王月月，陈民铀，姜振超，等. 基于云理论的智能变电站二次设备状态评估[J]. 电力系统保护与控制，2018，46(1)：71-77.

[9] 吴迪，汤小兵，李鹏，等. 基于深度神经网络的变电站继电保护装置状态监测技术[J]. 电力系统保护与控制，2020，48(5)：81-85.

[10] 宗志亚. 基于扰动激励的智能变电站继电保护故障诊断关键技术[J]. 电测与仪表，2019，56(21)：63-69.

[11] 张旭泽，郑永康，康小宁，等. 智能变电站继电保护系统所面临的若干问题[J]. 电力系统保护与控制，2018，46(6)：90-96.

[12] 孙辉，张国庆，高博，等. 采用组合赋权法的智能变电站继电保护设备状态模糊综合评估[J]. 电测与仪表，2020，57(7)：23-28，34.

[13] 肖繁，王紫薇，张哲，等. 基于状态监测的继电保护系统检修策略研究[J]. 电力系统保护与控制，2018，46(6)：74-83.

[14] 裘愉涛，周震宇，杨剑友，等. 继电保护远程运维技术研究与应用[J]. 电力系统保护与控制，2018，46(18)：17-24.

[15] 高旭，马迎新，王可，等. 基于连通状态矩阵的智能变电站安措校核方法[J]. 电力自动化设备，2019，39(7)：195-202.

(上接第 49 页)

参考文献

[1] 董坤祥. 网络空间安全视阈下恶意软件攻防策略研究[J]. 科研管理，2019，40(11)：164-174.

[2] 刘景玮，刘京菊，陆余良，等. 基于网络攻防博弈模型的最优防御策略选取方法[J]. 计算机科学，2018，45(6)：117-123.

[3] Tong W，Gao J，Li Z，et al. A Protection Method Based on Message Identification and Flow Monitoring for Managing the Congestion Arising From Network Attacks on Smart Substation[J]. IEEE Communications Letters，2018，22(11)：2214-2217.

[4] 郝唯杰，杨强，李炜. 基于 FARIMA 模型的智能变电站通信流量异常分析[J]. 电力系统自动化，2019，43(01)：215-226.

[5] 宋佳翰，李婧娇，皮杰，等. 基于马尔可夫决策过程的变电站网络安全攻防策略[J]. 电力建设，2019，40(10)：104-110.

[6] 张恒巍，杨豪璞. 基于攻防信号博弈的 APT 攻击防御决策方法[J]. 计算机工程与设计，2019，40(1)：59-64.

[7] 赵艳军，梁坤杰，龙霏，等. 考虑灾害事件攻防顺序的电网防灾资源分配策略[J]. 中国电力，2020，53(1)：49-55.

[8] 余萍，王宁，李勇. 基于波分复用的新一代智能变电站通信网络鲁棒性分析[J]. 光通信技术，2018，42(12)：59-62.

[9] 张恒巍，黄世锐. Markov 微分博弈模型及其在网络安全中的应用[J]. 电子学报，2019，47(3)：606-612.

[10] 宋贺，王晓锋. 基于轻量级虚拟化的 LDDoS 仿真方法[J]. 计算机工程，2020，46(3)：105-113.

[11] 张程，尚海涛. 基于数学建模的网络数据流异常检测仿真[J]. 计算机仿真，2019，036(011)：423-426，453.

[12] 雷程，马多贺，张红旗，等. 基于网络攻击面自适应转换的移动目标防御技术[J]. 计算机学报，2018，41(5)：1109-1131.

[13] 蒋侣，张恒巍，王晋东. 基于信号博弈的移动目标防御最优策略选取方法[J]. 通信学报，2019，41(6)：42-52.

[14] 孙骞，高岭，刘涛，等. 基于非零和博弈的多路径组合攻击防御决策方法[J]. 西北大学学报：自然科学版，2019，49(3)：343-350.

[15] 张伟丽，王兴伟，张爽，等. 基于安全博弈的 SDN 数据包抽检策略[J]. 郑州大学学报(理学版)，2018，50(1)：15-19.

[16] 张为，苏旸，陈文武. 面向分布式网络结构的 APT 攻击双重博弈模型[J]. 计算机应用，2018，38(5)：1366-1371.

[17] 董彦伯，周鹏，李雪，等. 网络化系统拒绝服务攻击对抗式检测方法研究[J]. 仪器仪表学报，2018，39(5)：205-213.

[18] 朱小栋，张瑶瑶，姚润坤，张钰. 基于区块链的政府信息开放与共享模式研究[J]. 重庆工商大学学报(自然科学版)，2020，37(5)：122-128.