DOI: 10.7667/PSPC170784

面向SCADA的网络攻击对电力系统可靠性的影响

丁 明，李晓静，张晶晶

(合肥工业大学电气与自动化工程学院，安徽 合肥 230009)

摘要：电力系统的运行和控制越来越依赖于数据采集与监控(SCADA)系统。通过攻击 SCADA，攻击者可以操纵信息或重新配置设备动作参数使断路器跳闸。考虑几种常见的攻击 SCADA 使断路器跳闸的方式，利用攻击树模型评估不同攻击场景的成功率。在断路器常规可靠性模型基础上，考虑 SCADA 受网络攻击的影响，建立断路器修正后的强迫停运率模型。利用非序贯蒙特卡洛方法计算电力系统可靠性指标。用 IEEE-RTS79 系统仿真，分析不同攻击场景对电力系统可靠性的影响，验证了该方法的可行性与有效性。

关键词：网络攻击；SCADA；断路器；攻击树；非序贯蒙特卡洛

Effect of SCADA-oriented cyber attack on power system reliability

DING Ming, LI Xiaojing, ZHANG Jingjing

(School of Electrical and Automation Engineering, Hefei University of Technology, Hefei 230009, China)

Abstract: The operation and control of power systems are increasingly dependent on the Supervisory Control and Data Acquisition (SCADA) system. By attacking SCADA, an attacker can manipulate the information or reconfigure the device parameters to trip the circuit breaker. This paper considers several common ways to attack SCADA to trip the circuit breaker, and uses the attack tree model to evaluate the success rate of different attack scenarios. On the basis of the conventional reliability model of the circuit breaker, and considering the influence of SCADA cyber attacks, a revised forced outage rate model of the circuit breaker is established. Non-sequential Monte Carlo method is used to calculate power system reliability index. IEEE-RTS79 system simulation is used to analyze the influence of different attack scenarios on the reliability of power system, which verifies the feasibility and validity of the method.

This work is supported by National High-tech R & D Program of China (863 Program) (No. 2015AA050104).

Key words: cyber attack; SCADA; circuit breaker; attack tree; non-sequential Monte Carlo

0 引言

随着信息技术应用于电力系统的各个方面，电力系统正在成为一个融合电力和通信网络的复杂大系统[1]。数据采集与监控(SCADA)系统作为电力系统的重要通信网络，在加强电力系统可观测性和可控性的同时，也是网络攻击的高价值目标，可能造成电力系统重大安全隐患和经济损失。例如，2015年12月23日，乌克兰国家电网SCADA受到网络攻击，突发大规模停电事故。这次攻击被认为是第一例网络攻击造成的大停电事件，引起了世界范围内的广泛关注[2]。因此，评估 SCADA 受网络攻击对电力系统可靠性的影响非常重要，有助于分析 SCADA 的薄弱环节，并且有针对性地对漏洞采取相应的防御措施。

目前国内外对于电力系统可靠性和信息系统可靠性的评估方法都各自有较为成熟的模型[3-6]。在此基础上，将电力系统与信息系统融合，分析网络攻击对电力系统可靠性的影响，国内外学者已经开展了研究。文献[7-8]认为攻击树、Petri 网可用于SCADA的建模和评估，提出了一个包含实时监控、影响分析、异常检测和减灾措施的 SCADA 安全框架，在此框架内建立了集成密码策略和端口审查的攻击树模型；文献[9]将攻击树按攻击场景进行划分，对电力 SCADA 的脆弱性进行定量分析；文献[10]

基金项目：国家高技术研究发展计划(863 计划)资助项目(2015AA050104)

利用广义随机 Petri 网(GSPN)对 SCADA 的网络安全进行了脆弱性评估。文献[11-13]总结了电力信息物理融合系统的实现技术与挑战及其混合仿真方法；文献[14-15]构建了由信息系统功能、一次系统元件及信息-电力作用关系组成的系统可靠性模型。但是由于信息系统和电力系统的交互十分复杂，影响机理尚待进一步分析，所以网络攻击对电力系统可靠性影响的研究还处于探索阶段，理论基础和系统模型有待进一步完善。

本文讨论了电力系统受网络攻击影响的一种典型情景—攻击者通过攻击 SCADA 实现断路器无故障跳闸的目标。首先分析实现该目标的常见攻击方式，其次利用攻击树模型量化各攻击场景的成功率；继而在断路器常规可靠性模型基础上考虑 SCADA 受网络攻击的影响，建立断路器修正后的强迫停运率模型；最后，以 IEEE-RTS79 系统为例，使用非序贯蒙特卡洛模拟方法进行可靠性计算，分析不同攻击场景对电力系统可靠性的影响，验证本文方法的可行性与有效性。

1 SCADA 与网络攻击方式

1.1 SCADA 的结构

SCADA 中，各厂站配置测量传感器，传感器信号连接到远程终端单元(RTU)。RTU 将接收的模拟信号转换为数字格式，并按照规定协议的要求做成报文包，通过传输系统送到控制中心。应用服务器为人机界面(HMI)提供数据，达到监视和控制的目的。控制命令通过前端处理器发给远端的 RTU 执行，执行后 RTU 将执行结果返校给操作员。

如图 1 所示，SCADA 由控制中心网络、控制中心和变电站之间的通信网络、变电站自动化系统等网络组件构成。攻击者利用各个网络组件的漏洞

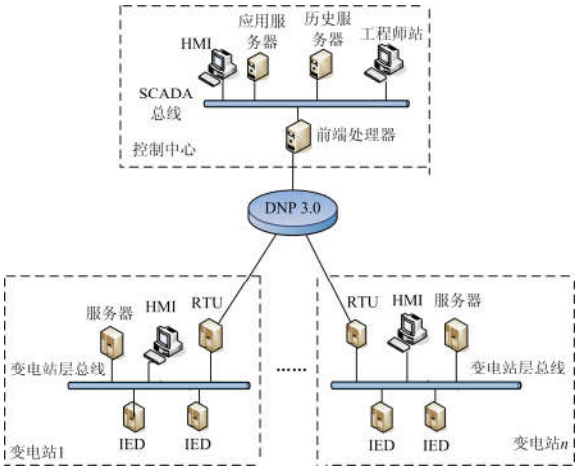


图 1 SCADA 结构图

Fig. 1 Structure of SCADA

进行非授权操纵，可能造成电力系统安全隐患和经济损失。

1.2 导致断路器无故障跳闸的常见攻击方式

导致断路器无故障跳闸的常见攻击方式有 5 种[16-18]，归纳了攻击者如何利用 SCADA 各组件中的漏洞，直接或间接控制保护继电器发出跳闸命令，导致断路器无故障跳闸。

1) 攻击控制中心

攻击者绕过硬件防火墙后能够通过端口扫描方法访问交换机。当攻击者成功侵入到控制中心网络时，能够通过侵入历史服务器来扫描网络的主机和服务器。由于应用服务器能够直接向其他设备发送命令，因此被选为网络入侵的目标。应用服务器用于存储数据，并将更新的数据发送到其他客户端，例如 HMI。获得应用服务器的根特权，跳闸命令可以通过前端处理器直接发送到一个变电站中的 RTU 执行。

2) 攻击控制中心与变电站之间的通信网络

通过访问控制中心和变电站之间的通信网络，攻击者在有线或无线网络中安装窃听设备。攻击者监控流量，截取并捕获测量值或状态数据包，用所制造的异常数据替换一些正常状态数据，这些假数据被发送到状态估计模块。当假操作条件最终呈现给操作者时，一些操作者可能被误导并且发送不正确的跳闸命令到继电器。

3) 访问变电站 HMI

攻击者利用 IP 和端口扫描工具，识别一个变电站的活动系统端口，使用基于字典或强力密码攻击登录其中一个路由器。由于对手已经访问变电站的网络，因此 IP 扫描工具被再次部署用于变电站用户界面入侵。然后通过用户接口访问变电站 HMI，向一个或多个继电器发送跳闸命令。

4) 访问 RTU

通过拨打一个城市中的所有号码，可以到达变电站的应答调制解调器。一些测试信号被发送到调制解调器以寻找可用的调制解调器连接。一旦登录对话框提交给攻击者，就可以使用密码攻击来访问调制解调器。由于一些 RTU 能够识别调制解调器，所以它们可以在没有认证的情况下被访问。如果可以理解 RTU 协议并且利用 RTU 的漏洞，攻击者可以控制由 RTU 监视的继电器或者远程执行一些模块上的重新配置使断路器跳闸。

5) 访问保护继电器

攻击者成功访问变电站网络后，可能无法到达用户界面。若网络使用默认密码或弱密码，则攻击者可以获得对保护继电器的未授权访问并控制继电器。

2　面向 SCADA 的网络攻击建模

2.1 攻击树模型

1988 年，美国国防部在制定计算机安全标准研究时，使用了图示的方法来模拟网络攻击。Schneider 受到这种图示法和研究可靠性时所用的故障树方法的启发，提出攻击树的概念。攻击树在实践中已被证明具有概念清晰、易于分析结果和建模能力强等优点。

攻击树包含根节点、叶节点和攻击子树三部分。根节点表示最终期望达到的攻击目标，叶节点表示组成攻击树的单一攻击尝试行为，攻击子树表示攻击叶可以实现的比根节点低层次的攻击子目标。攻击树中的节点可以是与(and)节点、或(or)节点。and 节点表示为了使此节点的攻击成功需要使 and 节点下面的所有分支的攻击都成功，or 节点表示为了使此节点的攻击成功只需要有一个分支的攻击成功。and 节点和 or 节点的图形表示方法如图 2 所示。

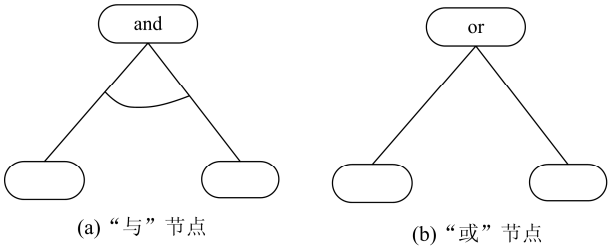


图 2 攻击树中的“与”节点和“或”节点

Fig. 2 The “and” and “or” node in attack tree

2.2 面向 SCADA 的攻击树建模过程

2.2.1 构造攻击树

本文假定攻击目标是断路器无故障跳闸，在前面分析的基础上，构造攻击树如图 3 所示。

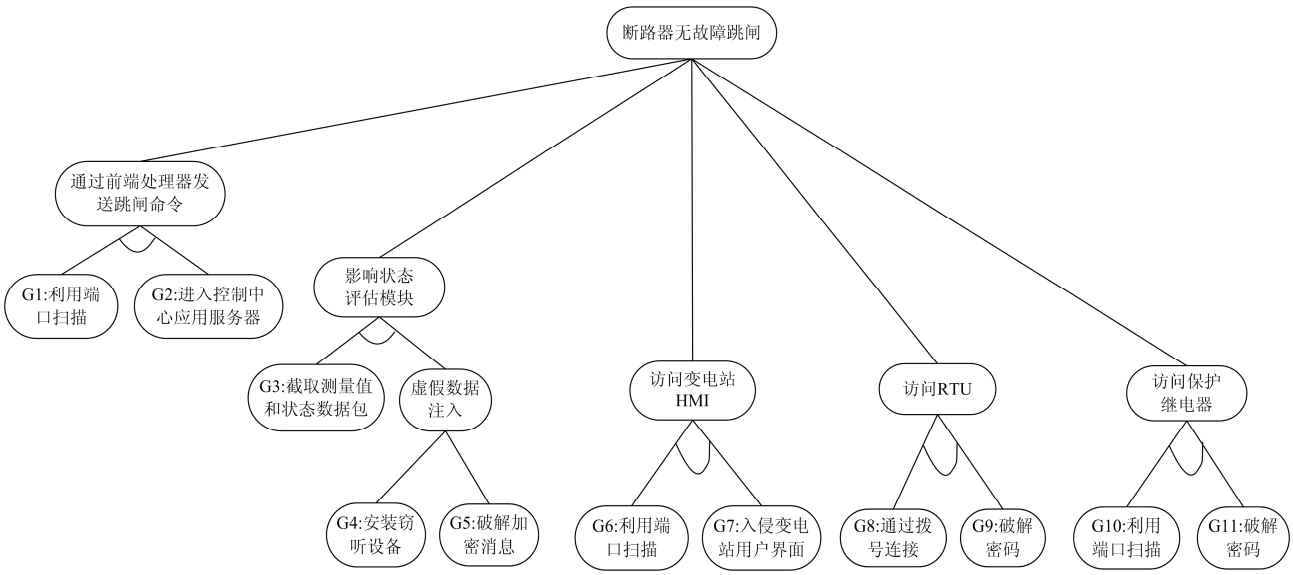


图 3 断路器无故障跳闸的攻击树

Fig. 3 Attack tree for fault-free tripping of the circuit breaker

2.2.2 每个叶节点的攻击成功率

在这里采用属性的观点，给每个叶节点赋予三个属性，即攻击的成本、攻击的难度和攻击被发现的可能性，表 1 示出了三个属性的评分标准[19]。应用多属性效用理论，将以上属性转换成其实现目标的效用值(即该叶节点发生的成功率)。计算公式如式(1)。

$$P_G = W_{\text{cost}} \times U(cost_G) + W_{\text{diff}} \times U(diff_G) + W_{\text{det}} \times U(det_G) \tag{1}$$

式中：G 表示任意的一个叶节点；P_G 表示该叶节点的攻击成功率；参数 $cost_G$ 表示攻击该叶节点的成本；$diff_G$ 表示攻击该叶节点的难易程度；det_G 表示攻击该叶节点可能被发现的等级；W_{cost} 是成本参数的权重；W_{diff} 是难度参数的权重；W_{det} 是被发现的可能性参数的权重；$U(cost_G)$ 表示成本参数的效用性；$U(diff_G)$ 表示难度参数的效用性；$U(det_G)$ 表示被发现的可能性参数的效用性。

对于三个权重系数，可以利用模糊层次分析法算出。对于叶节点各属性的评分，评估人员根据系统的实际情况给出。为了计算叶节点的攻击成功率，还要把各属性评分转换成相应的效用性 $U(cost_G)$，$U(diff_G)$，$U(det_G)$。通过分析可知，$cost_G$、$diff_G$、det_G 与 $U(cost_G)$、$U(diff_G)$、$U(det_G)$ 是成反比例

关系的。为了方便计算，三组变量之间的对应关系均取为 $U(x)=1/x$ 。

表 1 等级评分标准

Table 1 Grade standard

攻击成本/万元	等级	攻击难度	等级	被发现的可能性	等级
>5	5	很难	5	很难	1
2~5	4	难	4	难	2
1~2	3	中等	3	中等	3
0.5~1	2	容易	2	容易	4
<0.5	1	很容易	1	很容易	5

2.2.3 各个攻击场景的成功率

攻击场景是一组叶节点的集合，实现了这组叶节点就可以达到攻击树根节点，即攻击者的最终目标。本文从攻击树识别攻击场景，这可以根据攻击树的拓扑结构，利用下行法或上行法求攻击树最小割集的方法来求取。通过对图 3 进行分析，得到攻击场景 S_i 如下：

$\prod_{i=1,2} G_i \to S_1$，$\prod_{i=3,4} G_i \to S_2$，

$\prod_{i=3,5} G_i \to S_3$，$\prod_{i=6,7} G_i \to S_4$，

$\prod_{i=8,9} G_i \to S_5$，$\prod_{i=10,11} G_i \to S_6$。

一旦所有的攻击场景都确定，即可以计算攻击场景成功率。攻击场景成功率是一系列叶节点攻击成功率的组合。计算公式如式(2)。

$$P(S_i)=\begin{bmatrix} P(S_1)=\prod_{j\in s_1} P(G_j) \\ P(S_2)=\prod_{j=s_2} P(G_j) \\ \vdots \\ P(S_k)=\prod_{j\in s_k} P(G_j) \end{bmatrix} \tag{2}$$

式中：$P(S_1)$ $P(S_2)$ … $P(S_k)$ 是攻击场景的成功率；k 是攻击场景的总数。

需要说明的是：对于 and 节点，其攻击成功率等于该节点各分支攻击成功率的乘积；对于 or 节点，其攻击成功率等于该节点各分支攻击成功率的最大值。

3 面向 SCADA 的网络攻击对电力系统可靠性的影响

3.1 断路器的重要性和存在的攻击尝试次数

按攻击者的目的，针对 SCADA 的攻击可分为两大类：一类是为了炫耀自身能力而进行的无准确目标的随意攻击，另一类则是对重要的断路器进行蓄意攻击。本文重点研究蓄意攻击的情况。

对于蓄意攻击事件，攻击者会事先了解电网的拓扑结构甚至负荷情况，并对断路器的重要性进行判断，重要性越高的断路器受攻击的次数越多。

考虑到电力系统传送电能的本质功能，本文用因断路器无故障跳闸所导致的电力系统失负荷量来衡量断路器的重要性，并进行归一化处理。

$$C_i=\frac{P_{\mathrm{sh}i}}{\sum P_{\mathrm{sh}i}} \tag{3}$$

式中：C_i 表示断路器 i 的重要性；$P_{\mathrm{sh}i}$ 表示因断路器 i 无故障跳闸导致的电力系统失负荷量；$\sum P_{\mathrm{sh}i}$ 表示攻击范围内的所有断路器(包括断路器 i)分别切除后电力系统失负荷量之和。

本文采取 N-1 开断模式下系统停电功率最小的有功调度策略来计算 $P_{\mathrm{sh}i}$，目标函数为

$$P_{\mathrm{sh}i}=\min\sum_{j\in ND}\Delta P_{\mathrm{L}j} \tag{4}$$

约束条件如下。

a) 节点有功功率平衡，即流入节点和流出节点的有功功率相等。

$$\sum_{k\in j} P_{jk}=P_{\mathrm{G}j}-(P_{\mathrm{L}j}-\Delta P_{\mathrm{L}j}) \quad j\in NB \tag{5}$$

b) 发电机出力约束。

$$P_{\mathrm{G\,min}}\le P_{\mathrm{G}}\le P_{\mathrm{GN}} \tag{6}$$

c) 线路有功潮流约束。

$$\left|P_{jk}\right|\le P_{jk\max} \quad jk\in NL \tag{7}$$

d) 节点切负荷约束。

$$0\le\Delta P_{\mathrm{L}j}\le P_{\mathrm{L}j}-P_{\mathrm{L}j}^{(1)} \quad j\in ND \tag{8}$$

式(4)—式(8)中，各符号含义如下：节点集合 NB；线路集合 NL；发电机集合 NG；负荷集合 ND；发电机出力 $P_{\mathrm{G}j}$；负荷 $P_{\mathrm{L}j}$；切负荷量 $\Delta P_{\mathrm{L}j}$；不可停电负荷 $P_{\mathrm{L}j}^{(1)}$；线路潮流 P_{jk} 及限额 $P_{jk\max}$；机组额定出力 P_{GN}；机组最小技术出力 $P_{\mathrm{G\,min}}$。

得到攻击范围内各断路器的重要性后，一年中各断路器上的攻击尝试次数可由式(9)求出。

$$N_i=C_i\cdot V \tag{9}$$

式中：N_i 表示一年中断路器 i 上的攻击尝试次数；V 表示一年中对攻击范围内所有断路器的攻击尝试总次数。

3.2 电力系统可靠性建模

可靠性评估中元件的强迫停运率(FOR)用于描述元件的强迫中断模式的发生概率，即处于不可用状态的概率。SCADA 受网络攻击后对电力系统断路器可靠性的影响可以通过增加断路器的 FOR

值来评估。考虑 SCADA 受网络攻击后，电力系统断路器 i 修正后的强迫停运率 FOR_i' 的计算公式如式(10)。

$$FOR_i' = FOR_i + n_i \cdot \alpha_i \tag{10}$$

式中：FOR_i 表示断路器 i 的原始强迫停运率；$n_i \cdot \alpha_i$ 表示由于 SCADA 受网络攻击而增加的强迫停运率；n_i 表示一年中断路器 i 上的攻击成功次数；α_i 表示一次成功攻击造成的断路器 i 的不可用率。n_i、α_i 可以表示如下：

$$n_i = N_i \cdot P \tag{11}$$

$$\alpha_i = \frac{T_{F_i} + T_{R_i}}{8\,760} \tag{12}$$

在式(11)中，N_i 表示一年中断路器 i 上的攻击尝试次数，由式(9)求得；P 是攻击成功率，由式(2)求得。在实际情况下，SCADA 受到一次网络攻击尝试需要时间和成本，因此本文假定攻击尝试次数 N_i 有限，不会使式(10)的取值大于 1。式(12)中，8 760 h 为断路器 i 一年工作小时数，T_{F_i} 为断路器 i 被攻击后的网络取证和恢复时间，T_{R_i} 为断路器的重新投运时间。T_{F_i} 和 T_{R_i} 的取值可参考文献[20]。

求得断路器 FOR' 后，应用基于非序贯蒙特卡洛模拟的电力系统可靠性分析方法计算电力系统的停电概率 $LOLP$ 和停电功率 $EDNS$ 以评价 SCADA 受网络攻击对电力系统可靠性的影响，所采用的最小停电功率模型同式(4)—式(8)，差别在于考虑了多重停运。$LOLP$、$EDNS$ 定义如式(13)和式(14)。

$$LOLP = m / M \tag{13}$$

$$EDNS = (\sum_{i=1}^{m} p_{shi}) / M \tag{14}$$

式中：m 为系统停电次数；M 为模拟抽样次数；p_{shi} 为每次的停电功率。

考虑 SCADA 受网络攻击的电力系统可靠性评估流程图如图 4 所示。

4　算例分析

本文以 IEEE-RTS79 节点为例[21-22]，研究 SCADA 受网络攻击对电力系统可靠性的影响。该系统含 32 台发电机、33 条线路、5 台变压器和 24 条母线。假定攻击者的攻击目的是使发电机停运，因此通过 SCADA 蓄意攻击的对象是发电厂的机端断路器，机端断路器被攻击后将导致发电机组无故障跳闸停运。为方便起见，在以下的讨论中将机端断路器与发电机合并为单元接线发电机组，断路器的强迫停运率合并到发电机强迫停运率中。

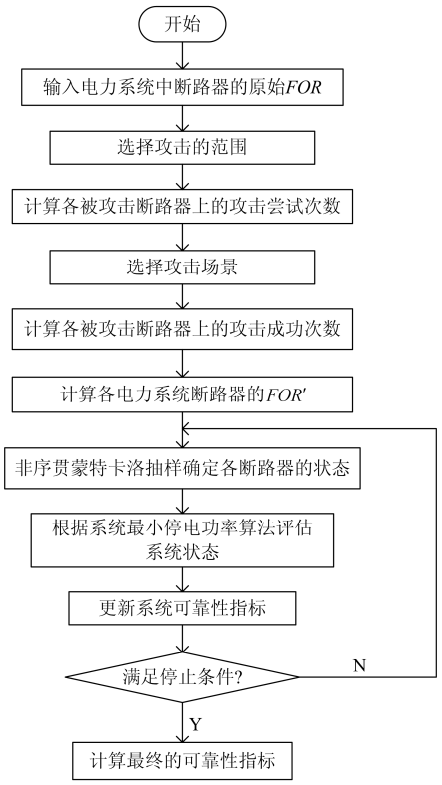


图 4　考虑 SCADA 受网络攻击的电力系统可靠性评估流程图

Fig. 4 A diagram for reliability evaluation of power system considering cyber attack to SCADA

4.1　不同攻击场景下的攻击成功率

对于式(1)中的三个权重系数，根据文献[23]中的数据，由模糊层次分析法计算出，$W_{cost} = 0.433$，$W_{diff} = 0.333$，$W_{det} = 0.233$。评估人员根据实际情况对各个叶节点进行评分，其得分情况如表 2 所示。然后将各值代入式(1)，得到各个叶节点的攻击成功率如表 2 所示。

表 2　各个叶节点的属性得分和成功率

Table 2 Attribute score and success rate of each leaf

攻击叶	攻击成本等级得分	攻击难度等级得分	攻击被发现的可能性等级得分	攻击成功率
G_1	5	5	5	0.200
G_2	5	5	4	0.212
G_3	2	2	2	0.500
G_4	2	2	3	0.461
G_5	1	1	2	0.389
G_6	3	3	3	0.333
G_7	3	3	2	0.372
G_8	2	2	3	0.461
G_9	1	1	2	0.883
G_{10}	3	3	3	0.333
G_{11}	1	1	2	0.883

根据 2.2 节中确定的 6 种攻击场景，由式(2)得到各个攻击场景的成功率，如图 5 所示。

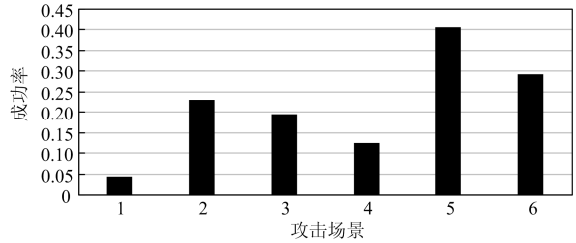


图 5 各个攻击场景的成功率

Fig. 5 Success rate of each attack scene

由图 5 可知每个攻击场景的成功率不同，发现最难以直接入侵控制中心主站，攻击成功率为 0.042；而通过变电站网络的攻击中，最难的攻击场景是侵入变电站 HMI，最容易的攻击场景是访问 RTU，攻击成功率分别为 0.124 和 0.407。

4.2 网络攻击下修正后的强迫停运率

以攻击对象是 IEEE-RTS79 系统中的 32 台发电机机端断路器为例，给定一年中对 32 台发电机组的攻击尝试总次数为 2 000 次。根据 3.1 节模型，可以得到每台发电机组上的攻击尝试次数，如图 6 所示。

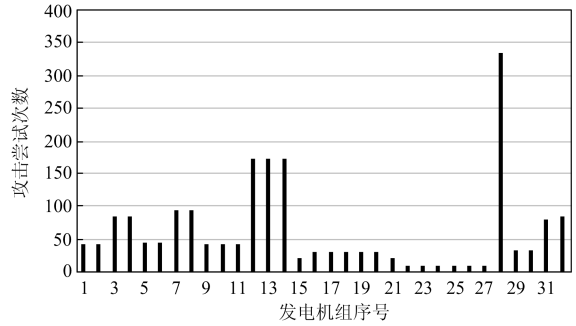


图 6 发电机组上的攻击尝试次数

Fig. 6 The number of attack attempts to each generator set

得到各发电机组上的攻击尝试次数后，结合各个攻击场景的成功率，可利用式(11)求得 6 种攻击场景分别对每台发电机组的攻击成功次数，如表 3 所示。

参考文献[20]中数据，假定发电机组被攻击后的网络取证和恢复时间是 8 h，发电机组重新投运时间是 2 h。由式(10)可以得到在攻击场景 1~6 条件下，32 台发电机组经修正后的强迫停运率，见附录 1。

图 7 示出了 32 台发电机组的原始强迫停运率和利用攻击场景 5 攻击时，发电机组修正后的强迫停运率。其余攻击场景对应的发电机组修正后的强迫停运率介于不考虑攻击和攻击场景 5 之间。

表 3 各攻击场景对 32 台发电机组的攻击成功次数

Table 3 The number of successful attacks on 32 generating units in each attack scenario

序号	不同攻击场景下的攻击成功次数					
	S1	S2	S3	S4	S5	S6
1	2	10	8	5	17	13
2	2	10	8	5	17	13
3	4	19	16	10	34	25
4	4	19	16	10	34	25
5	2	10	8	5	18	13
6	2	10	8	5	18	13
7	4	22	18	12	38	28
8	4	22	18	12	38	28
9	2	10	8	5	18	13
10	2	10	8	5	18	13
11	2	10	8	5	18	13
12	7	40	34	21	71	51
13	7	40	34	21	71	51
14	7	40	34	21	71	51
15	1	5	4	3	9	6
16	1	7	6	4	13	9
17	1	7	6	4	13	9
18	1	7	6	4	13	9
19	1	7	6	4	13	9
20	1	7	6	4	13	9
21	1	5	4	3	8	6
22	0	2	2	1	4	3
23	0	2	2	1	4	3
24	0	2	2	1	4	3
25	0	2	2	1	4	3
26	0	2	2	1	4	3
27	0	2	2	1	4	3
28	14	77	65	41	136	98
29	1	8	6	4	13	10
30	1	8	6	4	13	10
31	3	19	16	10	33	24
32	4	19	16	10	34	25

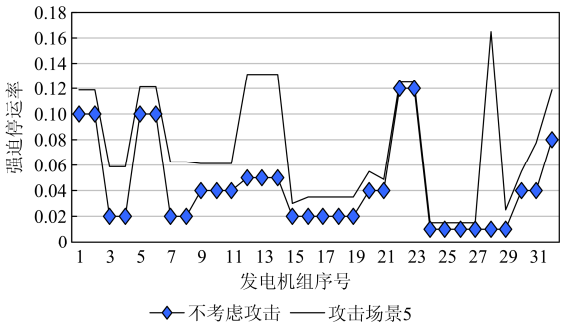


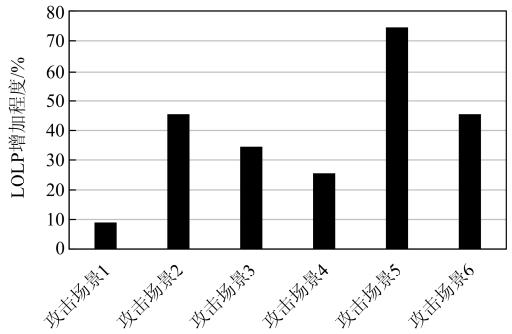
图 7 32 台发电机组的强迫停运率

Fig. 7 Forced outage rate of 32 generator sets

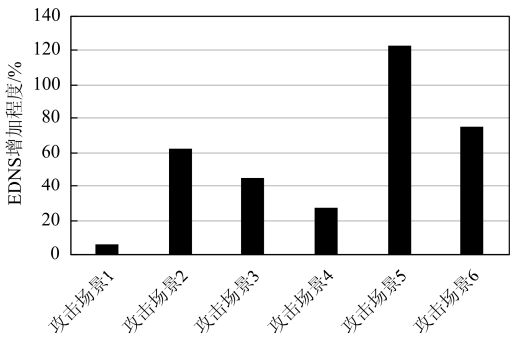
由附录 1 和图 7 可以看出，考虑攻击时，发电机组的强迫停运率会增大。不同的攻击场景对强迫停运率的影响不同，攻击场景 5 造成的影响最大，攻击场景 1 造成的影响最小。还可以看出，同一个攻击场景中，重要性越高的发电机组，强迫停运率值增加得越多，意味着这些重要的发电机组更有可能被网络攻击隔离。

4.3 电力系统可靠性指标

求得各个发电机组修正后的强迫停运率后，根据 3.2 节模型，抽样 20 000 次，可以得到电力系统被攻击前后的 LOLP 和 EDNS。与系统被攻击前的 LOLP 和 EDNS 相比，6 种不同攻击场景造成的电力系统 LOLP 和 EDNS 增加的百分比如图 8 所示。



(a) IEEE-RTS79系统被攻击后LOLP值增加程度



(b) IEEE-RTS79系统被攻击后EDNS值增加程度

图 8 IEEE-RTS79 系统被攻击后 LOLP 和 EDNS 增加程度

Fig. 8 Degree of increase of LOLP and EDNS after attacking the IEEE-RTS79 system

由图 8 可以发现，由攻击场景 5 造成的 LOLP 值和 EDNS 值增加的百分比明显大于其他攻击场景，表明攻击场景 5 给电力系统带来的影响大于其他攻击场景。因此，应该重点针对此攻击场景中的漏洞采取相应的防御措施。

结合各攻击场景上不同的攻击成功次数可以发现：LOLP 值和 EDNS 值增加百分比的大小很大程度上受网络攻击成功次数的影响。攻击成功次数越多， LOLP 和 EDNS 值增加的百分比越大，对电力系统的影响越严重。这也意味着随着攻击者技术的提高和攻击工具的增加以及电力系统网络协议本身漏洞的增加，相应的电力系统可靠性将会降低。

5 结论

随着电力系统越来越依赖于 SCADA，其网络安全不容忽视。本文研究面向 SCADA 的网络攻击对电力系统可靠性的影响，得到以下结论：

1) 分析了 SCADA 的结构和其中存在的漏洞，在此基础上总结了几种常见的使断路器无故障跳闸的攻击方式。建立攻击树模型，评价 6 种攻击场景的成功率。攻击的成功率与攻击的成本、攻击的难度和攻击被发现的可能性有关。

2) 考虑到 SCADA 受网络攻击使断路器跳闸，增加了断路器的不可用率，建立了修正后的强迫停运率模型。该模型考虑了攻击尝试次数、攻击成功的次数和攻击后断路器的不可用时间。

3) 以 IEEE-RTS79 系统为例的仿真结果表明，对于攻击 32 台发电机组，不同的攻击场景对电力系统可靠性的影响不同。攻击场景的成功率越大，攻击场景的成功次数越多，对电力系统可靠性的影响也就越大。

附录 1

IEEE-RTS79 系统发电机组被攻击后的强迫停运率

The forced outage rate of the generator set in the IEEE-RTS79 system after being attacked

序号	机组原始 *FOR*	不同攻击场景下机组修正后的强迫停运率					
		S1	S2	S3	S4	S5	S6
1	0.100	0.102	0.111	0.109	0.106	0.119	0.115
2	0.100	0.102	0.111	0.109	0.106	0.119	0.115
3	0.020	0.025	0.042	0.038	0.031	0.059	0.049
4	0.020	0.025	0.042	0.038	0.031	0.059	0.049
5	0.100	0.102	0.111	0.109	0.106	0.121	0.115
6	0.100	0.102	0.111	0.109	0.106	0.121	0.115
7	0.020	0.025	0.045	0.041	0.034	0.063	0.052
8	0.020	0.025	0.045	0.041	0.034	0.063	0.052
9	0.040	0.042	0.051	0.049	0.046	0.061	0.055
10	0.040	0.042	0.051	0.049	0.046	0.061	0.055
11	0.040	0.042	0.051	0.049	0.046	0.061	0.055
12	0.050	0.058	0.096	0.089	0.074	0.131	0.108
13	0.050	0.058	0.096	0.089	0.074	0.131	0.108
14	0.050	0.058	0.096	0.089	0.074	0.131	0.108
15	0.020	0.021	0.026	0.025	0.023	0.030	0.027
16	0.020	0.021	0.028	0.027	0.025	0.035	0.030
17	0.020	0.021	0.028	0.027	0.025	0.035	0.030
18	0.020	0.021	0.028	0.027	0.025	0.035	0.030
19	0.020	0.021	0.028	0.027	0.025	0.035	0.030

续附表

序号	机组原始 *FOR*	不同攻击场景下机组修正后的强迫停运率					
		S1	S2	S3	S4	S5	S6
20	0.040	0.041	0.048	0.047	0.045	0.055	0.050
21	0.040	0.041	0.046	0.045	0.043	0.049	0.047
22	0.120	0.12	0.122	0.122	0.121	0.125	0.123
23	0.120	0.12	0.122	0.122	0.121	0.125	0.123
24	0.010	0.01	0.012	0.012	0.011	0.015	0.013
25	0.010	0.01	0.012	0.012	0.011	0.015	0.013
26	0.010	0.01	0.012	0.012	0.011	0.015	0.013
27	0.010	0.01	0.012	0.012	0.011	0.015	0.013
28	0.010	0.026	0.098	0.084	0.057	0.165	0.122
29	0.010	0.011	0.019	0.017	0.015	0.025	0.021
30	0.040	0.041	0.049	0.047	0.045	0.055	0.051
31	0.040	0.043	0.062	0.058	0.051	0.078	0.067
32	0.080	0.085	0.102	0.098	0.091	0.119	0.109

参考文献

[1] 俞斌, 郭创新, 王越, 等. 考虑信息系统作用的电力系统可靠性研究[J]. 电力系统保护与控制, 2013, 41(7): 7-13.
YU Bin, GUO Chuangxin, WANG Yue, et al. Power system reliability research considering information system[J]. Power System Protection and Control, 2013, 41(7): 7-13.

[2] 郭庆来, 辛蜀骏, 王剑辉, 等. 由乌克兰停电事件看信息能源系统综合安全评估[J]. 电力系统自动化, 2016, 40(5): 1-3.
GUO Qinglai, XIN Shujun, WANG Jianhui, et al. Comprehensive security assessment for a cyber comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout[J]. Automation of Electric Power Systems, 2016, 40(5): 1-3.

[3] 孙腾飞, 程浩忠, 张立波, 等. 基于改进混合抽样与最小切负荷计算的电力系统可靠性评估方法[J]. 电力系统保护与控制, 2016, 44(13): 96-103.
SUN Tengfei, CHENG Haozhong, ZHANG Libo, et al. Power system reliability evaluation method based on improved hybrid sampling and minimum load shedding[J]. Power System Protection and Control, 2016, 44(13): 96-103.

[4] 李小燕, 丁明, 齐先军. 考虑天气因素的输电网可靠性区间评估及其仿射算法[J]. 电力系统保护与控制, 2016, 44(16): 8-13.
LI Xiaoyan, DING Ming, QI Xianjun. Interval reliability evaluation and affine arithmetic of transmission network considering weather factors[J]. Power System Protection and Control, 2016, 44(16): 8-13.

[5] 丁明, 张瑞华. 发输电组合系统可靠性评估的蒙特卡洛模拟[J]. 电网技术, 2000, 24(3): 9-12.
DING Ming, ZHANG Ruihua. Monte Carlo simulation of reliability evaluation for composite generation and transmission system[J]. Power System Technology, 2000, 24(3): 9-12.

[6] 潘伟, 陈旭, 许立强, 等. 基于无线传感器网络的应急保护通道可靠性及通信性能研究[J]. 电力系统保护与控制, 2016, 44(17): 71-77.
PAN Wei, CHEN Xu, XU Liqiang, et al. Reliability and performance of emergency communication channel based on wireless sensor network[J]. Power System Protection and Control, 2016, 44(17): 71-77.

[7] TEN C W, GOVINDARASU M, LIU C C. Cybersecurity for electric power control and automation systems[C] // IEEE International Conference on Systems, Man and Cybernetics, October 7-10, 2007, Montreal, Canada: 29-34.

[8] TEN C W, GOVINDARASU M, LIU C C. Cybersecurity for critical infrastructures: attack and defense modeling[J]. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 2010, 40(4): 853-865.

[9] TEN C W, LIU C C, GOVINDARASU M. Vulnerability assessment of cybersecurity for SCADA systems using attack trees[C] // Power Engineering Society General Meeting, June 24-28, 2007, Tampa, USA: 1-8.

[10] TEN C W, LIU C C, GOVINDARASU M. Vulnerability assessment of cybersecurity for SCADA systems[J]. IEEE Transactions on Power Systems, 2008, 23(4): 1836-1846.

[11] 叶夏明, 文福栓, 尚金成, 等. 电力系统中信息物理安全风险传播机制[J]. 电网技术, 2015, 39(11): 3072-3079.
YE Xiaming, WEN Fushuan, SHANG Jincheng, et al. Power system information physical security risk communication mechanism[J]. Power System Technology, 2015, 39(11): 3072-3079.

[12] 赵俊华, 文福栓, 薛禹胜, 等. 电力CPS的架构及其实现技术与挑战[J]. 电力系统自动化, 2010, 34(16): 1-7.
ZHAO Junhua, WEN Fushuan, XUE Yusheng, et al. Power CPS architecture and its implementation technology and challenges[J]. Automation of Electric Power Systems, 2010, 34(16): 1-7.

[13] 汤奕, 王琦, 倪明, 等. 电力和信息通信系统混合仿真方法综述[J]. 电力系统自动化, 2015, 39(23): 33-41.
TANG Yi, WANG Qi, NI Ming, et al. Summary of hybrid simulation methods for power and information communication systems[J]. Automation of Electric Power Systems, 2015, 39(23): 33-41.

[14] 郭创新, 陆海波, 俞斌, 等. 电力二次系统安全风险评

估研究综述[J]. 电网技术, 2013, 37(1): 112-118.
GUO Chuangxin, LU Haibo, YU Bin, et al. Research on safety risk assessment of electric secondary system[J]. Power System Technology, 2013, 37(1): 112-118.

[15] 曹志昆, 章杜锡, 董树峰, 等. 改进功能分解的二次系统风险评估方法[J]. 电网技术, 2016, 40(4): 1265-1270.
CAO Zhikun, ZHANG Duxi, DONG Shufeng, et al. Risk assessment method for secondary system of improved functional decomposition[J]. Power System Technology, 2016, 40(4): 1265-1270.

[16] ZHANG Y C, WANG L F, XIANG Y M, TEN C W. Power system reliability evaluation with SCADA cybersecurity considerations[J]. IEEE Transactions on Smart Grid, 2015, 6(4): 1707-1721.

[17] ZHANG Y C, WANG L F, XIANG Y M. Reliability analysis of power grids with cyber vulnerability in SCADA system[C] // IEEE Power & Energy Society General Meeting, July 27-31, 2014, National Harbor, USA: 1-5.

[18] XIANGY M, WANG L F, ZHANG Y C. Power system adequacy assessment with probabilistic cyber attacks against breakers[C] //Pes General Meeting, Conference & Exposition, July 27-31, 2014, National Harbor, USA: 1-5.

[19] 黄慧萍, 肖世德, 孟祥印. 基于攻击树的工业控制系统信息安全风险评估[J]. 计算机应用研究, 2015, 32(10): 3022-3025.
HUANG Huiping, XIAO Shide, MENG Xiangyin. Attack tree-based method for assessing security risk of industrial control system[J]. Computer Application Research, 2015, 32(10): 3022-3025.

[20] STAMP J, MCINTYRE A, RICARDSON B. Reliability impacts from cyber attack on electric power systems[C] // Power Systems Conference & Exposition, March 15-18, 2009, Seattle, USA: 1-8.

[21] 程林, 何剑. 电力系统可靠性原理和应用[M]. 2 版. 北京: 清华大学出版社, 2015.

[22] 史慧杰. 电网运行调度可靠性算法研究及软件实现[D]. 合肥: 合肥工业大学, 2005.
SHI Huijie. Research on reliability algorithm of grid operation scheduling and software implementation[D]. Hefei: Hefei University of Technology, 2005.

[23] 何明亮, 陈泽茂, 龙小东. 一种基于层次分析法的攻击树模型改进[J]. 计算机应用研究, 2016, 33(12): 3755-3758.
HE Mingliang, CHEN Zemao, LONG Xiaodong. An improved method of attack tree based on analytic hierarchy process[J]. Application Research of Computers, 2016, 33(12): 3755-3758.

收稿日期：2017-05-25；　修回日期：2017-07-05

作者简介：

丁　明(1956—)，男，教授，博士生导师，主要研究方向为电力系统规划及可靠性、新能源及其利用、柔性输电系统的仿真控制；E-mail: mingding56@126.com

李晓静(1994—)，女，硕士研究生，主要研究方向电力信息系统耦合分析；E-mail:1906109973@qq.com

张晶晶(1977—)，女，副教授，主要研究方向为电力系统规划及可靠性、电力系统继电保护。

（编辑　魏小丽）