DOI: 10.7667/PSPC162060

智能电网状态维持拓扑攻击及其对经济运行的影响

田继伟，王布宏，李 夏

(空军工程大学信息与导航学院，陕西 西安 710077)

摘要：随着传感器技术、计算机和通信网络技术的迅猛发展，现代电力系统已经成为一个复杂的信息物理系统。信息技术在电力系统大量运用的同时，也增加了电力系统遭受网络攻击的风险。为了评估电力系统面临的攻击威胁，研究了通过“错误”的拓扑信息对智能电网控制中心进行误导的网络攻击。在此类拓扑攻击中，攻击者拦截远程终端单元的数据，对其进行修改，并将修改后的数据发送到控制中心。对不被检测的状态维持拓扑攻击的条件和一个更加现实可行的攻击策略进行了分析研究，并在 IEEE 9-bus 和 14-bus 系统上进行了仿真实验。仿真结果表明该类拓扑攻击能对经济运行造成破坏性影响。

关键词：拓扑攻击；虚假数据注入攻击；状态估计；坏数据检测；最优潮流

State-preserving topology attacks and its impact on economic operation of smart grid

TIAN Jiwei, WANG Buhong, LI Xia

(Information and Navigation College, Air Force Engineering University, Xi’an 710077, China)

Abstract: With rapid advances in sensor, computer and communication networks, modern power systems have become complicated cyber-physical systems. The increasing use of information technologies in power systems has increased the risk of power systems to cyber-attacks. In order to evaluate the threat of attack on the power system, cyber attacks on smart grids aiming at misleading the control center with incorrect topology information are considered. In such topology attacks, an adversary intercepts network and meter data from the remote terminal units, modifies part of them, and forwards the modified data to the control center. A necessary and sufficient condition for an undetectable state-preserving topology attack and a more realistic and feasible attack strategy are analyzed and studied. The proposed attacks are tested with IEEE 9-bus and 14-bus systems. The simulation results show that the topology attack can have the destructive influence on the economic operation.

This work is supported by National Natural Science Foundation of China (No. 61272486) and Research on New Theory and Key Technology of Cryptography in Cloud Computing Security Open Topic Foundation in State Key Laboratory of Information Security (No. 2014-02).

Key words: topology attack; false data injection attack; state estimation; bad data detection; optimal power flow

0 引言

随着智能电网的不断发展，电力网络的自动化程度迅速提高，电力系统传感器数量、决策单元数量和信息网络规模都大大增加[1]。此外，能源互联网的推广使得更多的外部信息通过各种途径影响着电力系统控制决策[2]，电力网络与信息网络的融合交互日趋复杂[3]。现代电网已不再是传统意义上的电力网络，而发展成为具备典型 CPS(Cyber Physical System)特征的电力 CPS。

电力 CPS 借助更大规模的量测系统和更复杂的信息通信系统实时获取电网全面的运行状态信息。因此，电力 CPS 对信息通信系统的依存度越来越高，网络安全在整个电网运行中扮演的角色也愈加重要。针对电网的网络攻击具有隐蔽性高、潜伏期长和攻击代价小的特点[4]，虽然它不直接破坏电力一次设备，但可以通过削弱甚至完全破坏二次系统的正常功能，达到类似于物理攻击的效果，对系统的经济、稳定运行以及社会安定产生重大影响。

基金项目：国家自然科学基金(61272486)；信息安全国家重点实验室开放课题基金(2014-02)

电力系统实时量测由数据采集、数据传输等多个环节最终达到能量管理系统(Energy Management System, EMS)。随着电力系统信息化和网络化的发展，这些环节均可能受到网络攻击，从而产生量测坏数据。电力系统状态估计是量测坏数据检测与辨识的主要手段之一[5]。然而，掌握配置信息及网络拓扑的攻击者，可以构造“合法”的虚假量测，从而成功躲避坏数据检测，导致状态估计结果偏离真实状态，并进一步影响最优潮流和事故分析等分析决策功能的准确性和可靠性。这种通过篡改量测值以影响状态估计结果的攻击方式叫做虚假数据注入攻击[6](False Data Injection Attack, FDIA)。

FDIA 攻击关联性高，难以辨识。2009 年，文献[7]对几种不同的 FDIA 攻击策略进行了详细的分析。自此 FDIA 攻击受到了广泛关注，研究者开始从不同角度研究在不同攻击策略下的 FDIA 攻击及保护措施[8-13]。2013 年，文献[14]提出了和传统的 FDIA 攻击相结合的拓扑攻击，该种攻击通过修改拓扑信息并注入特定的量测信息，使传输到控制中心的错误拓扑信息不被检测出来，以达到“改变”拓扑信息的目的。

本文将探讨该类拓扑攻击对最优潮流和发电成本的影响。本文首先对状态估计、坏数据检测和最优潮流进行介绍，然后对实施该类攻击的方法进行分析，并对该类攻击对发电成本的影响进行了仿真验证。通过本文研究，发现该类拓扑攻击可以在不被检测的情况下改变最优潮流导致发电成本的增加，破坏电网的经济运行。

1　电力系统相关理论

1.1 状态估计

电力系统状态估计是能量管理系统 EMS 和广域监测系统 WAMS(Wide Area Measurement System)执行最优潮流计算、负荷预测和暂态稳定分析等相关分析控制功能的基础，主要作用包括提高量测数据的精度、推算出准确的电力系统的各种电气参数和提高数据采集与监视控制(Supervisory Control and Data Acquisition, SCADA)系统的可靠性等[15]。在具有 N 条母线的电力系统中，状态变量一般取为母线的复电压，包括电压的幅值和相角，除去参考节点，一共有 $2N-1$ 个状态变量，统一表示为 $\boldsymbol{x}=[x_1, x_2, \cdots, x_n]^{\mathrm{T}}$，$n=2N-1$。量测值一般为母线的注入有功和无功功率、支路有功和无功功率或母线电压幅值，假如有 m 个量测值，并且 $m>n$，量测值可统一表示为 $\boldsymbol{z}=[z_1, z_2, \cdots, z_m]^{\mathrm{T}}$，则状态变量和量测值的关系可以表示为

$$\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{e} \tag{1}$$

式中：$\boldsymbol{h}(\boldsymbol{x})$ 表示量测值和状态变量间的非线性关系；$\boldsymbol{e}=[e_1, e_2, \cdots, e_m]^{\mathrm{T}}$ 表示测量误差，并且服从均值为 0、方差为对角矩阵 $\boldsymbol{\Sigma}_{\mathrm{e}}=\mathrm{diag}[\sigma_1^2, \sigma_2^2, \cdots, \sigma_m^2]$ 的高斯分布。

一个正常稳定运行的电力系统，母线电压在额定电压附近，且支路两端相角差很小，而且对于超高压电力网，支路的电阻比电抗小得多。因此，假设所有母线的电压幅值相等且均为 1，忽略线路电阻，则测量值中不存在无功功率，状态变量只有电压相角。此时，状态变量和量测值之间满足线性关系，得到式(2)所示的直流潮流方程

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x} \tag{2}$$

式中：$\boldsymbol{z}$ 为量测值；$\boldsymbol{H}$ 为测量雅可比矩阵；$\boldsymbol{x}$ 为待估计的状态量；$\boldsymbol{e}$ 为测量误差。电力系统状态估计问题以冗余的测量信息为基础，通过加权最小二乘法(Weighted Least-Squares，WLS)来获得状态变量的估计值。

$$\hat{\boldsymbol{x}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{z} \tag{3}$$

1.2 坏数据检测及虚假数据注入攻击

能量管理系统 EMS 接收到的量测数据并不完全准确，它除了带有一定的噪声，还可能含有由于传感器的错误连接、偏移和设备故障，通信系统受到干扰等引起的不良数据。不良数据的存在可能导致状态估计结果受到影响，使其偏离实际情况。

由于状态估计以冗余的测量信息为基础，其中的测量值可能含有坏数据或者恶意数据，这就需要检测坏数据并加以剔除，以确保状态估计结果的可靠性。为消除不良数据对状态估计结果的影响，以残差为基础的不良数据检测方法得到了广泛应用。残差的表达式为

$$\boldsymbol{r}=\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}} \tag{4}$$

检测坏数据的判据是：$\|\boldsymbol{r}\|<\tau$，τ 为判断的阈值。如果 $\|\boldsymbol{r}\|<\tau$ 成立，认为没有坏数据；否则就要剔除相应的坏数据并重新进行状态估计，直到通过坏数据检测为止[16]。

虚假数据注入攻击 FDIA 就是利用了该检测方法的缺陷，若用 $\boldsymbol{a}=[a_1, a_2, \cdots, a_m]^{\mathrm{T}}$ 表示攻击者在量测值中注入的虚假数据向量，则篡改后的测量值为 $\boldsymbol{z}_{\mathrm{bad}}=\boldsymbol{z}+\boldsymbol{a}$，此时状态变量的估计值为 $\boldsymbol{x}_{\mathrm{bad}}=\hat{\boldsymbol{x}}+\boldsymbol{c}$，$\boldsymbol{c}=[c_1, c_2, \cdots, c_n]^{\mathrm{T}}$ 表示攻击者在状态变量中引入的误差向量。此时残差表达式为

$$\|\boldsymbol{r}\|=\|\boldsymbol{z}_{\text{bad}}-\boldsymbol{H}\boldsymbol{x}_{\text{bad}}\|=\left\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(\hat{\boldsymbol{x}}+\boldsymbol{c})\right\|=\left\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}\right\| \tag{5}$$

当 $\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$ 时，有式(6)成立。

$$\|\boldsymbol{r}\|=\|\boldsymbol{z}_{\text{bad}}-\boldsymbol{H}\boldsymbol{x}_{\text{bad}}\|=\left\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\right\| \tag{6}$$

此时，传统的不良数据检测方法无法发现攻击的存在，攻击者可以任意地篡改量测值和状态变量，危害到电力系统的安全稳定运行。

1.3 最优潮流

最优潮流是指从电力系统稳定运行的角度来调整系统中各种控制设备的参数，在满足节点正常功率平衡及各种安全指标的约束下，实现目标函数最小化的优化过程[17-19]。

最优潮流模型通常的数学描述如下。

目标函数为

$$\min\sum f_i(P_i)+c_{\text{s}}^{\text{T}}\boldsymbol{J} \tag{7}$$

约束条件为

$$\sum\boldsymbol{P}=\sum(\boldsymbol{D}-\boldsymbol{J}) \tag{8}$$

$$\boldsymbol{F}=\boldsymbol{S}\times(\boldsymbol{U}\times\boldsymbol{P}-\boldsymbol{V}\times(\boldsymbol{D}-\boldsymbol{J})) \tag{9}$$

$$\boldsymbol{P}_{\min}\le\boldsymbol{P}\le\boldsymbol{P}_{\max} \tag{10}$$

$$-\boldsymbol{F}_{\max}\le\boldsymbol{F}\le\boldsymbol{F}_{\max} \tag{11}$$

$$\boldsymbol{0}\le\boldsymbol{J}\le\boldsymbol{D} \tag{12}$$

式中：$\boldsymbol{P}$、$\boldsymbol{D}$、$\boldsymbol{J}$、$\boldsymbol{F}$ 分别为发电量、负荷量、切负荷量以及支路潮流量；f_i 为第 i 个发电厂发电成本函数(一般用二次函数表达式来表示)；c_{s} 为切负荷单位成本；$\boldsymbol{U}$、$\boldsymbol{V}$ 分别为母线发电厂关联矩阵和母线负荷关联矩阵；$\boldsymbol{S}$ 为转移因子矩阵。式(8)为功率平衡方程，式(9)为支路潮流方程，式(10)为发电机的发电量限制，式(11)为支路潮流的条件限制，式(12)表示切负荷量不超过负荷实际值。

当攻击者实施下文提到的拓扑攻击时，会导致电力系统观测到的拓扑信息发生改变，而基于拓扑信息和系统状态的最优潮流也势必会受到攻击的影响。

2 不被检测的拓扑攻击

智能电网控制中心从遍布整个电力系统的仪表和传感器接收两种类型的数据：一种是电力网络拓扑数据 $\boldsymbol{s}\in\{0,1\}^d$，代表断路器的状态(0 代表开，1 代表关)。另一种是测量数据 $\boldsymbol{z}\in\boldsymbol{R}^m$，其中包括母线注入功率和线路功率的量测值[12]。

网络拓扑是极其重要的电力系统信息，在能量管理系统 EMS 的很多模块都发挥着关键的作用。电力系统故障或者恶意的物理攻击可能导致网络拓扑的改变，通常情况下，这种拓扑的变化可以被检测出来。然而，有经验的攻击者可以以一种不被检测的方式实施“改变”系统拓扑的网络攻击(文中提到的此类攻击只是使控制中心观测到的拓扑信息发生变化，真实的物理拓扑并未发生变化)。

如图 1 所示，攻击者可以实施中间人攻击(Man-in-the-Middle Attack, MITM)：拦截 RTU (Remote Terminal Units, 远程终端单元)的数据 $(\boldsymbol{s},\boldsymbol{z})$，并对其进行修改，将修改后的数据 $(\bar{\boldsymbol{s}},\bar{\boldsymbol{z}})$ 发送到控制中心。

$$\bar{\boldsymbol{s}}=\boldsymbol{s}+\boldsymbol{b}(\boldsymbol{mod}2) \tag{13}$$

$$\bar{\boldsymbol{z}}=\boldsymbol{z}+\boldsymbol{a} \tag{14}$$

式中：$\boldsymbol{a}$ 为测量值攻击向量，$\boldsymbol{b}$ 为线路状态攻击向量。

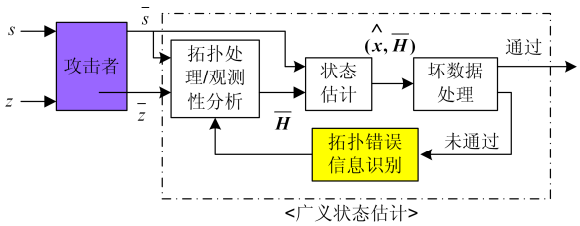

图 1 广义状态估计攻击模型

Fig. 1 Attack model with generalized state estimation

这里我们考虑一种特殊的拓扑攻击：状态维持拓扑攻击，即在“改变”拓扑信息的情况下(改变控制中心观测到的拓扑信息)，通过量测值的修改，使得系统当前的状态变量保持不变。此时，在不存在噪声的情况下，测量值攻击向量满足式(15)。

$$\boldsymbol{a}=\bar{\boldsymbol{H}}\boldsymbol{x}-\boldsymbol{H}\boldsymbol{x} \tag{15}$$

其中，$\bar{\boldsymbol{H}}$ 为拓扑信息“改变”后的测量雅可比矩阵(拓扑信息影响测量雅克比矩阵)。

上述攻击向量的构建需要攻击者掌握系统测量矩阵以及系统的状态变量信息，实现起来有很大难度。在此，考虑一种简单的情形：假如攻击者试图“断开”某条输电线路，则只需要修改该线路的相关测量值。如图 2 所示，在攻击前，z_{ij} 是从节点 i 到节点 j 的潮流测量值，满足 $z_{ij}=B_{ij}(x_i-x_j)$，B_{ij} 为线路的电纳，x_i、x_j 分别为节点 i 和 j 的相角。则测量矩阵中的相应行为 $h(i,j)=\left[0\cdots0\ \underbrace{B_{ij}}_{\text{第}i\text{个}}\ 0\cdots0\ \underbrace{-B_{ij}}_{\text{第}j\text{个}}\ 0\cdots0\right]$。在攻击后，线路“断开”，测量值 $z_{ij}=0$，新的测量矩阵中相应的行为

$\overline{h(i,j)}=\left[\begin{matrix}0\cdots0 & \underbrace{0}_{第i个} & 0\cdots0 & \underbrace{0}_{第j个} & 0\cdots0\end{matrix}\right]$，即全变为0。而对于节点 i 的注入功率测量值 z_i 来说，其为所有的流出节点 i 的潮流测量值的总和，其测量矩阵的相应行为所有相应支路潮流测量值对应列的总和。

在图 2 中，为了改变线路的拓扑信息且不被检测到，需要对测量值作如下修改：

1) 对于输电线路 (i,j)，将母线 i 处的注入功率测量值减去 z_{ij}，将母线 j 处的注入功率测量值减去 z_{ji}。

2) 对于输电线路 (i,j)，将 z_{ij} 和 z_{ji} 均改为 0。

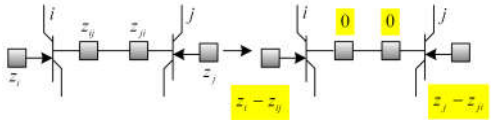

图 2 攻击特定线路需修改的测量信息

Fig. 2 Manipulated measurements around target line

在上述这种简单的攻击形式中，我们只需掌握特定攻击线路的局部拓扑信息以及相关的测量信息，即可以实现状态维持拓扑攻击。在攻击向量成功躲避坏数据检测后，系统观测到的电网拓扑信息发生“变化”，而当前状态变量保持不变。随后，系统根据拓扑信息变化的“事实”，其最优潮流模块将重新对系统进行潮流分配，以达到“新的”拓扑信息下的最优潮流。

3　仿真分析

为了评估上述攻击的有效性和对最优潮流造成的影响，将在 IEEE 9-bus(图 3)和 14-bus 系统[19](图 4)上使用最优潮流模型进行仿真实验，并对该类攻击对发电成本造成的影响进行实验分析。

在仿真试验中，支路潮流约束、发电机功率约束、负荷以及发电成本函数等信息均来自 matpower[20](相关参数均可从中得到)。其中，电力系统发电机成本函数为机组有功出力的二次函数，其表达式为 $f_i(P_i)=a_i(P_i^2)+b_i(P_i)+c_i$，$P_i$ 为第 i 个机组的有功出力，a_i、b_i、c_i 为成本函数的系数。IEEE 9-bus 和 14-bus 的发电成本函数和发电机功率约束如表 1 和表 2 所示。试验中，将状态变量视为具有较小方差的高斯分布，其均值为相应系统正常运行状态时的数据，在每一次蒙特卡洛试验中，产生符合上述高斯分布的状态变量，并使用潮流模型产生含有高斯噪声的测量值(测量噪声标准差取为测量值的 1%)。攻击者根据网络拓扑信息、测量值信息，构造并注入相应的攻击向量，传输到控制中心。控制中心使用状态估计器进行状态估计以及基于残差的坏数据检验。如果控制中心没有检测到攻击，将根据拓扑信息的“变化”重新进行最优潮流计算。

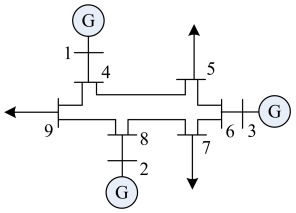

图 3 IEEE 9-bus 系统

Fig. 3 IEEE 9-bus system

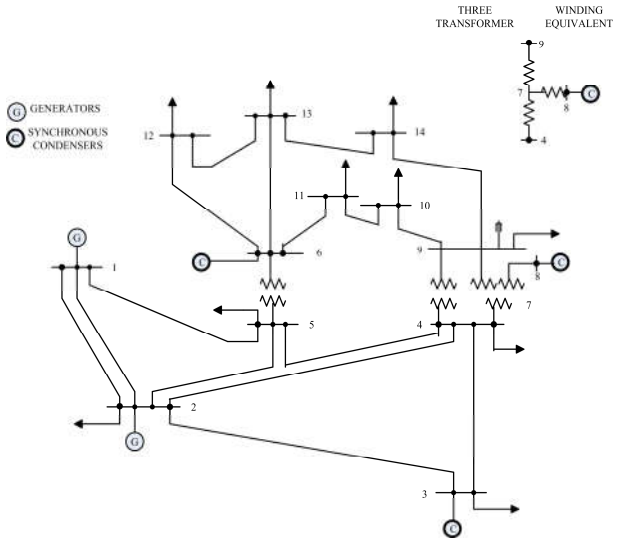

图 4 IEEE 14-bus 系统

Fig. 4 IEEE 14-bus system

表 1 IEEE 9-bus 系统发电机相关参数

Table 1 Parameter about generators in IEEE 9-bus system

发电机编号	母线编号	发电机成本函数系数			最大功率/MW	最小功率/MW
		a	b	c		
1	1	0.11	5	150	150	10
2	2	0.085	1.2	600	100	10
3	3	0.1225	1	335	150	10

表 2 IEEE 14-bus 系统发电机相关参数

Table 2 Parameter about generators in IEEE 14-bus system

发电机编号	母线编号	发电机成本函数系数			最大功率/MW	最小功率/MW
		a	b	c		
1	1	0.043 029 3	20	0	332.4	0
2	2	0.25	20	0	140	0
3	3	0.01	40	0	100	0
4	6	0.01	40	0	100	0
5	8	0.01	40	0	100	0

这里假设攻击者试图“断开”系统中的一条传输线路(这里的“断开”并不是物理上的断开，而是通过篡改数据使得系统控制中心“认为”线路断开了)。图 5 展示了在 IEEE 9-bus 系统上，通过攻击“断开”不同的线路时，检测到攻击的概率(IEEE 9-bus 系统一共 9 条线路，这里只攻击其中的 6 条线路)。图中显示，在大部分的线路上，检测到攻击的概率都很低，大概在 0.08 左右。图 6 展示了在 IEEE 14-bus 系统上，通过攻击“断开”不同的线路时，检测到攻击的概率(IEEE 14-bus 系统一共 20 条线路，但是在攻击 7-8 线路时，将导致系统潮流算法不收敛，故仿真实验时只针对剩下的 19 条线路)。图中显示，在大部分的线路上，检测到攻击的概率都很低，大概在 0.06 左右。表 3 中展示了 IEEE 14-bus 系统攻击部分线路时的攻击向量数据的组成(只显示了攻击者需要篡改的数据)。

同时，攻击也对最优潮流及发电成本造成了影响。图 7 和图 8 分别展示了在 IEEE 9-bus 和 14-bus 系统上攻击不同的线路时发电成本的变化。图 7 中，编号 0 代表系统未遭受攻击时的发电成本，其余分别代表攻击不同的线路时发电成本的变化。由图 7 中可以看出，在大部分的线路上，发电成本均有所增加，尤其是攻击线路 9-4 时，发电成本由 5467.16 美元/h 增加到 5661.63 美元/h，这导致了资源的极大浪费，破坏了系统的经济运行。图 8 中，编号 0 代表系统未遭受攻击时的发电成本，编号 1-19 分别代表攻击不同的线路时发电成本的变化。由图 8 中可以看出，在大部分的线路上，发电成本均有所增加，尤其是攻击编号线路 1 时(即线路 1-2)，发电成本由 9692.88 美元/h 增加到 10 524.55 美元/h，这导致了资源的极大浪费，破坏了系统的经济运行。

表 3 IEEE 14-bus 系统攻击某线路需篡改的测量数据

Table 3 Manipulated measurements around target line in IEEE 14-bus system

攻击的线路	需要篡改的测量数据/MW								
	母线测量数据						支路测量数据		
	母线编号	真实值	篡改后	母线编号	真实值	篡改后	支路	真实值	篡改后
3-4	3	94.2	70.01	4	97.8	121.99	3-4	24.19	0
4-5	4	97.8	36.05	5	7.6	69.35	4-5	61.75	0
4-9	4	97.8	114.35	9	29.5	12.95	4-9	16.55	0
9-10	9	29.5	35.27	10	9	3.23	9-10	5.77	0
9-14	9	29.5	39.14	14	14.9	5.26	9-14	9.64	0
10-11	10	9	5.77	11	3.5	6.73	10-11	3.23	0
12-13	12	6.1	7.61	13	13.5	11.99	12-13	1.51	0
13-14	13	13.5	18.76	14	14.9	9.64	13-14	5.26	0

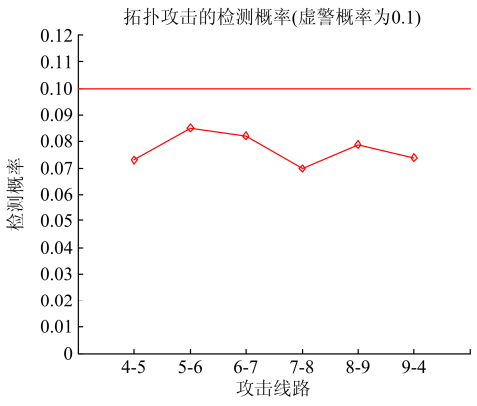

图 5 IEEE 9-bus 系统检测概率(1000 次蒙特卡洛试验)

Fig. 5 Detection probability in IEEE 9-bus system (1000 Monte Carlo runs)

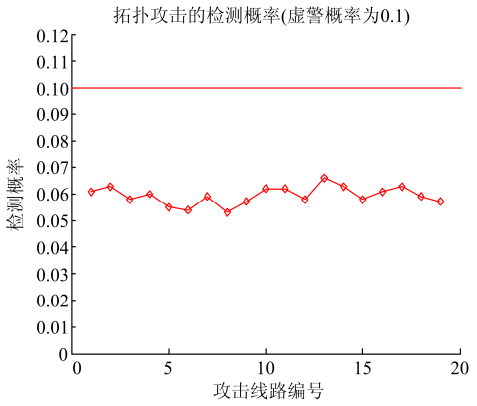

图 6 IEEE 14-bus 系统检测概率(1000 次蒙特卡洛试验)

Fig. 6 Detection probability in IEEE 14-bus system (1000 Monte Carlo runs)

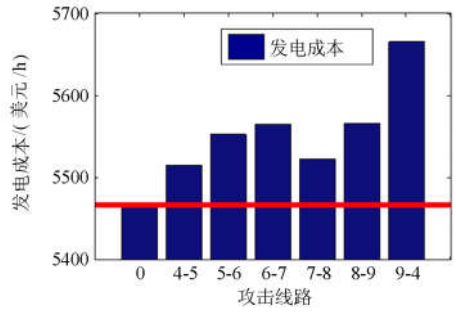

图 7 拓扑攻击对发电成本造成的影响(IEEE 9-bus)

Fig. 7 Impact of topology attacks on generation cost (IEEE 9-bus)

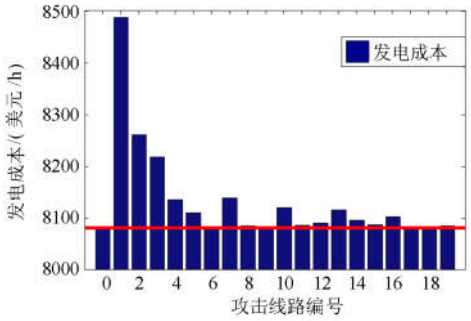

图 8 拓扑攻击对发电成本造成的影响(IEEE 14-bus)

Fig. 8 Impact of topology attacks on generation cost (IEEE 14-bus)

4 结语

信息通信系统和电力系统的深度融合使得现代电力系统面临信息安全的严峻挑战。攻击者对电力系统进行攻击的方式多种多样，除了引起关注的虚假数据注入攻击等攻击方法外，和传统虚假数据注入攻击相结合的拓扑攻击同样能够躲避电力系统的检测，并对电力系统造成影响。本文针对智能电网的拓扑攻击进行分析，研究了躲避检测的拓扑攻击的方法和策略，通过仿真实验仿真分析了该类拓扑攻击对最优潮流和发电成本的影响，发现该类攻击导致发电成本增加，破坏了系统的经济运行，浪费了能源和资源。当然，该类拓扑攻击也可能对电力系统的安全运行[21]造成更加严重的影响(如发生级联故障、大停电事故和电网崩溃等)，我们也需要提出针对性的防御策略应对此类攻击，这些都是下一步的研究方向。

参考文献

[1] 郭庆来, 辛蜀骏, 孙宏斌, 等. 电力系统信息物理融合建模与综合安全评估: 驱动力和构想[J]. 中国电机工程学报, 2016, 36(6): 1481-1489.
GUO Qinglai, XIN Shujun, SUN Hongbin, et al. Power system cyber-physical modelling and security assessment: motivation and ideas[J]. Proceedings of the CSEE, 2016, 36(6): 1484-1489.

[2] 丁少倩, 林涛, 翟学, 等. 基于短路容量的含大规模新能源接入的电网状态脆弱性评估方法研究[J]. 电力系统保护与控制, 2016, 44(13): 40-47.
DING Shaoqian, LIN Tao, ZHAI Xue, et al. Research on state vulnerability assessment method of grid with large scale new energy sources based on short-circuit capability[J]. Power System Protection and Control, 2016, 44(13): 40-47.

[3] 杨佩, 蔡皓, 裘洪彬, 等. 面向能源互联网的大数据关键技术研究[J]. 电力信息与通信技术, 2016(4): 9-12.
YANG Pei, CAI Hao, QIU Hongbin, et al. Research on key technologies of big data for energy interconnection[J]. Electric Power Information and Communication, 2016(4): 9-12.

[4] 刘念, 余星火, 张建华. 网络协同攻击: 乌克兰停电事件的推演与启示[J]. 电力系统自动化, 2016, 40(6): 144-147.
LIU Nian, YU Xinghuo, ZHANG Jianhua. Coordinated cyber-attack: inference and thinking of incident on Ukrainian power grid[J]. Automation of Electric Power Systems, 2016, 40(6): 144-147.

[5] 于尔铿. 电力系统状态估计[M]. 北京: 中国水利出版社, 1985.

[6] 王先培, 田猛, 董政呈, 等. 输电网虚假数攻击综述[J]. 电网技术, 2016, 40(11): 3406-3414.
WANG Xianpei, TIAN Meng, DONG Zhengcheng, et al. Survey of false data injection attacks in power transmission systems[J]. Power System Technology, 2016, 40(11): 3406-3414.

[7] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids[C] // Proceedings of the 16th ACM conference on Computer and Communications Security, New York, USA, November 9-13, 2009: 21-32.

[8] SANDBERG H, TEIXEIRA A, JOHANSSON K H. On security indices for state estimators in power networks[C] // First Workshop on Secure Control Systems (SCS), Stockholm, 2010.

[9] DAN G, SANDBERG H. Stealth attacks and protection schemes for state estimators in power systems[C] // 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, October 4-6, 2010: 214-219.

[10] KOSUT O, LIYAN J, THOMAS R J, et al. Malicious data

attacks on the smart gird[J]. IEEE Transactions on Smart Grid, 2011, 2(4): 645-658.

[11] KIM J, TONG L. On the topology attack of a smart grid: undetectable attacks and countermeasures[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(7): 1294-1305.

[12] RAHMAN M A, MOHSENIAN-RAD H. False data injection attacks against nonlinear state estimation in smart power grids[C] // IEEE Power and Energy Society General Meeting (PES): IEEE, 2013: 1-5.

[13] 王昕, 田猛, 赵艳峰, 等. 一种基于状态估计的新型窃电方法及对策研究[J]. 电力系统保护与控制, 2016, 44(23): 141-146.
WANG Xin, TIAN Meng, ZHAO Yanfeng, et al. A new kind of electricity theft based on state estimation and countermeasure[J]. Power System Protection and Control, 2016, 44(23): 141-146.

[14] KIM J, TONG L. On topology attack of a smart grid: undetectable attacks and countermeasures[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(7): 1294-1305.

[15] 赵俊华, 梁高琪, 文福拴, 等. 乌克兰事件的启示: 防范针对电网的虚假数据注入攻击[J]. 电力系统自动化, 2016, 40(7): 149-151.
ZHAO Junhua, LIANG Gaoqi, WEN Fushuan, et al. Lessons learnt from the Ukrainian blackout: protecting power grids against false data injection attacks[J]. Automation of Electric Power Systems, 2016, 40(7): 149-151.

[16] 朱杰, 张葛祥, 王涛, 等. 电力系统状态估计欺诈性数据攻击及防御综述[J]. 电网技术, 2016, 40(8): 2406-2415.
ZHU Jie, ZHANG Gexiang, WANG Tao, et al. Overview of fraudulent data attack on power system state estimation and defense mechanism[J]. Power System Technology, 2016, 40(8): 2406-2415.

[17] 李彩华, 郭志忠. 最优潮流的发展[J]. 电力系统保护与控制, 2002, 30(1): 1-6.
LI Caihua, GUO Zhizhong. Development of optimal power flow[J]. Power System Protection and Control, 2002, 30(1): 1-6.

[18] 黄国栋, 崔晖, 许丹, 等. 安全约束经济调度中有功潮流调整方法[J]. 电力系统保护与控制, 2016, 44(4): 91-96.
HUANG Guodong, CUI Hui, XU Dan, et al. A method of active power flow adjustment in security constrained economic dispatch[J]. Power System Protection and Control, 2016, 44(4): 91-96.

[19] 公茂法, 柳岩妮, 姜文, 等. 基于可信状态集合的状态估计方法在最优潮流中的应用[J]. 电力系统保护与控制, 2016, 44(17): 78-82.
GONG Maofa, LIU Yanni, JIANG Wen, et al. State estimation method based on trusted state set in the application of the optimal power flow[J]. Power System Protection and Control, 2016, 44(17): 78-82.

[20] ZIMMERMAN R D, MURILLO-SÁNCHEZ C E, THOMAS R J. MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education[J]. IEEE Transactions on Power Systems, 2011, 26(1): 12-19.

[21] BO Zhiqian, LIN Xiangning, WANG Qingping, et al. Developments of power system protection and control[J]. Protection and Control of Modern Power Systems, 2016, 1(1): 1-8. DOI 10.1186/s41601-016-0012-2.

收稿日期：2016-12-16； 修回日期：2017-04-14

作者简介：

田继伟(1993—)，男，通信作者，硕士研究生，主要研究方向为智能电网、网络安全； E-mail: tianjiwei2016@163.com

王布宏(1975—)，男，教授，博士生导师，主要研究方向为信号处理、信息安全、智能电网； E-mail: adhd2016@163.com

李 夏(1991—)，男，博士研究生，主要研究方向为信息安全、智能电网、电力系统分析。E-mail: 2417162923@qq.com

(编辑 葛艳娜)