

基于部分配置信息的错误数据注入攻击

李 勒, 洪爽俊, 张 驰

(中国科学技术大学 电子工程与信息科学系, 安徽 合肥 230027)

摘 要: 分析了电力系统配置矩阵, 并提出了基于部分配置信息的错误数据注入攻击, 使得攻击者的第一个攻击需求也是最强的一个攻击需求得到了大幅度的减弱. 最后通过对 IEEE 测试系统进行仿真分析, 验证了方案的有效性和可行性.

关键词: 电力系统状态估计; 错误数据注入攻击; 信息物理融合系统; 安全; 信息战

中图分类号: TP393.0

文献标识码: A

文章编号: 1000-7180(2014)02-0085-05

False Data Injection Attack Based on Partial Configuration Information

LI Le, HONG Shuang-jun, ZHANG Chi

(Dept. of Electronics Engineering and Information, University of Science and Technology of China, Hefei 230027, China)

Abstract: False data injection attack (FDIA), systematically tampering with measurements of power system, could bypass the classical bad data detection algorithm and then result in wrong output of power system state estimation, which poses a great threat to power system. However, FDIA also gives great challenges to attackers. To launch FDIA, attackers have to access the current power system configuration information firstly and manipulate the measurements of meters secondly. To lower the first attack condition, we analysis the configuration matrix of power system and propose FDIA based on partial configuration information, which greatly alleviates burdens on attackers. At last, we demonstrate the success of this attack through simulation of IEEE test systems.

Key words: power system state estimation; false data injection attack; information warfare; CPS; security

1 引言

电力系统是重要的国家基础设施, 其安全稳定运行对社会稳定和国民经济快速健康发展起关键作用^[1]. 美国在 1999 年于第 63 号总统法令中将电力供应部门确定为国家 8 大关键基础设施部门. 美国在 2001 年 1 月颁布了《爱国者法案》中明确指出, “关键性基础设施”指的是“对国家具有重要意义的物理或信息系统及资产的总和, 其瘫痪或被摧毁将对国家国防、经济、卫生和安全领域产生破坏性影响”. 在我国, 由国家重大基础研究计划(“九七三”计划)所资助的首批 10 个重大项目中, 就有电力系统灾变防治与经济运行重大科学问题的研究项目^[2]. 电力基础设施安全已上升到国家安全的范畴.

随着信息化的逐步深入, 信息战(包括网络战)对当今的战争产生了很大的格局变化, 受影响的不仅是战场上的军事对抗, 政府和国家特殊部门的系统, 还包括金融网、电力网、通信网、导航系统和其他各类基础设施^[3-4]. 美国已将电力系统作为未来网络战攻击目标之一.

电力系统状态估计利用工业数据采集和控制系统(SCADA 系统)提供的测量数据的冗余度来提高数据精度, 自动排出随机干扰所引起的错误信息, 估计或预报系统的运行状态^[5]. 它构建了电力系统在线安全分析功能的核心模块, 像个滤波器架设在原始数据和所有需要使用当前系统状态最可靠的数据基础的应用之间.

然而从信息战角度来看, 状态估计的数据来源

收稿日期: 2013-03-15; 修回日期: 2013-05-10

基金项目: 国家自然科学基金(61201240)

SCADA 系统是信息化战争中敌对势力实施硬打击和软杀伤的重要目标^[6]. 2010 年,“震网”病毒正是通过入侵了西门子公司提供的 SCADA 系统——SIMATIC WinCC 系统从而对伊朗核电站进行了攻击^[6]. 在理论上, Y. Liu 等研究者从攻击者的角度给出了针对电力系统状态估计的错误数据注入攻击^[7], 该方法通过篡改电表测量值(如入侵 SCADA 系统), 并可绕过传统的错误数据监测, 从而成功的影响状态估计, 以此来对电力系统进行攻击. 错误数据注入攻击^[7]的提出也引起了不少研究者的关注^[8-14]. 国内的研究者杨清宇等人综述了错误数据注入攻击的研究现状^[1].

错误数据注入攻击能给电力系统带来致命的危害, 但同时它的确给攻击者提出了很大的考验. 第一, 攻击者必须知道目标电力系统的目前配置, 特别是系统的拓扑. 第二, 攻击者能操控一定数量的电表测量值. 本文研究了错误数据注入攻击, 从降低错误数据注入攻击的第一个要求, 提出了基于部分电力系统配置信息构建错误数据注入攻击的方案.

2 相关研究

Y. Liu 等^[7]指出, 如果一个攻击者知道电力系统的当前配置, 那么所有已有的基于 DC 潮流模型的坏测量值检测和识别方法都有相似的缺陷, 使得攻击者可以绕过它们的防护. 最基本的理由就是, 所有的已有的基于 DC 潮流模型坏测量值检测和识别算法都基于一个假设, 即“当坏测量值出现时, 观察到的测量值和它们对应的估计值的差的平方将很大”. 而文献^[7]证明了该假设不总是成立, 并给出了构建可绕过传统检测和识别方法的攻击向量的方法, 从攻击者角度实现了错误数据的注入攻击.

错误数据注入攻击^[7]的提出也引起了不少研究者的关注. 文献^[8-11]从攻击防护技术出发, 对错误数据注入攻击进行了进一步研究. Bobba 等人给出了需要保护的电表数量的下界, 以防止错误数据注入攻击的构建, 同时也指出广义错误数据注入攻击的存在性^[8]. Sandberg 等人通过操纵一个电流测量值, 并用一种一致的行为来改变相关的测量值, 使得不会激发警报, 从而构建秘密的恶意数据注入攻击, 并在文中引入了量化构建错误数据注入攻击最小代价的一些指数^[9]. Kosut 等提出了贝叶斯框架, 利用先验知识来帮助检测错误数据注入攻击^[10]. 此后 Kosut 等进一步研究了错误数据注入攻击, 使用图论的方法提出了多项式时间复杂度的算法用于寻找

最小尺寸的攻击向量, 并提出了基于最大似然比测试检测器用于检测和定位攻击^[11]. 此外, 文献^[12-13]对错误数据注入攻击应用的角度, 对错误数据注入攻击对实时电力市场的影响进行了研究.

3 预备知识

3.1 DC 状态估计

对于基于 DC 潮流模型的状态估计^[15], 电力系统测量值和电力系统状态变量间的关系可以用以下线性回归模型表示,

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \quad (1)$$

n 维向量 $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$ 表示待估计的电力系统状态(在 DC 潮流模型, n 个状态变量 x_i 实际上为 n 个母线的电压相角 θ_i);

m 维向量 $\mathbf{z} = (z_1, z_2, \dots, z_m)^T$ 表示布设在电网中的测量电表测得测量值;

$\mathbf{H}$ 为 $m \times n$ 阶的导纳矩阵;

$\mathbf{e} = (e_1, e_2, \dots, e_m)^T$ 表示测量值中的随机误差.

测量值 $\mathbf{z}$ 和状态变量 $\mathbf{x}$ 即通过式(1)的线性方程组关联到一起.

通常, 会在电网中布设远远多于状态变量数的测量电表, 即 $m \gg n$. 于是 $\mathbf{z} = \mathbf{H}\mathbf{x}$ 构成了含有 m 个方程和 n 个未知数的超定线性方程组, 考虑到误差 $\mathbf{e}$ 的存在, 就会导致以上超定线性方程组有矛盾方程, 一般无法直接求解. 在状态估计中通常使用以下三个统计准则对状态向量 $\mathbf{x}$ 进行最优估计, 即最大似然估计、加权最小二乘法估计、最小方差估计^[12]. 当电表测量误差服从均值为 0 的正态分布时, 由以上三个准则将导出相同的最优估计结果,

$$\hat{\mathbf{x}} = (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{z} \quad (2)$$

式中, $\mathbf{W} = \mathbf{e} \mathbf{e}^T$ 是一个对角矩阵, 为测量电表误差的协方差矩阵, 其对角线中 σ_i^2 为第 i 个电表的方差 ($1 \leq i \leq m$).

坏值检测: 由于各种原因如电表错误和恶意攻击等都会引入坏测量值. 文献^[15-17]给出了许多关于坏值检测、识别和纠正的研究以保护状态估计. 直观的, 正常的电表测量值通常产生与实际值接近的状态变量. 因此, 在好值和坏值间通常存在着不一致. 电力系统研究者提出计算测量值残差 $\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$, 并使用残差的二阶范数 $\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\|$ 来判断坏值是否出现. $\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\|$ 将与阈值 τ 进行比较, 当 $\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| > \tau$ 时意味着有坏值存在.

假设所有的状态变量是相互独立的并且电表误差符合正态分布. 我们将 $\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\|^2$ 记为 $L(\mathbf{x})$,

服从自由度 $\nu = m - n$ 的 $\chi^2(\nu)$ 分布. 其中 τ 可由显著水平为 α 的假设检验过程确定, $\Pr(L(\mathbf{x}) \geq \tau^2) = \alpha$, 即 $L(\mathbf{x}) \geq \tau^2$ 的概率等于 α . $L(\mathbf{x}) \geq \tau^2$ 也就意味着很可能存在坏测量值, 于是状态估计器将对此发出警报, 并且该警报误报的概率为 α . 为了控制误报率, 可以把 α 设定的足够小. 此时, 一旦发出警报, 则有充分的把握断定坏值的出现. 但同时, 过小的 α 会导致漏检的概率变大. α 的大小选定需要根据系统的安全要求进行确定.

3.2 错误数据注入攻击

错误数据注入攻击^[7] 通过对原始测量值向量 $\mathbf{z} = (z_1, \dots, z_m)^T$ 注入一个非零攻击向量 $\mathbf{a} = (a_1, \dots, a_m)^T$, 从而得到含有恶意数据的测量值向量 $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$. 当将 $\mathbf{z}_a$ 输入状态估计器时, 将得到错误的状态估计向量 $\hat{\mathbf{x}}_{\text{bad}} = \hat{\mathbf{x}} + \mathbf{c}$, 其中 $\mathbf{c}$ 为攻击带来的错误向量.

定理1 假设原始测量值 $\mathbf{z}$ 能通过坏值检测. 那么当攻击向量 $\mathbf{a}$ 是 $\mathbf{H}$ 矩阵列向量的线性组合时, 即 $\mathbf{a} = \mathbf{H}\mathbf{c}$, 恶意测量值 $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$ 也能通过坏值检测.

证明: 由恶意测量值 $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$ 估计得到的电网状态变量如下:

$$\begin{aligned}\hat{\mathbf{x}}_{\text{bad}} &= (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{z}_a \\ &= \hat{\mathbf{x}} + (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{a}\end{aligned}\quad (3)$$

对于任意 $\mathbf{c}$, 如果 $\mathbf{a} = \mathbf{H}\mathbf{c}$, 则测量残差的2阶范数如下:

$$\begin{aligned}\|\mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_{\text{bad}}\| &= \|\mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{a})\| \\ &= \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{H}(\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{a})\| \\ &= \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{H}\mathbf{c} - \mathbf{H}\mathbf{c})\| \\ &= \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| \\ &\leq \tau\end{aligned}\quad (4)$$

τ 为检测阈值. $\mathbf{z}_a$ 的测量残差小于阈值 τ , 因此 $\mathbf{z}_a$ 也能通过坏值测量. 该攻击注入的错误为

$$\hat{\mathbf{x}}_{\text{bad}} - \hat{\mathbf{x}} = (\mathbf{H}^T \mathbf{W} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{W} \mathbf{a} = \mathbf{c}.$$

如上得证.

4 基于部分配置信息的错误数据注入攻击

为了构建错误数据注入攻击, 攻击者必须知道目标电力系统的目前配置矩阵 $\mathbf{H}$. 通常, 这种信息只有电力公司的控制中心才可能使用. 考虑到控制中心的敏感性, 对于控制中心的物理访问更是高度管制和保护的. 因此, 攻击者获取配置信息以发动该攻击时非常不易的. 我们的思路是尽可能地降低错误数据注入攻击的第一个要求, 尝试只有部分 $\mathbf{H}$ 矩阵

信息时构建攻击向量.

4.1 错误数据注入攻击与网络可观测性联系

文献[14] 将不可观测的错误数据注入攻击与经典的网络可观测性^[17] 概念建立了联系. 以下定理将说明成功不可观测错误数据注入攻击的代数条件等价于经典的网络不可观测条件^[17].

定义1 若非零攻击向量 $\mathbf{a}$ 可以表示为 $\mathbf{a} = \mathbf{H}\mathbf{c}$ 形式, 则称 $\mathbf{a}$ 为不可观测.

定义2 当给定可用测量值集合 $\mathbf{z}$ 和其对应的电网配置矩阵 $\mathbf{H}$, 可以估计出所有电力系统的状态 $\mathbf{x}$ 的分量, 则称该电力系统可观测, 或称状态可观测^[16].

定理2 存在一个不可观测的 k 稀疏(以下记含有 k 个非零元素的攻击向量 $\mathbf{a}$ 为 k 稀疏)非零攻击向量 $\mathbf{a}$, 即 $\mathbf{a} = \mathbf{H}\mathbf{c}$, 当且仅当 $\mathbf{a}$ 中 k 个非零元素对应的 k 个测量值被移除时电网变得不可观测, 也就是说, 存在 $(m - k) \times n$ 维的 $\mathbf{H}$ 子矩阵非列满秩.

具体证明见文献[14].

以上定理说明文献[7] 构建的错误数据注入攻击等价于从电网中移除 k 个测量电表, 因此而使得电网不可观测. 由定理2, 我们给出推论如下.

推论1 构建不可观测的攻击向量 $\mathbf{a}$, 等价于寻找 $\mathbf{H}$ 矩阵中的 k 个行向量, 使得删除该 k 个行向量后 $\mathbf{H}$ 矩阵非列满秩满秩.

以上推论将 k 稀疏攻击向量 $\mathbf{a}$ 的构建转化为寻找 k 个 $\mathbf{H}$ 矩阵行向量使得 $\mathbf{H}$ 矩阵非列满秩.

为了更清晰地进行讨论, 让我们首先来了解一下 $\mathbf{H}$ 矩阵的构建.

4.2 $\mathbf{H}$ 矩阵构建及分析

DC潮流模型下, 无错误的有功潮流和注入功率测量值(构成式(1)中的测量值向量 $\mathbf{z}$) 与电压相角(构成式(1)中状态向量 $\mathbf{x}$) 以如下的线性关系相联系^[16]:

$$\mathbf{z} = \mathbf{H}\boldsymbol{\theta} \quad (5)$$

式中, $\mathbf{z}$ 包括母线注入功率和线路有功功率, 即为式(1)中测量值向量, $\boldsymbol{\theta}$ 为母线的电压相角向量, 即为式(1)中的电力系统状态向量 $\mathbf{x}$, 此处为了含义明显用 $\boldsymbol{\theta}$ 来替换 $\mathbf{x}$.

对于母线 k 和母线 m , 其电压相角分别是 θ_k , θ_m . 考虑连接在母线 k 和 m 间的一个感抗为 x_{km} 的支路, 在 DC 潮流模型下, 可以记每个终端的电压幅值 V_k, V_m 为 1.0 p. u. .

由于 $\theta_k - \theta_m$ 趋向于 0, 从母线 k 到 m 的有功潮流可以近似可以表示如下:

$$P_{km} = \frac{V_k V_m}{x_{km}} \sin(\theta_k - \theta_m) \approx \frac{\theta_k - \theta_m}{x_{km}} \quad (6)$$

从母线 k 的注入功率等于从母线 k 流出的有功功率和,若与母线 k 连接的支路有 n 条,则母线 k 的注入功率 P_k 可以表示如下:

$$P_k = \sum_{i=1}^n P_{kj_i} = \sum_{i=1}^n \frac{(\theta_k - \theta_{j_i})}{x_{kj_i}} = \left[\sum_{i=1}^n \frac{1}{x_{kj_i}} \right] \theta_k - \sum_{i=1}^n \left[\frac{1}{x_{kj_i}} \theta_{j_i} \right] \quad (7)$$

将式(6)、(7)表示为矩阵形式即为式(5). 所有式(6)、(7)中 θ_k 的系数构成了 $\mathbf{H}$ 矩阵中列向量 $\mathbf{h}_k$ 中的非零元素, $\mathbf{h}_k$ 的每个非零元素即对应了一个与 θ_k 相关的形如(6)、(7)的方程. $\mathbf{H}$ 矩阵记录了式(6)和(7)两个方程所表示的功率测量值 $\mathbf{z}$ 和状态变量电压相角间 $\boldsymbol{\theta}$ 的关系,其元素的值由线路阻抗确定.

根据式(6)、(7)对于某个状态变量 θ_k ,有以下两种方式对于它进行求解:

$$\theta_k = x_{km} P_{km} + \theta_m \quad (8)$$

$$\theta_k = \frac{P_k + \left[\sum_{i=1}^n \frac{1}{x_{kj_i}} \theta_{j_i} \right]}{\sum_{i=1}^n \frac{1}{x_{kj_i}}} \quad (9)$$

4.3 攻击方案

由式(8)、(9)可知,在可观测的电力系统中,攻击者要使得其中的一个状态变量 θ_k 不可解,可以设法入侵并操纵式(8)、(9)中对应的测量值 P_{km} , P_k (可以通过入侵测量值对应的测量电表并修改其中值或者从入侵数据传输信道入手),那么使得所有可以求解 θ_k 的方程都被污染,根据定理 2,其效果相当于移除所有这相关的方程.

如上描述,对于状态变量 θ_k ,为了使其不可解,攻击者可以构建攻击向量 $\mathbf{a} = \lambda \mathbf{h}_k$, λ 为任意常数,根据定理 2,即移除 $\mathbf{a}$ 中 k 个非零元素对应的 k 个测量值,即移除 $\mathbf{h}_k$ 中 k 个非零元素对应的 $\mathbf{H}$ 矩阵行向量,移除 k 个非零元素后 $\mathbf{h}_k$ 为零向量,此时显然 $\mathbf{H}$ 矩阵非列满秩.

基于以上描述,给出结论如下.

结论 1 假设原始测量值 $\mathbf{z}$ 能通过坏值检测. 列满秩的 $\mathbf{H}$ 矩阵中某列向量 $\mathbf{h}_i$ 有 k 个非零元素,那么入侵这 k 个非零元素对应的 k 个测量电表构建 k 稀疏的攻击向量 $\mathbf{a} = \lambda \mathbf{h}_i$, λ 为任意常数,恶意测量值 $\mathbf{z}_a = \mathbf{z} + \mathbf{a}$ 也能通过坏值检测.

从定理 2 角度理解,以上结论的成立是显然的,

当删除了这 k 个行向量后,这 k 个非零元所在列就变成了 0 列向量,根据矩阵满秩的定义,那么显然所得矩阵非列满秩.

从式(8)、(9)角度理解,即污染了所有含有 θ_i ($\mathbf{h}_i$ 对应的状态变量)的方程,使得 θ_i 无法正确求解.

从实际电力系统角度理解,为了使得母线 i 的真实状态变量 θ_i 不可解,可以入侵如下电表:① 与母线 i 连接的线路功率测量电表;② 母线 i 上的注入功率测量电表.

那么为了发动此攻击,攻击者只需要两个条件:

① 能够知道 $\mathbf{H}$ 矩阵的某个列向量 $\mathbf{h}_i$ (在进行实际攻击操作时,攻击者并不需要知道 $\mathbf{h}_i$ 中哪些元素为 0 哪些元素非零,只需要知道非零元素的值);② 能够入侵 $\mathbf{h}_i$ 中非零元素对应的 k 个测量电表并修改其中的测量值.

条件 2 与文献[7]提出的错误数据注入攻击条件二相同,而条件 1 则比后者需要知道整个 $\mathbf{H}$ 矩阵降低了很多.

在进行实际攻击操作时,攻击者只要:

(1) 操纵母线 i 相关的电表测量值:① 操纵与母线 i 连接的线路功率测量值,影响方程(9);② 操纵与母线 i 相邻母线上的注入功率测量值,以使得式(7)继续成立,即母线 j 处功率守恒;③ 操纵母线 i 上的注入功率测量值,影响式(8);使得构建含有 k 个非零元素的攻击向量 $\mathbf{a}$ 成为可能.

(2) 测出与母线 i 相连的各条线路的阻抗,即可根据式(6)、(7)给出 $\mathbf{h}_i$ 中非零元素的值.

(3) 那么对于母线 i 与其相邻母线 j 间线路中的测量电表,修改原测量值 P_{ij} 为 $P_{ij} + \lambda / x_{ij}$, x_{ij} 为由步骤(2)测得的线路 $i-j$ 上的阻抗值,为了保持相邻母线 j 上功率遵守式(7),修改其注入功率 P_j 为 $P_j - \lambda / x_{ij}$;对于母线 i 上的注入功率测量电表,修改原测量值 P_i 为 $P_i + \lambda \left[\sum_{k=1}^n \frac{1}{x_{ik}} \right]$, $\left[\sum_{k=1}^n \frac{1}{x_{ik}} \right]$ 为与母线 i 相邻的 n 个母线间的阻抗倒数之和,可由步骤(2)的测量值得得;以上的 λ 为任意取定的常数.

有如上步骤就完成了攻击向量为 $\mathbf{a} = \lambda \mathbf{h}_i$ 的错误数据注入攻击,给状态变量 θ_i 注入了大小为 λ 的错误. 为了尽可能的降低成本,即使得入侵的测量电表数 k 尽可能的小,攻击者可以对相关测量值少的母线进行攻击,即对应的 $\mathbf{H}$ 矩阵中列向量非零元素个数最少的状态变量.

5 IEEE 测试系统仿真

用 IEEE 测试系统对错误数据注入攻击进行仿真,包括 IEEE 9-bus, 14-bus, 39-bus, 57-bus, 118-bus 测试系统. 从 MATPOWER(一个用于求解电力潮流的 MATLAB 包)中提取测试系统信息,如状态变量数、测量值数、 $\mathbf{H}$ 矩阵信息. 除去参照节点以后,其待估计状态变量数和测量值数如表 1 所示.

表 1 测试系统节点信息表

IEEE 测试系统	待估计状态变量数(n)	测量值数(m)
9-bus	8	27
14-bus	13	54
39-bus	38	131
56-bus	56	217
118-bus	117	490

由表 1 可以看出,测量值数远远大于待估计状态变量数,一般是 3 倍左右,这样设置的原因就是为了让系统具有足够的冗余度,而状态估计的精度保证及状态估计器中的错误辨识模块都需要依赖于测量值的冗余度. 同时,由上表可知待分析的对象 $\mathbf{H}$ 矩阵其阶数分别是: 27×8 、 54×13 、 131×38 、 217×56 、 490×117 . 考虑到 $\mathbf{H}$ 矩阵的规模较大,故不在此列出.

为了使得攻击代价尽可能小,攻击者会选择含有非零元素较少的 $\mathbf{H}$ 矩阵列向量作为目的向量,因此在仿真过程中,我们分别将各个测试系统对应的 $\mathbf{H}$ 矩阵中含有非零元素最少的列向量作为目的向量 $\mathbf{h}_{\text{tar}}$ 构建攻击向量 $\mathbf{a} = \lambda \mathbf{h}_{\text{tar}}$, λ 为任意非零常数.

由表 2 可以看出,对于各个测试系统,攻击者都只需要入侵非常少的 4 个特定测量值,并获取 $\mathbf{h}_{\text{tar}}$ 的信息后,就可以将测试系统的状态从可观测的变成不可观测的,如定理 2 所述,即说明错误数据注入攻击成功的绕过了坏值检测. 仿真中,我们选择了含有非零元素最少的 $\mathbf{H}$ 矩阵列向量作为目标向量,实

表 2 基于部分配置信息的错误数据注入攻击信息统计表

IEEE 测试系统	$\mathbf{H}$ 矩阵列向量最少非零元素个数	$\mathbf{H}$ 矩阵列向量平均非零向量个数	攻击前可观测性状态	攻击行向量集合	攻击后可观测性状态
9-bus	4	7.4	可观测	2,8,16,25	不可观测
14-bus	4	9.8	可观测	7,8,28,48	不可观测
39-bus	4	8.1	可观测	2,30,44,90	不可观测
56-bus	4	9.3	可观测	32,33,102,182	不可观测
118-bus	4	10.4	可观测	9,10,127,313	不可观测

际上,通过表 2 可以看出, $\mathbf{H}$ 矩阵列向量的平均非零元素个数也在 10 个左右,即对于各个测试系统,随机选择 $\mathbf{H}$ 矩阵的列向量作为目标向量,那么构建错误数据注入攻击时,所需要入侵的测量电表数也在 10 个左右,这是一个不算太大的攻击代价. 导致这个脆弱性的根本原因就在于量测冗余度 m/n 较小. 随着母线数量的从 9 个增加到 118 个,测量值数从 27 个增加到 490 个,但是攻击者都只要入侵 4 个特定的测量电表即可完成攻击. 我们分析该目标向量 $\mathbf{h}_{\text{tar}}$ 对应的母线,发现它只有一个邻居母线,这正是导致它成为安全瓶颈的原因.

6 结束语

错误数据注入攻击^[7]能给电力系统带来致命的危害,但同时它也给攻击者提出了很大的要求考验. 我们提出了基于部分配置信息构建错误数据注入攻击的方案,通过 IEEE 测试系统仿真验证了攻击方案的有效性和可行性.

参考文献:

- [1] 杨清宇, 杨洁, 马训鸣. 电力系统中假数据注入攻击研究[J]. 微电子学与计算机, 2011, 28(12): 175-179.
- [2] 韩祯祥, 曹一家. 电力系统的安全性及防治措施[J]. 电网技术, 2004, 28(9): 1-6.
- [3] 胡晓荷. 解读国际网络战最新形势[J]. 信息安全与通信保密, 2009(9): 7-9.
- [4] 李文武, 游文霞, 王先培. 电力系统信息安全研究综述[J]. 电力系统保护与控制, 2011, 39(10): 140-147.
- [5] 于尔铿, 电力工程. 电力系统状态估计[M]. 北京: 水利电力出版社, 1985.
- [6] 余勇, 林为民. 工业控制 SCADA 系统的信息安全防护体系研究[J]. 信息安全, 2012(5): 74-77.
- [7] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids [J]. Proceedings of the ACM Transactions on Information and System Security, 2011, 14(1): 21-32.
- [8] Bobba R B, Rogers K M, Wang Q, et al. Detecting false data injection attacks on dc state estimation[C]// Preprints of the First Workshop on Secure Control Systems. [s. l.]: IEEE, 2010.
- [9] Sandberg H, Teixeira A, Johansson K H. On security indices for state estimators in power networks[C]// Proceedings of the 1st Workshop on Secure Control Systems. Stockholm, Sweden: IEEE, 2010: 134-183.

(下转第 93 页)

节点接收数据概率能够更加有效的提高网络转发效率,而实验后期随着节点能量的消耗,此时接收概率越大将导致节点更快失效,从而影响网络生存周期。

5 结束语

本文结合节点剩余能量和数据有效传输距离建立了评价指标,并且利用云模型对上述评价指标进行刻画,提出了一种新的算法 ECBC,以此获得全局最优解。仿真实验对比研究了该算法与经典算法 HEED 之间的性能差异,结果表明 ECBC 算法更具有适应性。由于节点能量一直是 WSN 关注的重点和热点,而且 WSN 中能量空洞的出现阻碍了数据的传输,造成网络失效,所以在以后的研究过程中,可以考虑采用节点均匀分布以及梯度模型来解决能量消耗平衡的问题。

参考文献:

- [1] 吴小兵,陈贵海. 无线传感器网络中节点非均匀分布的能量空洞问题[J]. 计算机学报, 2008, 31(2): 253-261.
- [2] 洪榛,俞立,张贵军. 无线传感器网络自适应分布式聚簇路由协议[J]. 自动化学报, 2011, 37(10): 1197-1205.
- [3] Martalo M, Ferrari G. A simple information-theoretic analysis of clustered sensor networks with decentralized detection [J]. IEEE Communications Letters, 2010, 14(6): 560-562.
- [4] Luo X, Dong M, Huang Y. On distributed fault tolerant detection in wireless sensor networks [J]. IEEE Transactions on Computers, 2006, 55(1): 58-70.
- [5] Younis O, Fahmy S. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks [J]. IEEE Transactions on Mobile Computing, 2004, 3(4): 366-379.
- [6] 刘韬. 基于梯度的无线传感器网络能耗分析及能量空洞避免机制 [J]. 自动化学报, 2012, 38(8): 1353-1361.
- [7] 沈中,常义林,崔灿,等. 一种可自维护无线网络拓扑最小功耗特性的分布式拓扑控制算法[J]. 计算机学报, 2007, 30(4): 569-579.
- [8] 宋杰,李甜甜,闫振兴,等. 一种云计算环境下的能效模型和度量方法 [J]. 软件学报, 2012, 23(2): 200-214.
- [9] 李文泽,等. 基于云模型的 WSN 能量消耗平衡研究 [J]. 计算机学报, 2013, 36(10): 1985-1995.
- [10] Kosut O, Jia L, Thomas R J, et al. On malicious data attacks on power system state estimation [C] // Proceedings of the 45th International Universities Power Engineering Conference; Cardiff, Wales; IEEE, 2010: 1-6.
- [11] Kosut O, Jia L, Thomas R J, et al. Malicious data attacks on smart grid state estimation: attack strategies and countermeasures [C] // Proceedings of the First IEEE International Conference on Smart Grid Communications. Gaithersburg, MD; IEEE, 2010: 220-225.
- [12] Xie L, Mo Y, Sinopoli B. False data injection attacks in electricity markets [C] // Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications. Gaithersburg, MD; IEEE, 2010: 226-231.
- [13] Jia L, Thomas R J, Tong L. Malicious data attack on real-time electricity market [C] // Proceedings of the International Conference on Acoustics, Speech and Signal Processing. Prague; IEEE: 5952-5955.
- [14] Kosut O, Jia L, Thomas R J, et al. Malicious data attacks on the smart grid [J]. IEEE Transactions on Smart Grid, 2011, 2(4): 645-658.
- [15] Monticelli A. State estimation in electric power systems: a generalized approach [M]. Berlin: Springer, 1999.
- [16] Abur A, Exposito A G. Power system state estimation: theory and implementation [M]. New York: CRC Press, 2004.
- [17] Wu FF, Monticelli A. Network observability: theory [J]. IEEE Transactions on Power Apparatus and Systems, 1985(5): 1042-1048.

作者简介:

李文泽 男, (1979—), 硕士, 讲师. 研究方向为网络优化。

作者简介:

李 勒 男, (1987—), 硕士研究生. 研究方向智能电网安全、信息物理系统安全。

洪爽俊 男, (1990—), 硕士研究生. 研究方向网络安全。

张 驰 男, (1977—), 副教授, 博士生导师. 研究方向为赛博空间中的安全。

(上接第 89 页)