

电力系统中假数据注入攻击研究

杨清宇¹, 杨 洁¹, 马训鸣²

(1 西安交通大学 电信学院, 陕西 西安 710049; 2 西安工程大学 机电学院, 陕西 西安 710048)

摘 要: 假数据注入攻击是电力系统安全研究的重要问题之一, 对智能电网发展趋势下的电力系统安全、稳定运行具有重要的意义. 综述了电力系统中假数据注入攻击的研究进展, 分析了 EMS 和假数据注入攻击的原理, 并对假数据注入攻击研究工作进行了介绍, 最后总结了研究现状中存在的问题以及需要进一步研究的工作.

关键词: 电力系统; 假数据注入攻击; CPS

中图分类号: TM734

文献标识码: A

文章编号: 1000-7180(2011)12-0175-05

Research on False Data Injection Attacks in Power Systems

YANG Qing-yu¹, YANG Jie¹, MA Xun-ming²

(1 School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;

2 School of Mechatronics, Xi'an Polytechnic University, Xi'an 710048, China)

Abstract: The false data injection attack is one of the most important problems in the study of power system security. It is of great importance for the security and stabilization control of the power systems under the tendency of smart grids. This paper makes a full-scale introduction to the research on false data injection attacks in power systems. Firstly, the process of EMS including state estimation and bad data detection and false data injection attacks is presented. Secondly, an introduction is made to show the work on false data injection attacks. Finally, existing problems and open issues are discussed.

Key words: power system; false data injection attacks; CPS

1 引言

电力系统是重要的国家设施, 其安全稳定运行对社会稳定和国民经济正常发展起着关键作用. 它通过输电和配电网络将电厂和用户连接起来, 是一个典型的 CPS (cyber-physical system) [1]. 随着电力系统日趋复杂化和智能电网的推广, 为了使其安全、稳定运行, 监测和控制系统的实时状态不容忽视. 控制中心的能量管理系统 (Energy Management System, EMS) [2] 应用来自数据采集与监视控制 (Supervisory Control and Data Acquisition, SCADA) 系统接收到的传感器量测数据对系统的实时状态进行估计, 并利用估计结果和控制算法做出

实时的控制决策.

越来越多的 SCADA 系统与控制中心的局域网相连, SCADA 系统自身与传感器之间的数据传输网络亦是非常之混杂, 例如光纤、卫星、微波等 [3]. 这些因素使得电力系统很容易受到恶意网络攻击的入侵, 2003 年 1 月, 俄亥俄州的戴维斯-贝斯电厂网络被 Slammer 蠕虫病毒侵入, 导致了网络负载过重, 使得计算机之间不能相互通信, 并且使 SCADA 系统近 5 个小时不可用, 造成了巨大的经济损失. 由此可见, 电力系统的安全问题不容忽视, 它不是单纯的物理系统的安全问题, 也不是传统的网络信息安全问题.

然而, 2009 年之前大多数对电力系统安全保护

的研究都局限在对其可靠性(保护其不受随机错误的破坏)的研究,或者从通信网络的角度关注数据的完整性、有效性和可靠性,并没有考虑到攻击对应用层服务的影响:成功的攻击对状态估计和控制算法有何影响,最终如何影响到物理系统^[4]。

随着对 CPS 的深入研究,Liu^[5]于 2009 年首次提出了假数据注入攻击,攻击者在对电力系统拓扑结构有一定了解的情况下,篡改 EMS 接收到的传感器量测数据,按照预定的目标改变了状态估计的结果。自此,电力系统中假数据注入攻击受到了广泛的关注,研究者开始从各个角度展开了对假数据注入攻击的研究。

2 EMS 与假数据注入攻击原理

2.1 EMS

输电系统是由电厂、变电站及输电线路组成的电力网络。在任何时刻用户所用的电能一定与发电机发出的电能相等,冗余的输电线路使得在分布广阔的电网中任何发电厂发出的电可以畅通无阻地提供给每一个用户,电能分配的原则是使所需的运行费用最小。控制中心通常用于监测和控制电力系统和设备。

传感器在获取各个节点的实时信息后,通过网络传输给 SCADA 系统,SCADA 系统将这些遥测数据首先传输给 EMS 中的状态估计器,状态估计^[6-7]和不良数据检测算法对这些实时量测数据进行滤波,以排除测量误差和随机干扰所引起的错误信息,提高测量数据精度。状态估计是获得电网监测的实时数据和提高监测质量的重要手段,估计结果将用于 EMS 中的控制算法,例如事故分析、最优潮流、经济调度等,如图 1 所示。这些控制算法根据系统的实时状态做出相应的决策,通过 SCADA 系统反馈到远程终端(RTU)。

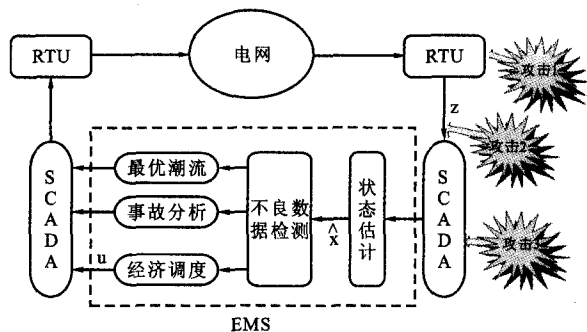


图 1 电力系统中的假数据注入攻击

假数据注入攻击是一种针对电力系统状态估计的恶意网络攻击。图 1 中,这样的攻击是在攻击者对

电力系统拓扑结构有所了解的情况下,通过直接篡改传感器量测数据(攻击 1),入侵传感器和 SCADA 系统之间的通信网络(攻击 2),或者通过控制中心局域网进入 SCADA 系统(攻击 3),使得控制中心接收到的传感器量测数据不等于真实的量测数据。这样的攻击可以有效地“逃过”现有的不良数据辨识方法,使 EMS 中的控制算法做出错误的决策。

2.2 状态估计与不良数据检测

(1) 状态估计

SCADA 系统将接收到来自传感器的量测数据传输给 EMS 中的状态估计器,估计出系统的实时状态。本文主要讨论基于加权最小二乘法(WLS)的直流系统状态估计。量测量与状态变量的关系可以用下面的式子来表示:

$$z = h(x) + e \quad (1)$$

式中, $z = (z_1, z_2, \dots, z_m)^T$, ($z_i \in R, i = 1, 2, \dots, m$), 表示量测量, 一般包括节点电压幅值、节点注入有功功率和无功功率以及支路有功和无功功率; $x = (x_1, x_2, \dots, x_n)^T$ ($x_j \in R, j = 1, 2, \dots, n$), 表示系统的状态变量, 包括节点电压幅值和相角; $e = (e_1, e_2, \dots, e_m)^T$ ($e_k \in R, k = 1, 2, \dots, m$), 表示量测误差, 一般认为 e_k 服从均值为 0 的高斯分布, 且 $\text{cov}(e) = R$ 。 $h(x)$ 是一个表示系统拓扑结构的非线性函数矩阵。对于一个简单的直流系统模型来说, 其传感器量测量只包括支路有功功率和节点注入有功功率, 状态变量包括节点电压相角, 节点电压幅值均为 1 p. u.。忽略所有的支路阻抗, 状态估计可以由下面的线性化模型来代替:

$$z = Hx + e \quad (2)$$

式中, 量测矩阵 $H^{m \times n}$ 是一个常数雅克比矩阵, 通常情况下传感器量测值数目要大于状态变量数目, 即 $m > n$, 冗余的量测量用来提高估计的精度。这样的直流静态状态估计问题就是求出一个与真实的状态向量 x 最接近的估计值 $\hat{x}$, 可以用 WLS 方法来解决:

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \quad (3)$$

(2) 不良数据检测和辨识

EMS 接受到的传感器量测数据并不是完全准确的, 它除了带有一定的量测噪声, 还可能含有由于设备故障、传感器的偏移、错误连接, 通信系统受到干扰等引起的不良数据(测量误差大于标准差的 3 倍以上)。不良数据的存在可能导致状态估计结果受到污染, 使其偏离实际情况。状态估计采取了一系列的方法来减少和避免不良数据带来的影响, 首先, 利

用冗余的量测量来滤除量测噪声和一些随机干扰,其次,利用不良数据检测和辨识方法来处理不良数据.关于不良数据的检测和辨识,已经有了较为成熟的研究成果^[8-11].其实质是利用最大标准残差(the largest normalized residual, LNR)方法来检验量测数据中是否含有不良数据.当加权矩阵取值为单位矩阵($R^{-1}=I$)时:

$$\text{LNR} = \|z - \hat{H}\hat{x}\|^2 \quad (4)$$

式中, $z - \hat{H}\hat{x}$ 表示量测估计误差,由于 $\|z - \hat{H}\hat{x}\|^2$ 服从自由度为最大为 $m-n$ 的 χ^2 分布,故若 $\|z - \hat{H}\hat{x}\|^2 > \tau$ (τ 为阈值,由显著性 α 水平来决定),表明量测向量中含有不良数据.那么将量测向量中估计误差最大的变量滤除,重复 LNR 检验法,直到满足 $\|z - \hat{H}\hat{x}\|^2 < \tau$.

2.3 假数据注入攻击

假数据注入攻击是对原有的量测向量 z 加入一个非零的攻击向量 $a = (a_1, a_2, \dots, a_m)^T$,那么观测到的量测向量就是 $z_a = z + a$.状态估计在接收到不良数据后利用 WLS 方法得到一个错误的估计量,记作 $\hat{x}_{\text{bad}} = \hat{x} + c$,其中 c 为攻击带来的估计误差.

文献[5]中提出了一种有效的攻击策略:当攻击向量 a 是 H 的列向量的线性组合时,例如 $a = Hc$,假数据注入攻击可以不被 LNR 方法检测出来,证明如下:

$$\begin{aligned} \|z_a - H\hat{x}_{\text{bad}}\| &= \|z + a - H(\hat{x} + c)\| \\ &= \|z - H\hat{x} + (a - Hc)\| \\ &= \|z - H\hat{x}\| \end{aligned}$$

3 研究现状

目前对电力系统攻击的研究可以分为攻击对状态估计和控制算法的影响的研究,以前者居多.

3.1 状态估计中的假数据注入攻击研究

(1) 静态状态估计中假数据注入攻击研究

Liu^[5]提出了 $a = Hc$ 的假数据注入攻击模型.对攻击者来说,要破坏所有的传感器量测量是不容易实现的,他们可能会被局限于只能破坏某个特定区域的传感器,或者只拥有破坏 k ($k < m$)个传感器的资源,在这样的情况下,应该如何构造攻击向量,攻击对状态估计的结果又有何影响?前者可以抽象成矩阵变换问题,后者属于 NP-Complete 问题.对于包括 490 个传感器量测量和 118 个状态变量的 IEEE-118 节点直流系统来说,在上述第二种情况下,应用正交匹配算法可以得出攻击者需要破坏 60~130 个传感器量测量,就可以改变 10 个状态变

量,整个攻击构造计算时间不超过 2s.

对于改变特定数目的状态变量值,需要破坏的传感器量测量数目,文献[5]中给出了一个大致的范围,Sandberg^[12]提出了两个安全参数,用来准确的量化成功实施攻击所需破坏的最少传感器量测值,在文献[13]中,他进一步提出了计算这两个参数的方法.

文献[5,12-13]都是从攻击者的角度研究假数据注入攻击的攻击策略,Bobba^[14]认为某些状态变量需要依赖更多的传感器量测量,而某些传感器量测量对状态变量的影响要更大一些,因此从系统管理者的角度,应用遍历搜索和保护基本传感器量测量的方法找到这些特殊的状态变量和传感器量测量,对这类状态变量进行认证,对传感器量测量进行保护,从而提高系统的安全性.Kosut^[15]应用图论和多项式时间复杂度方法构造了攻击模型,并用广义似然比检验方法来检测此攻击.

目前多数的研究工作为了简化问题的复杂度,都是针对直流电力系统的假数据注入攻击及其检测,并且认为攻击者可以获悉系统全部的拓扑结构^[5,12-15].实际中也存在交流系统,而且攻击者要掌握整个系统的所有信息非常之困难.Teixeira^[16]研究了基于交流电力系统的假数据注入攻击,同时研究了当攻击者只知道系统的部分拓扑结构时的攻击模型,并提出了相应的保护措施.研究表明,攻击者对系统的结构掌握的越多,那么他成功实施攻击的可能性就越大.在文献[17]中他进一步研究了状态估计对假数据注入攻击的敏感度,证明采用一些新的传感器并对其进行保护可以提高系统的安全性.

(2) 动态状态估计中假数据注入攻击研究

目前大多数假数据注入攻击研究都基于电力系统静态状态估计,静态状态估计中 SCADA 系统每 2~4 s 将传感器量测数据传输给 EMS 中的状态估计器,在未使用任何先验信息的情况下可以对系统某个时间断面的静态参数(如节点电压与相角)进行估计.卡尔曼滤波算法将来自 SCADA 和 PMU (Phasor Measurement Units,每秒采集 30 次量测信息)的量测信息相结合,并且用到了系统过去的信息而可以连贯地估计出系统的状态信息,包括一些动态参数,例如发电机速度等.

Mo^[18]对动态卡尔曼滤波算法中的假数据注入攻击进行了初步的研究,基于一个简单的带有 LQG 控制器的线性连续高斯控制系统,提出了攻击模型,并分析了攻击对状态估计结果的影响.

3.2 控制系统中的假数据注入攻击研究

研究假数据注入攻击对电力系统的危害,就是要分析假数据注入攻击如何影响状态估计,以及控制算法,最终如何影响物理系统.电力系统包括发电、输电、配电这几个方面,EMS 是基于发电和输电系统的,状态估计的结果应用于某些控制算法,例如事故分析,潮流优化、经济调度等.

目前对于假数据注入攻击对控制算法的研究刚刚起步,Xie^[19]提出了一种针对电力市场(经济调度)的攻击模型,用凸优化方法构造了攻击模型,并分析了假数据注入攻击对电力市场潜在的经济影响,但并没有提出相应的假数据注入攻击检测方法.

4 存在的问题及进一步的研究

(1) 针对控制系统中的假数据注入攻击研究较少

状态估计的目的是利用冗余量测量对系统的实时状态做出准确的估计,估计出的状态变量结果将被用于 EMS 中的控制算法.攻击者对用于状态估计的量测量进行破坏,目的是改变状态估计结果,进而使得控制算法做出错误的决策.目前对于假数据注入攻击对状态估计的影响研究已经有了一定的深度,包括攻击构造的方法,达到攻击目的需要付出的最小代价以及如何构造此类攻击,根据提出的攻击模型进一步找到攻击检测的方法.然而对假数据注入攻击对控制算法的影响研究非常之少,目前只有假数据注入攻击对电力市场潜在的经济影响的研究^[19].

因此,未来电力系统中的假数据注入攻击的研究热点之一是研究假数据注入攻击对控制算法有何影响,在受到假数据注入攻击,做出错误的控制决策后,系统的运行会产生何种变化.

(2) 从 CPS 的角度研究假数据注入攻击

电力系统中假数据注入攻击与传统的网络攻击本质的不同,在于电力系统是物理与控制系统的交互.而现有的网络安全关注的只是对信息的保护,关注数据的完整性、有效性和可靠性,不能够为控制系统提供深度的防御,当攻击突破这些安全措施时,可能会对物理系统造成巨大的破坏.

未来对电力系统中假数据注入攻击的研究,不仅仅是将控制理论(鲁棒控制、容错控制等)与网络安全(认证、接纳控制等)相结合,而且是要从 CPS 的角度,将物理系统和网络看作一个整体,研究攻击如何影响到状态估计和控制算法,最终如何影响物

理系统.

(3) 设计新的对攻击具有弹性的算法和结构

电力系统对假数据注入攻击除了检测以外,更高级别的安全措施是在受到网络攻击时系统仍可以存活,其核心功能不受影响.目前还没有这方面的研究,早先的故障诊断不可以用来处理恶意攻击.因此对未来系统的设计目标是即使攻击突破了最基本的安全设施,仍需面对更高级别的弹性算法和结构,从而减小攻击对系统的破坏程度.

5 结束语

文中综述了电力系统中的假数据注入攻击研究现状,并分析了当前研究中存在的问题和研究趋势.目前的研究成果多集中于假数据注入攻击模型的构造及其检测,很少有研究深入关注假数据注入攻击对控制算法的影响,最终如何影响到物理层面.电力系统是一个复杂的控制系统,是物理系统与网络相融合的系统,研究假数据注入攻击对其影响,需要从 CPS 的角度,将控制理论与网络安全相结合,研究攻击模型的构造、攻击的检测,最后设计出新的算法和结构,使得系统在受到攻击后,仍可稳定运行.

参考文献:

- [1] Cardenas A A, Amin S, Sastry S, et al. Secure control: Towards survivable cyber-physical systems[C]// Proceedings of the First International Workshop on Cyber-Physical Systems. China: Beijing, IEEE, 2008: 495 - 500.
- [2] 于尔铿. 能量管理系统(EMS)[M]. 北京: 科学出版社, 1998.
- [3] 于尔铿. 电力系统状态估计[M]. 北京: 水利电力出版社, 1985.
- [4] Cardenas A A, Amin S, Lin Z S, et al. Attacks against process control systems: Risk assessment, detection, and response[C]// Proceedings of ACM Symposium on Information, Computer and Communications Security, AsiaCCS 2011. Hong Kong: ACM, 2011.
- [5] Liu Yao, Reiter M K, Ning Peng. False data injection attacks against state estimation in electric power grids [C]// Proceedings of the 16th ACM conference on Computer and Communications Security. Chicago, USA: ACM, 2009: 21 - 32.
- [6] Schweppe F C, Wildes J, Rom D B. Power system static state estimation. parts 1, 2, 3[J]. IEEE Transactions on Power Apparatus and Systems, 1970, 89(1): 120 - 135.

- [7] Albur A, Exposito A G. Power system state estimation: theory and implementation [M]. CRC Press, 2004.
- [8] Monticelli A, Wu F F, Multiple M Y. Bad data identification for state estimation by combinatorial optimization [J]. IEEE Transactions on Power Delivery, 1986, 1 (3):361-369.
- [9] Granelli M M G P. Identification of interacting bad data in the framework of the weighted least square method [J]. Electric Power System Research, 2008, 78(5):806-814.
- [10] Khwanram J, Damrongkulkamjorn P. Multiple bad data identification in power system state estimation using particle swarm optimization[C]//Proceedings of 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology. Pattaya Thailand;IEEE,2009: 2 - 5.
- [11] 周苏荃, 张艳军. 新息图状态估计中多相关不良数据辨识[J]. 电力系统及其自动化学报, 2008, 20(4): 1-6.
- [12] Sandberg H, Teixeira A, Johansson K H. On security indices for state estimators in power networks[C]//Proceedings of the First Workshop on Secure Control Systems, CPSWEEK 2010. Stockholm Sweden; IEEE, 2010.
- [13] Dan G, Sandberg H. Stealth attacks and protection schemes for state estimators in power systems[C]//Proceedings of 1st IEEE International Conference on Smart Grid Communications. MD USA;IEEE, 2010.
- [14] Bobba R B, Rogers K M, Wang Q, et al. Detecting false data injection attacks on dc state estimation[C]//Proceedings of the First Workshop on Secure Control Systems, CPSWEEK 2010, Stockholm Sweden; IEEE, 2010.
- [15] Kosut O, Jia L, Thomas R J, et al. Malicious data attacks on smart grid state estimation: attack strategies and countermeasures [C]//Proceedings of 1st IEEE International Conference on Smart Grid Communications. MD USA;IEEE, 2010.
- [16] Teixeira A, Amin S, Sandberg H, et al. Cyber security analysis of state estimators in electric power systems [C]//Proceedings of 49th IEEE Conference on Decision and Control. USA;IEEE, 2010:15-17.
- [17] Teixeira A, Dan G, Sandberg H, et al. A cyber security study of a scada energy management system: Stealthy deception attacks on the state estimator[C]//Proceedings of 18th IFAC World Congress. Milano Italy;IEEE, 2011:11271-11277.
- [18] Mo Y L, Sinopoli B. False data injection attacks in control systems[C]//Proceedings of the 1st Workshop on Secure Control Systems, CPSWEEK 2010. Stockholm Sweden;IEEE, 2010:226-231.
- [19] Xie L, Mo Y L, Sinopoli B. False data injection attacks in electricity markets [C] // Proceedings of 1st IEEE International Conference on Smart Grid Communications. MD USA;IEEE, 2010.

作者简介:

杨清宇 男,(1974-),副教授,硕士生导师.研究方向为电力系统控制与诊断、智能控制理论及应用.

杨洁 女,(1987-),硕士研究生.研究方向为电力系统状态估计与网络安全.

马训鸣 男,(1963-),教授,硕士生导师,研究方向为机电控制及自动化.