分类号：TM76　　单位代码：10363

密　级：公开　　学　　号：2210330120

题　　目 面向 GPS 欺骗攻击的智能电网状态估计研究

题　　目 Research on Smart Grid State Estimation for GPS Spoofing Attacks

论文作者：华峰

校内导师：高文根教授

校外导师：刘建

专　　业：电子信息

研究方向：人工智能与系统集成

论文提交日期：2024 年 5 月 31 日

安徽工程大学学位论文原创性声明

本人郑重声明：我恪守学术道德，崇尚严谨学风。所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已明确注明和引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品及成果的内容。论文为本人亲自撰写，我对所写的内容负责，并完全意识到本声明的法律后果由本人承担。

学位论文作者签名：华峰

日期： 2024 年 5 月 26 日

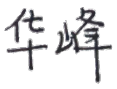
安徽工程大学学位论文版权使用授权书

学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅或借阅。本人授权安徽工程大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

保密 □，在 ____ 年解密后适用本版权书。

本学位论文属于

不保密 ☑。

学位论文作者签名：  　　指导教师签名： 

日期：2024 年 5 月 26 日　　日期：2024 年 5 月 26 日

面向 GPS 欺骗攻击的智能电网状态估计研究

摘 要

智能电网测量设备相量测量单元（Phasor Measurement Unit, PMU）的应用已经彻底改变了传统状态估计的执行方式。PMU 因其采样率高、可实时估计电力系统状态而被广泛应用于电力系统状态估计中。然而，PMU 使用未加密的 GPS 民用信号进行时间同步，而民用 GPS 信号的详细信息是公开的，所以恶意用户可以利用这一点构建设备来生成伪 GPS 信号。攻击者可诱导伪 GPS 信号被 PMU 接受，进而操纵 PMU 的时间基准，将错误的相角信息引入 PMU 的量测值中，这一过程称为 GPS 欺骗攻击（GPS Spoofing Attack, GSA）。GPS 欺骗攻击会导致电力系统的状态估计出现严重错误和电网的大范围故障，这大大影响了电网的可靠运行。因此，对于研究面向 PMU 的 GPS 欺骗攻击的智能电网状态估计具有重要意义。本文针对智能电网中的 GPS 欺骗攻击以及电网系统状态估计校正的问题，探讨了 GSA 的构成原理，推导建立了 PMU 的 GSA 模型，并以该模型为研究对象，分别采用了基于测量残差的欺骗检测及系统状态估计方法以及联合最大后验和最大似然算法对 GSA 进行检测和系统状态估计，以实现在系统中 PMU 受 GSA 时，对受攻击 PMU 进行精准定位和系统状态数据的恢复。具体研究内容如下：

首先，对 PMU 布局下的电力系统量测模型和 GPS 欺骗攻击原理进行分析，明确了 GPS 欺骗攻击对 PMU 量测值造成的具体影响，并

在此基础上建立了受欺骗攻击下系统 PMU 的量测模型，为后续的攻击检测和系统安全状态估计提供理论基础。

其次，针对所建立的攻击状态下系统 PMU 量测模型中参数矩阵特殊性，提出了一种基于测量残差的电网 GPS 欺骗检测与测量校正算法，该算法可以检测和缓解不同攻击角度的多个 GSA。算法由两个关键子算法组成，即 GPS 欺骗攻击检测算法和不良测量数据校正算法。GPS 欺骗攻击检测算法通过监测测量残差的欧几里得范数，以区分安全和欺骗攻击场景。在安全场景中，没有任何 PMU 被欺骗，而在欺骗场景中，有一个或多个 PMU 被不同的攻击角度欺骗而导致原始数据被篡改。不良数据校正算法将前一步的欺骗攻击检测算法中检测出的不良数据进行校正，以使得这些数据仍可以用于后续得系统状态估计。在 IEEE-14 算例上进行实验，结果显示该方法能够有效检测出系统中一个或多个 GSA 的存在，并且能够对受攻击下系统状态估计的进行恢复。

最后，针对受攻击后 PMU 量测模型中存在的参数耦合未知和目标函数非凸等问题，基于混合建模方法建立 PMU 测量模型，引入双模混合分布来表示 PMU 混合测量中的误差，该模型更准确地表示了 PMU 中测量误差。在此基础上提出了一种联合最大后验和最大似然（Joint Maximum a Posteriori and Maximum Likelihood, JMAP-ML）算法，该方法可以安全地估计 PMU 混合测量中系统的正确状态和检测 GSA。实验结果表明，该方法可以有效解决系统模型中参数耦合的难题，适用于系统发生不同个数 GSA 场景的状态估计，可实现电网系

统的持续稳定运行。

综上所述，本文研究的检测算法与防御策略能有效定位电网中受 GPS 欺骗攻击的 PMU，并能恢复由攻击带来的不良数据，为维护电网系统的安全稳定运行具有重要的研究意义与实际的应用价值。

关键词：智能电网，相量测量单元，GPS 欺骗攻击，攻击检测，状态估计

RESEARCH ON SMART GRID STATE ESTIMATION FOR GPS SPOOFING ATTACKS

ABSTRACT

The application of Phasor Measurement Units (PMUs) in smart grid measurement equipment has fundamentally changed the execution of traditional state estimation. PMUs are widely used in power system state estimation due to their high sampling rates and ability to estimate power system states in real-time. However, PMUs use unencrypted GPS civilian signals for time synchronization, and the detailed information of civilian GPS signals is publicly available. Therefore, malicious users can exploit this to construct devices to generate fake GPS signals. Attackers can induce PMUs to accept fake GPS signals, thereby manipulating the time reference of PMUs and introducing incorrect phase angle information into the measured values of PMUs. This process is known as a GPS Spoofing Attack (GSA). GPS spoofing attacks can lead to severe errors in power system state estimation and widespread failures in the power grid, greatly affecting the reliable operation of the grid. Therefore, researching GPS spoofing attacks targeting PMUs in smart grid state estimation is of great significance. This paper addresses the issues of GPS spoofing attacks in smart grids and the correction of grid system state estimation. It explores the composition principles of GSA, derives and establishes a GSA model

for PMUs. With this model as the research object, it employs deception detection based on measurement residuals and system state estimation methods, as well as a joint maximum a posteriori and maximum likelihood algorithm, to detect GSA and estimate system states accurately when PMUs are under attack, aiming to achieve precise positioning of attacked PMUs and recovery of system state data. The specific research contents are as follows:

Firstly, the paper analyzes the power system measurement model under PMU layout and the principle of GPS spoofing attacks, clarifying the specific impacts of GPS spoofing attacks on PMU measurements. Based on this, it establishes a measurement model of PMUs under attack, providing a theoretical basis for subsequent attack detection and system security state estimation.

Secondly, considering the particularity of parameter matrices in the established PMU measurement model under attack states, a measurement residual-based grid GPS spoofing detection and measurement correction algorithm are proposed. This algorithm can detect and mitigate multiple GSAs from different attack angles. The algorithm consists of two key sub-algorithms: GPS spoofing attack detection algorithm and correction algorithm for bad measurement data. The GPS spoofing attack detection algorithm distinguishes between safe and spoofed attack scenarios by monitoring the Euclidean norm of measurement residuals. In a safe

scenario, no PMU is spoofed, while in a spoofed scenario, one or more PMUs are spoofed from different attack angles, leading to tampering with the original data. The bad data correction algorithm corrects the bad data detected in the previous step of the GPS spoofing attack detection algorithm so that these data can still be used for subsequent system state estimation. Experiments conducted on the IEEE-14 bus demonstrate that this method can effectively detect the presence of one or more GSAs in the system and can recover the system state estimation under attack.

Finally, addressing the problems of parameter coupling unknowns and non-convex objective functions in the PMU measurement model after the attack, a mixed modeling method is proposed to establish the PMU measurement model, introducing a double-mode mixed distribution to represent errors in PMU mixed measurements, which more accurately represents measurement errors in PMUs. Based on this, a Joint Maximum a Posteriori and Maximum Likelihood (JMAP-ML) algorithm is proposed, which can safely estimate the correct state of the system in PMU mixed measurements and detect GSAs. Experimental results show that this method can effectively solve the problem of parameter coupling in the system model, suitable for state estimation scenarios in which different numbers of GSAs occur, and can achieve continuous stable operation of the power grid.

In summary, the detection algorithms and defense strategies studied in this paper can effectively locate PMUs under GPS spoofing attacks in the grid and recover bad data caused by attacks, which is of great research significance and practical application value for maintaining the safe and stable operation of power grid systems.

KEY WORDS: smart grid, phasor measurement unit, GPS spoofing attack, attack detection, state estimation

目录

第 1 章 绪论

1.1 研究背景及意义

新一代电网被称为智能电网，它将更先进的信息通信技术（Information and Communication Technology, ICT）和分布式可再生能源集成到传统电网中。信息通信技术是推动这一整合的关键支撑。ICT 涵盖了广泛的技术工具，涉及计算机、互联网、传感器、通信网络和数据处理系统等，这些技术的运用使得传统电网得以更为有效地管理和整合分散的可再生能源资源。分布式可再生能源，例如太阳能和风能，往往分布广泛，地理位置多样。将这些能源融入传统电网系统面临着一系列挑战。其中包括能源波动性、可靠性和复杂的管理需求。ICT 技术的应用为解决这些挑战提供了全新的解决途径[1]。ICT 技术使得实时监控和控制成为现实。透过传感器和监测设备，能够实时追踪监测可再生能源系统的产能、输出和波动。这些实时数据赋予电网运营者更为准确的能源波动预测和管理能力，确保电网的稳定运行。此外，ICT 技术赋能智能能源管理，其借助数据分析和人工智能技术，优化能源的分配和利用，使得可再生能源的接入更为高效和可控。智能系统能够灵活动态地调整电网运行模式，以应对需求和资源的变化。ICT 技术还可以提供可再生能源系统与电网之间高效的通信和互联网连接。这种协同连接性有助于各个能源源头之间的协调合作，使电网更加灵活地管理分散的能源资源。在数据传输和存储方面，ICT 技术注重安全性，可以有效地防范潜在的网络安全威胁[2]。

在面向智能电网发展愈加迅速的今天，电网安全是一个愈加重要的问题。有了这些同步相量类型设备的应用，电网的运行更加稳定、可靠、高效和环保。然而，由于同步应用需要大量的数据通信，智能电网比传统电网更依赖于数据传输，具有更高的服务质量。因此，智能电网也容易受到网络威胁和攻击。例如，2015 年 12 月 23 日，乌克兰电网遭遇网络攻击。约 23 万人停电 1～6 小时。2017 年，美国东北部遭遇了一次大规模停电，涉及纽约市和新英格兰地区。虽然停电仅持续了几个小时，但却影响了数百万人。2018 年巴西曾遭受一次网络攻击，导致南部地区和东北部地区的大范围停电。尽管攻击并没有像乌克兰那样造成长时间的

停电，但它引起了对电网系统的恶意入侵威胁的担忧[3]。这些事件显示了电网系统容易受到网络攻击威胁的现实性。电网系统的数字化和互联化程度提高了其面临的网络安全风险。对电网进行网络攻击可能会导致停电、系统中断甚至数据篡改等影响，对供电稳定性和社会运转产生严重影响。因此，为了了解网络事件对同步量应用的潜在影响以及网络和电力领域之间复杂的相互依赖性，需要一个集成的实时网络物理测试平台来辅助和验证相关的概念研究工作。此外，为了分析同步相量分散在电力系统运行和控制中的应用，需要对大型电力系统进行实时建模和仿真。然而，单个实时模拟器单元的仿真能力有限。增强仿真能力的最常见方法是使用一组本地连接的实时模拟器。然而，建立一个大规模的实时模拟器库需要大量的财政投资，因此可能不是在所有的研究设施都可行。使用实时模拟器的电力和能源系统研究设施位于不同的物理位置。除了实时模拟器，世界各地的研究设施还拥有一系列具有独特动力、能源和控制系统的设施，用于创新研究。为了利用这些独特的研究设施，解决仿真能力有限的问题，需要基于广域网（Wide Area Network, WAN）的地理分布式实时仿真[4]。

为了保证电力系统运行的可靠性，系统监控在电网中得到了广泛的应用。它根据所有变电站的电表读数提供系统条件，根据这些数据对系统进行状态估计。状态估计是系统监控的重要组成部分，其是基于电表测量和电力系统模型对电力系统状态进行最优估计的方法[5]。然而，由于测量误差、通信噪声和可能的网络攻击，状态估计的估计结果将受到严重影响[6]。为了检测这些不同类型的坏数据，坏数据检测技术被广泛应用于保护状态估计。此外，状态估计的结果还被许多其他同步量应用所利用，如频率和电压监测、事件检测、振荡检测、自动化广域控制和补救行动方案。因此，分析状态估计的网络物理安全性是对其他同步应用进行网络物理安全性分析的最重要方面之一。

电力系统状态估计是电力系统运行与控制中至关重要的一环。它通过对电网实时数据的收集与分析，结合数学模型和估计算法，用以推断和估算电力系统中无法直接测量的参数，从而确保对电网运行状态的准确把控。实时准确的状态估计可以确保电网的稳定运行，通过收集实时数据，如电流、电压、频率等参数的监测，状态估计有助于预测和检测电网中的潜在问题，及时采取措施以避免可能导致电力系统失稳或发生其他故障的情况。

PMU 设备在智能电网中的布局使用作为 ICT 在电力系统中的一部分，不仅为电力系统的监测、控制和保护提供了关键性支持，也在电力系统状态估计中扮演着至关重要的角色。PMU 是智能电网中最重要的监控设备之一，长期以来，监控和数据采集（Supervisory Control and Data Acquisition, SCADA）系统一直是电力系统中主要的网络组成部分，被认为是一个脆弱、缓慢且信息不足的测量网络系统。SCADA 系统每 2～4 秒提供一个测量样本，没有同步时间戳[7]。在电网中引入相量测量单元（PMU）网络是为了改善 SCADA 系统的缺点。PMU 可以在其部署的节点上每秒产生 30～120 个同步时间戳的节点电压和支路电流相量，而 SCADA 只能监测它们的幅值。此外，PMU 利用 GPS 提供 1 毫秒精度的高速同步采样，因此 PMU 测量是全局同步的，称为同步相量。这意味着来自不同位置的 PMU 数据能够在同一时间戳上进行比较和集成。这种同步性使得状态估计系统能够更加精确地理解电力系统的运行状况，从而提高状态估计的准确性和可靠性。由于 PMU 可以提供高速、准确、全局同步的同步相量测量，因此同步相量应用广泛应用于智能电网的不同方面，如频率和电压监测、振荡检测、事件检测、自动化广域控制和补救行动方案[8]。

PMU 的同步特性与其所使用的 GPS 接收器有密切关系。PMU 通常利用 GPS 接收器获取高精度的时间戳，以确保数据的时间同步性。GPS 接收器提供了高精度的全球定位系统时间信号，这些信号用于同步 PMU 设备的内部时钟。这样，不同位置的 PMU 设备可以在相同的时刻记录电力系统中各种参数的测量数据，从而实现对电网状态的全面监测和准确估计。但 PMU 的使用的是未加密的 GPS 民用信号进行同步而易受到网络的攻击[9]，这种干扰 GPS 接收器的攻击方式常被称为 GPS 欺骗攻击（GPS Spoofing Attacks, GSA）。

GPS 欺骗攻击可以通过发送虚假的 GPS 信号，欺骗 PMU 设备，使其误认为当前时间或位置是虚假的。这可能导致 PMU 的时间同步出现偏差，影响其对电力系统状态的准确估计。攻击者可以干扰 GPS 信号，使 PMU 无法准确获得时间信息，进而影响数据的时间同步性。这种影响可能导致对电网状态的错误理解，使运营者难以及时发现或应对电力系统中的异常情况，从而可能增加电网故障的风险，甚至影响电力系统的稳定性和安全性[9]。所以，建立针对现实的 GPS 欺骗攻击的防御机制以保护电力系统的状态估计对保证电力系统的安全有重要意义。

本文从电力系统拓扑结构角度出发，基于估计理论方法提出相应策略检测和缓解GSA并对受攻击影响的电力系统进行安全状态估计。

1.2 国内外研究现状

1.2.1 电力系统估计研究现状

随着电力系统的日益庞大和复杂，为了实现电力系统的可靠运行，实时监测和控制变得非常重要。能源管理系统（Energy Management System , EMS）功能负责这项监测和控制任务。状态估计是能源管理系统的支柱，它为其他 EMS 功能提供了系统实时状态的数据库[10]。因此，高效、准确的状态估计是电力系统高效、可靠运行的前提。正确了解状态（如节点电压的幅值和相位）使我们能够制定控制方案以提高系统的稳定性和可靠性。

电网的状态估计包括通过 SCADA 采集实时测量数据，包括线流、注入量和电压测量，并使用预定义的状态估计算法计算状态向量。如果从同一时刻的测量集中获得 k 时刻的状态向量，则这种估计技术称为静态估计（Static State Estimation, SSE）。为了有规律地了解电力系统的状态，在适当的时间间隔内重复计算状态向量的过程。静态估计器在电力系统中有着广泛的应用，对输配电系统的可靠运行起着非常重要的作用。然而，随着系统中负荷的变化，发动机也必须进行相应的调整，这反过来又改变了整个系统的流量和注入，从而使整个系统动态。并且随着电力系统规模的扩大，发电机组和负荷的增加，系统变得非常庞大，需要在短时间间隔内进行静态估计，这将消耗大量的计算资源。因此，静态估计器可能无法有效地捕捉电力系统的这种动态行为。这导致了另一组称为“动态状态估计”（Dynamic State Estimation, DSE）技术的算法的发展，其使用了电力系统时变特性的实际物理建模。这些算法具有精度更高和能够提前一步预测系统状态的双重优点。即根据已知时刻“t”的状态向量，结合系统的数学模型，预测下一个时刻“$t+1$”的电力系统的状态向量。这种预测能力具有巨大的优势，因为安全分析现在可以提前一个时间戳进行，从而使操作员有更多的时间采取控制行动，特别是在任何紧急情况下[11]。因此，电力系统的动态状态估计算法是电力系统状态估计技术的一个重要分支，有可能影响电力系统实时监测和控制的运行

性质。

自 20 世纪 70 年代初 Schweppe 等在文献[12]-[14]将状态估计的概念引入电力系统领域以来，已经提出了许多计算电力系统状态向量的方法。在 1970 年之前，对准确状态估计的需求并不大，但随着电力系统的发展，电力电子设备的发展及其在电力系统中的应用，确定系统状态的旧做法变得难以继续。最初使用的是最小二乘估计（Least Square Estimation, LSE），多年来一直是许多研究人员的选择，但缺点是对系统模型精度的依赖程度高，不适合实时应用，数值稳定性差迫使研究人员对更新的算法产生兴趣。然而，这些算法适用于监控和数据采集（Supervisory Control and Data Acquisition, SCADA）系统，该系统使用远程终端单元（Remote Terminal Units, RTU）进行广域监控（Wide Area Monitorings, WAMs）的数据采集。为了提高 LSE 的速度，文献[15]中开发了一种使用有功和无功方程解耦的状态估计算法，并包括调节变压器比的估计，这种改进将估计时间减少了 80%。Irving 等人在文献[16]中提出了用于状态估计的线性规划，但其主要缺点是很难利用稀疏性和解耦现象，而这些现象加速了负荷流的研究，文献[17]中指出了这一点。滤波器提供了非线性系统状态的递归近最优最小方差估计。据报道，卡尔曼滤波（Kalman Filter, KF）方法的数值精度和稳定性较差，因此在上述基础上文献[18]提出使用平方根滤波器，提高了数值可靠性，仿真结果与传统 KF 方法几乎相同。近年来，基于 KF 的算法已经变得非常流行，因为它们可以实时给出状态估计的结果，在 KF 算法上的一些改进算法，如扩展卡尔曼滤波（Extended Kalman Filter, EKF）、无迹卡尔曼滤波（Unscented Kalman Filter, UKF）可以应用于非线性系统，这对于基于电力系统的应用来说是完美的，如文献[19]中就使用了 UKF 来确定系统状态并将其用于保护方案。但与这些算法相关的问题是它们需要精确的系统建模，部分或不确定的模型可以通过鲁棒迭代 KF 来处理[20]。数据采集和测量设备的进步，如 PMU 具有较高的数据传输刷新率，用于算法中可以大大提高估计的精准度和实时性。

更先进的技术，如文献[21]-[23]开发的粒子滤波（Particle Flter, PF）算法，以高计算量为代价提供了非常精确的估计。图 1-1 对静态估计下的最小二乘估计（LSE）和加权最小二乘估计（Weight Least Square, WLS）等各种状态估计技术进行了分类。动态状态估计包括序贯卡尔曼滤波（Sequential Kalman Filter, SKF）、

无迹卡尔曼滤波（UKF）、扩展卡尔曼滤波（EKF）和粒子滤波等方法。

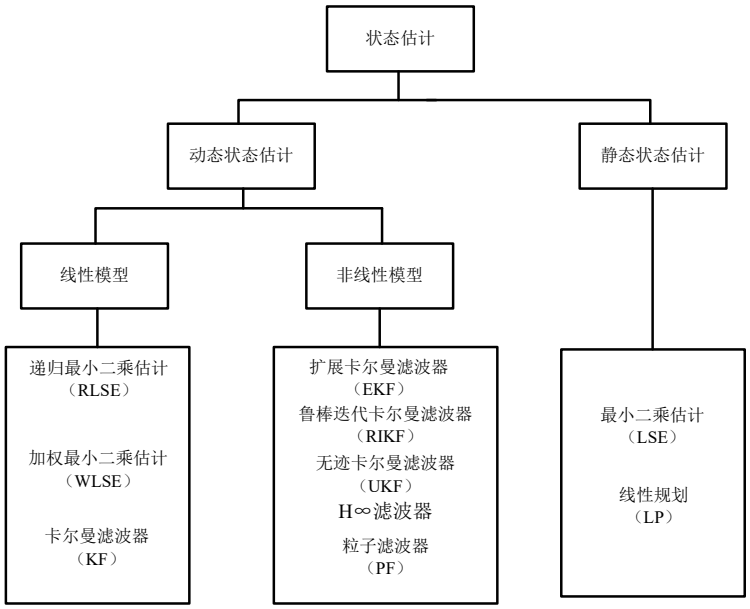


图 1-1 状态估计技术分类

在实际应用中，相量测量单元(Phasor measurement unit, PMU)已广泛应用于输电系统中，主要涵盖故障监测、保护和控制等电力系统。在配电网中，当可用的测量集合足以计算系统的状态向量时，称为可观测系统。为了对电力系统进行实时监控，在状态估计之前需要进行可观测性测试。如果系统是可观测的，那么可以直接进行状态估计。然而，在不可观测系统中，可以使用伪测量来估计网络的状态。电力系统状态估计的目的是对电力系统或输配电网络进行监测。新型信息设备的使用带来了更加精确的状态估计模型和估计精度。

文献[24]提出了一种新的基于 PMU 的多接地安全状态（Secure State Estimate，SSE）估计公式。基于支路电流的状态估计（Based on branch Current State Estimation, BCSE）方法在文献[25]中被提出。另外，文献[26]对所测试的两种不同网络模型的状态估计结果进行了分析。文献[27]在此基础上提出了一种基于混合测量的混合状态估计算法。从设备和其放置角度出发，文献[28]提出了智能电表放置和实现最优运行的混合状态估计器的概念。文献[29]提出了一种使用伪测量进行分布状态估计的方法。文献[30]讨论了线性化的三相配电类 SE 算法在智能配电系统中的应用。文献[31]讨论了满足精度约束的可靠性。为了提高配电系统的状态估计精度，文献[32]提出了一种基于人工神经网络的负荷预测模型。为了提高现有方法的准确性，文献[33]提出了 PASE 方法，并使用使用 EKF 估计方

法进行估计。针对数据随机传输时延、数据包丢失和无序的分布式网络系统，文献[34]提出了一种信息融合估计方法。

随着智能电网的发展，电网状态估计变得越来越重要，与此同时状态估计方法的发展也在同步进行，能够实时安全准确的对电网进行状态估计是智能电网进一步发展的基础和保障。

1.2.2 智能电网 GPS 欺骗攻击研究现状

近年来，智能电网持续加强基础设施建设以提升其安全性和可信赖度。然而，在这一过程中，智能化设备的广泛部署使得它们成为网络攻击的重点目标，暴露出了一些安全隐患。特别是 PMU 所产生的同步相量数据，由于其高度依赖于网络基础设施，更容易受到攻击。其中，GPS 欺骗攻击便是一种针对 PMU 的恶意行为，攻击者通过欺骗 PMU 的 GPS 接收机，使其接收到伪造的 GPS 信号，这些信号带有错误的时间戳，进而将误差引入 PMU 测量的相角值中。这种误差不仅干扰了电网的保护、控制功能，还可能影响监测系统的正常运行，给智能电网的安全带来严重威胁。因此，为更全面地了解这一威胁，我们有必要从攻击手段、检测方法和防御措施三个维度，对 GPS 欺骗攻击的现状进行研究现状分析。

随着电网安全和电网智能化的发展日益受到人们的关注，PMU 在电力系统状态估计中的作用越来越重要[35]-[40]。传统的电力系统监测方法依赖于 SCADA 系统进行稳态运行，但在预测电网状态、低频振荡、故障分析和实时安全监测方面的作用有限。相比之下，PMU 可以提供同步测量并生成可用于系统状态估计的线性模型。此外，它们的采样率远快于 SCADA，可以实时估计电力系统的状态，并对异常情况做出快速反应。通过为每个单元配备一个利用民用信号进行同步的 GPS 接收机[41]-[43]，可以实现 PMU 的高采样率和准确的时间同步。然而，民用 GPS 接收机容易受到产生虚假信号的网络攻击[44]，即 GPS 欺骗攻击(GPS spoofing attacks, GSA)。GPS 欺骗攻击会导致 PMU 与控制中心不同步，导致 PMU 的时间延迟和采样相位失配[45]，从而阻碍了对电网状态的实时准确估计，导致状态估计误差很大。因此，这些攻击对电力系统的安全性和经济性都是极为不利的。PMU 测量中的时间延迟问题及其补偿方法已在文献[46]中进行了讨论，但与 GSA 相比，这些方法的有效性有限。因此，人们对 GSA 的检测和对策进行了广泛的

研究，并提出了一些缓解其对电力系统造成严重破坏的方法。

在以往的研究中，针对 GPS 欺骗攻击的检测工作常采取两个阶段的策略：首先是在 GPS 信号接收阶段进行初步检测，随后在 PMU 测量数据后进行验证确认。在接收 GPS 信号的初步检测阶段，各种方法旨在识别无效的导航数据，进而判断系统是否受到 GPS 欺骗攻击。这些方法主要涵盖信号处理、天线防御、与其他时间源相关性的计算以及密码策略等四大类。其中，信号处理方法通过对接收到的 GPS 信号进行功率和质量的监测，提取特定导航信息特征来排除不相关数据，并利用 GPS 信号的数学关系来区分真实与虚假信号。而天线防御方法则依赖于波达角识别技术，但通常要求配备高水平的额外硬件支持。计算与其他卫星系统相关性的方法只适用于文献[45]中提到的 GPS 信号。而文献[47]中使用的加密策略用于检测 GPS 欺骗攻击，但成本高昂，需要修改 GPS 信号结构，并主要应用于军用 GPS 信号。

文献[48]中阐述了各种欺骗攻击以及针对商用接收机的建议对策。对抗策略包括漂移监测和基于加密的防御，以及基于信号几何的防御。GPS 原始信号中是否存在加密军用 P(Y)码，在文献[49]中进行了 GSA 检测。检测的方式是通过在广泛的发电站网络之间交叉相关 GPS 原始信号来查找被欺骗的节点。研究人员在文献[50]中设计了一种新的 GPS 接收器架构，该架构使用多个接收器来检测和定位欺骗者。所设计的接收机结构利用 GPS 信号在多个接收机之间的互相关特性来检测 GSA。文献[51]中的工作比较了预测和实际可见卫星，以确定静态接收器的 GSA。文献[52]设计了基于广义似然比的假设检验来进行 GSA 检测。[50]中开发的 GSA 检测算法需要额外的硬件来提供 GPS 原始测量，例如伪距。但上述文献[50]、[52]-[54]中的算法在检测 GSA 时没有提供减轻检测到的攻击的机制，也就是说，这些算法不估计对校正 PMU 测量中至关重要的攻击角度，这对于所提方法的有效性未能得到一个全面的分析。

除了检测 GSA 外，制定有效的 GSA 的对策也具有重要意义。之前的研究[53]-[55]中，GSA 通常被建模为附加的加性噪声。然而，如文献[56]已经表明，随着同步误差和同步间隔的增加，传统的估计方法会出现显著的退化。为了解决这些问题，文献[57]提出了一种新的欺骗弹性状态估计（Spoofing Resilience State Estimation, SR-SE）方法。文中为了提高 SR-SE 的估计性能，采用了扩展卡尔曼

滤波器来融合时变 GPS 和 PMU 测量值，建立了 GPS 和 PMU 测量耦合的测量模型。除此之外，目前已经提出了各种方法来试图缓解 GSA 带来的影响。例如从校正受攻击 PMU 测量的角度入手[37]·[48]-[55]。文献[58]分析了网格节点面对攻击的脆弱性，并提出了一种交替最小化（Alternative Minimization, AM）算法来重构这种攻击。文献[59]推导了一种由两阶段组成的欺骗匹配（Spoof Matching, SpM）算法。在第一阶段，SpM 算法检测电网欺骗攻击，并利用黄金分割搜索算法定位攻击相角。在第二阶段，SpM 算法对遭受 GSA 的数据进行校正。然而，它没有估计系统状态变量，这使得作者可以放松对电网可观测性的假设，并且最终状态变量估计的性能是未知的。与传统的基于残差的缓解时间同步攻击的技术相比，文献[36]提出了一种基于图形信号处理（Graphical Signal Processing, GSP）的算法，并使用机器学习算法将电力系统状态建模为低通图形信号。

1.2.3 研究现状分析

目前针对 GPS 欺骗攻击的智能电网状态估计研究，在国内外都有一定的探索。在国内，研究者们对 GPS 欺骗攻击进行了模型分析，探讨了其对智能电网状态估计的影响，并提出了一些针对性的安全算法，以增强系统的鲁棒性。一些研究团队也进行了实验验证和仿真工作，以验证这些安全算法的有效性。在国外，学者们通过对历史案例的分析，总结了 GPS 欺骗攻击的手法和后果，为今后的防御提供了借鉴。另外，一些国外团队还着眼于安全协议的设计，利用加密技术和认证机制提高智能电网系统对攻击的抵抗能力。此外，跨学科合作也成为国外研究的一个特点，将密码学、信息安全和智能电网技术相结合，探索更加全面的解决方案。然而，尽管有许多已提出的 GPS 欺骗攻击检测方法，但目前都存在各自的不足，比如在复杂攻击模型的分析上仍有待深入，检测性能有限尤其是同时面对多个 GSA 的情况下性能显著恶化。由于 GPS 欺骗攻击的类型多样化，若未能及时检测出这种攻击，可能对电网造成严重威胁。为了有效评估 GPS 欺骗攻击对电网的影响，迫切需要研究新的检测方法以提高准确性，从而能够更加精确实时的对电网状态进行估计。另外，跨领域合作的推进也需要更加深入，同时实验验证与仿真平台的完善也是未来研究的重要方向。综合而言，国内外针对 GPS 欺骗攻击的智能电网状态估计研究虽然取得了一定进展，但仍需要进一步

深入挖掘和完善。

1.3 本文主要研究内容及创新点

GPS 欺骗攻击是智能电网面临的一种新兴网络风险。攻击者通过制造并发送伪造的 GPS 信号，诱导 GPS 接收器接收这些虚假信息，进而在 PMU 的测量数据中注入误差。这些经过篡改的测量数据被传递至状态估计器，用于对系统运行状态进行评估，并最终送至控制中心，可能导致控制中心基于错误数据做出不恰当的决策。在充分借鉴国内外相关研究的基础上，本文深入剖析了 GPS 欺骗攻击的内在机理，并据此推导建立了基于 PMU 的 GPS 欺骗攻击状态估计模型。最后以该模型为研究对象，采用了基于测量残差的欺骗检测及系统状态估计方法，同时针对量测模型参数耦合的问题提出联合最大后验和最大似然算法对 GSA 进行检测及系统状态估计。并通过仿真验证了本文所提方法的可行性与有效性。

本文的具体内容如下：

第一章：阐述本文的研究背景及意义，阐述了 GPS 欺骗攻击对于智能电网的威胁以及智能电网实时精确状态估计的意义。说明了本文的研究背景、动机和意义，还概括了国内外相关的研究方法，并对研究现状进行分析，得出目前研究的不足及可以优化改进的方向；最后概括了本文的主要研究以及章节的安排。

第二章：首先分析研究了 PMU 受 GPS 欺骗攻击的原理，显示了该攻击对于系统实现实时状态估计的巨大挑战，随后介绍了 PMU 的布置对于系统全局可观测的影响，明确了系统全局可观测性是研究系统状态估计的必要部分。最后通过比较攻击前后线路中电压电流的变化情况以及安全条件下的量测模型推导出受 GSA 下的系统量测模型，并对推导出的模型进行分析，讨论其关键难点以及解决思路。为后续的攻击检测以及系统安全状态估计提供模型和理论基础。

第三章：针对所建立的受攻击下的 PMU 量测模型，提出了一种新的基于测量残差的电网欺骗检测与测量校正算法，该算法可以检测和缓解不同攻击角度的多个 GSA。其由两个关键的子算法组成：欺骗检测算法通过监测测量残差的欧几里得范数，以区分安全和欺骗攻击场景。在安全场景中，没有任何 PMU 被欺骗，而在欺骗场景中，有一个或多个 PMU 被不同的攻击角度欺骗。测量校正算

法将前一算法中检测出来的不良数据进行校正，最后将校正后的数据进行正确的系统状态估计。最后在不同测试系统进行了仿真实验，并且与其他研究方法进行了对比分析，仿真结果表明该方法对于检测和缓解 GSA 尤其是多个 GSA 存在时具有明显的效果。

第四章：针对受攻击后 PMU 量测模型的中存在的参数耦合未知和目标函数非凸等问题，提出了一种基于混合建模的测量模型，引入双模混合分布来表示 PMU 混合测量中的误差，该模型准确地表示了 PMU 的测量误差，并且提出了一种联合最大后验和最大似然算法来安全地估计 PMU 混合测量中系统的正确状态并检测 GSA。最后在不同测试系统进行了仿真实验，并且与其他研究方法进行了对比分析，仿真结果表明该方法对于检测和缓解 GSA 具有良好的效果。

第五章：对全文的工作内容和研究成果进行分析总结，分析目前存在的不足，最后对未来工作进行展望。

本文创新点可以总结为以下三个方面：

（1）推导出系统 PMU 受 GPS 欺骗攻击下通用测量模型：通过比较攻击前后线路中节点电压和支路电流的变化，推导出一种 GPS 欺骗攻击下通用的 PMU 量测模型，该模型可适用于不同规模和复杂程度的电力系统。这一通用模型为分析和检测电网中 PMU 的 GPS 欺骗攻击提供了统一的框架，具有广泛的适用性。

（2）针对量测模型中未知参数矩阵的特殊性，提出了一种有效的不良数据检测和校正算法。该算法能够将受攻击后的不良数据恢复到安全测量的残差范围内，即校正后的数据能够继续用于系统状态估计，并且该算法还可以精准定位到受攻击 PMU。这种处理避免了模型中两个未知参数难以估计的耦合问题。

（3）针对量测模型中存在的参数耦合以及目标函数的非凸等问题提出了基于混合建模的测量模型与安全联合估计算法。算法首先引入双模混合分布来表示 PMU 混合测量中的误差，提出了一种基于混合建模的测量模型，更准确地捕获了安全状态和受攻击状态下出现的测量变化。其次，提出了联合最大后验和最大似然估计算法（Joint Maximum a Posteriori and Maximum Likelihood, JMAP-ML），该算法克服了 GSA 下 PMU 测量模型中存在的参数耦合未知和目标函数非凸等问题，能够精确估计系统的状态，并通过引入二元隐变量来分类即检测出受攻击的 PMU，这为系统状态的准确估计和 GSA 的有效检测提供了新的解决方案。

第 2 章 基于 PMU 的智能电网 GPS 欺骗攻击模型

2.1 引言

在智能电网系统中，GPS 可以提供亚微秒级的精确授时，在 PMU 测量的时间同步中起到重要作用。然而由于民用 GPS 信号的低信号功率和非加密结构，PMU 容易受到攻击。GPS 欺骗攻击（GPS Spoofing Attacks, GSA）就是这样一种攻击，伪造的 GPS 信号以比民用信号更大的信号功率传输，从而诱导传统的 GPS 接收器采用伪造的 GPS 信号。攻击者可以通过这种方式引起时间延迟。感应的延时可以使得 PMU 测量的相位角发生偏移。不正确的相位角会降低网络的监控算法的性能。GSA 引起的 2.8 毫秒的时间延迟可以使故障线路检测算法误差 180 公里。此外，在 GSA 过程中，电网监测算法可能会对电力系统稳定性提出虚假警报，并提供错误的状态估计。这些程度上的误差已经超出了所规定允许的最大相位误差等的标准，可以被认为是一个不良数据的注入。以往对于 GPS 欺骗攻击的检测以及系统的状态估计方法已经提出很多，但是大都是没有明确的模型，它们通过检测出被攻击的数据进而剔除这些数据的方法来提高系统状态估计精度。这些方法损失了大量量测数据，检测性能不是很好，尤其是同时面对多个攻击时状态估计精度将产生极度恶化的情况。有攻击下的系统模型的量测模型，可以更加准确的确定被篡改的量测值的特征，进而可以更好对这一挑战研究出相应的防御对策，与此同时也需要充分了解 GSA 的工作原理以及其对电网的影响。

2.2 GPS 欺骗攻击

在现代化的社会中，GPS 已经成为一个重要的定位和导航技术。GPS 的最基本功能是提供位置定位服务，通过接收来自卫星的信号，可以确定地球上任何一个位置的经度、纬度和海拔高度等信息。此外，由于 GPS 可以提供非常准确的时间同步服务，可以帮助不同系统在时间上保持同步。现代智能电网系统对于能对系统进行实时监控提出了更高的要求，这就要求系统中布置的传感器要有更加精确的时间戳。带有 GPS 接收器的 PMU 就成为满足提高时间精度这一要求的最优解决方案。在系统中布置一定数量的 PMU 使得整个系统全局可观测便让可以

实现对整个系统进行实时的监控。但由于电力系统是一个分布式系统，因此需要保证各个 PMU 设备间的时间同步。GPS 提供了高精度的时间同步服务，可以为 PMU 设备提供精确的时间戳，从而提高电力系统的测量精度和稳定性。在本节中，将简要介绍 PMU 的组成和工作原理、基于 PMU 的电网系统的全局可观测性和 GPS 欺骗攻击原理。

2.2.1 相量测量单元

PMU 即同步相量测量单元，是一种专用于测量电力系统中同步量及相关参数的设备，用于采集原始信息、实时监测并反馈给其他设备。PMU 具有高测量精度、快速响应时间、无需外部电源等优点，能够快速而准确地完成同步相量测量。典型的 PMU 结构包括模拟采集部分、数字处理部分和通信接口部分。模拟采集部分由相位测量单元、电压测量单元和电压开关量采集单元组成，负责采集广范围内的同步相量和电压开关量，并将其转换为数字信号。数字处理部分包括数据处理模块、时间频控模块和状态提取模块，执行电压、功率计算、数据处理和转发等功能。PMU 具备卓越的通信能力，可通过以太网、GPRS 等方式传输采集的数据至监控系统，使监控系统更准确地判断电力系统状态。图 2-1 显示了 PMU 的基本原理框图。

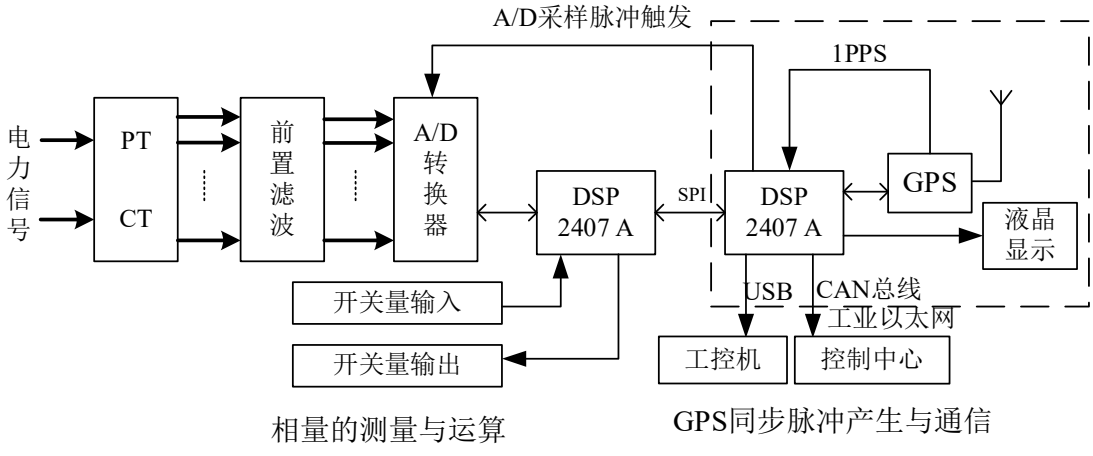


图 2-1 PMU 基本原理框图

每个 PMU 都配备有 GPS 接收器，来进行多个 PMU 的时间同步。GPS 系统是一个空间导航系统，通过 4 颗或更多全球定位系统卫星向地面发送地球的位置和时间信息。这些卫星能够连续发射无线电测距信号。而导航数据则包含了 GPS

接收器在计算卫星位置和时钟偏差时所需的关键信息。接收器接收卫星信号后，会进行一系列计算以确定位置和时间。这一过程中得到的距离被称为伪距，因为在计算时可能包含误差。图 2-2 详细展示了 GPS 接收器如何完成位置和时间的计算过程。

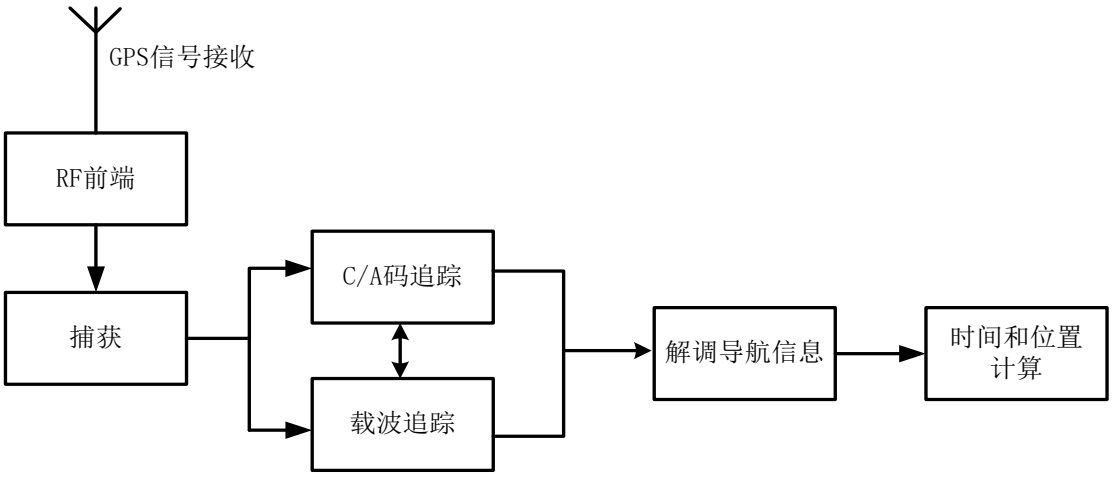


图 2-2 GPS 信号处理过程

2.2.2 基于 PMU 的电网可观测性分析

随着智能化电力系统的发展，对于电力系统运行状态的实时准确的监测就变得十分重要。PMU 因其高采样率，能实时监测电网状态而被广泛应用于电力系统状态估计中。状态估计是确保系统安全稳定运行的关键环节。而 PMU 作为现代电力系统中的关键测量设备，对于实现精确的状态估计具有不可替代的作用。然而，当 PMU 的布置无法满足全局可观测性时，其对状态估计的影响不容忽视。全局可观测性是状态估计的基石，它要求系统中的每个节点和支路的状态都能通过直接或间接的测量手段得到准确反映。然而，当 PMU 布置不全时，部分节点的状态信息将无法直接获取，导致状态估计算法无法全面、准确地反映系统的实时状态。这不仅限制了状态估计的准确性，还可能引入偏差和不确定性，使得估计结果难以信赖。

当 PMU 安装在电网的某个节点上时，可测量出该节点上的电压相位以及与该节点相连的支路的电流大小。如果 PMU 部署在电网的所有节点上，可以是整个电网系统可观测，即系统全局可观测。然而，由于 PMU 的部署成本昂贵以及技术等因素的限制，PMU 不可能大规模安装。因此，在关键位置部署 PMU 是保

证系统可观性的基础，使用最少数量的 PMU 使系统保持可观测性是当前一项重要研究课题。

在节点系统中，如果节点电压可以由测量装置直接或间接测量，则称该节点为可观察节点。如果该系统中所有的节点都是可观察节点，那么该系统就是可观察的。因此，在包含 PMU 的测量系统中，所有节点可以分为三类：直接测量节点（PMU 所安装的节点），间接测量节点（PMU 安装节点附近的节点）和其他可以计算的节点。系统的全局可观测性是实现电网实时监测和状态估计的前提。

以往的研究大多通过引入二元决策变量 x，将 PMU 最优化布置问题描述为一个整数线性规划问题，目标函数的基本形式为：

$$S = \min \sum_{i=1}^{k} w x_i \tag{2-1}$$

式中，k 表示系统中节点数量，w 表示每个 PMU 的成本，一般为了便于分析，认为所有 PMU 成本相同且均设为 1，这样最小化目标函数 S 的值即最小的 PMU 的数量。x_i 等于 1 或 0 分别表示节点 i 上安装 PMU 与否。然而，随着序贯二次规划（Sequential Quadratic Programming, SQP）的发展，非线性规划（Nonlinear Programming, NLP）在最优 PMU 布局问题中的应用已经成为可能。

与 ILP 不同，x_i 在 NLP 中被视为连续决策变量。因此，对于 NLP，必须约束 $x_i(x_i - 1) = 0$ 才能使 $x_i = 0$ 或 $x_i = 1$。

考虑每个 PMU 相同的 PMU 成本，最优 PMU 布局问题的非线性规划可以被表示为

$$S' = \min x^T x = \min \sum_{i=1}^{k} x_i^2 \tag{2-2}$$

$$subject \quad to \begin{cases} g(x) = 0 \\ 0 \le x \le 1 \end{cases} \tag{2-3}$$

其中 $g(x)$ 是一个相量函数，0、1 分别表示全 0 和全 1 列向量。并且函数 $g(x)$ 可以被表示为

$$g_i(x) = (1 - x_i) \prod_{j \in \xi_i} (1 - x_j) = 0 \tag{2-4}$$

其中第 i 项表示对第 i 节点的可观察性的约束，ξ_i 表示与节点 i 相邻的所有节点的

集合。

因此，通过在约束条件下求解目标函数 S' 即可得到使得某个电网系统全局可观测的最少的 PMU 数量。为之后的电网的实时安全监控带来可行性的基础铺垫。

2.2.3 GPS 欺骗攻击原理

全球导航卫星系统（Global Navigation Satellite System, GNSS）与 GPS 和伽利略系统一样，广泛用于军事和民用工业的许多重要应用，包括时间同步系统。GPS 授时信号还被金融、广播、移动通信、银行等分布式计算机网络应用等各个领域所使用。

恶意的传输是更加隐蔽的，这样接收者就无法识别攻击。如果恶意发射的信号向接收机提供了误导信号，接收机就会在空间中使用伪造信号并计算出错误的位置。这样的传输被称为欺骗。这与阻塞或干扰不同，阻塞或干扰会阻止位置锁定并导致激活备用导航设备。因此，一个成功的 GPS 欺骗是一个比阻断或干扰更有害的攻击。GPS 的 P 码是加密的，因此很难被欺骗，而民用 GPS 信号 C/A 码则更容易被欺骗，因为信号结构、编码和调制方式都是公开的。

PMU 中的 GPS 接收器接收到的信号就是采用未加密的民用信号。这就给在 GPS 接收器附近的攻击者机会通过带有篡改 C/A 码的 GPS 信号发生器数据进而发送带有公共 GPS 参数的伪造的 GPS 信号。这使得 PMU 中 GPS 接收器的信号接收前端接受到受欺骗的信号并将其视为真实信号进行处理。

欺骗可以分为简单型、中级型和高级型三种类型。简单欺骗器可以产生 GPS 信号，但不试图使其与当前广播的 GPS 信号一致。该简单欺骗器由连接到发射天线的 GPS 信号发生器组成。欺骗器向目标 GPS 接收器发送不一致的信号。因此，GPS 接收器既接收到真实信号，也接收到欺骗信号。此外，这种欺骗器需要 GPS 信号模拟器，通常在硬件中实现，这可能意味着高成本。中间欺骗者将伪造的 GPS 信号与当前广播的 GPS 信号同步。欺骗装置具有观测卫星的几何形状、多普勒频移、导航数据位和接收信号功率的知识。欺骗者首先进行码相对准，然后迫使跟踪环路跟踪伪造信号，同时攻击目标接收机的每个跟踪信道。复杂的欺骗器不仅可以与当前广播的GPS信号同步，还可以与附近其他欺骗器的伪造GPS

信号同步。更复杂的欺骗攻击可以通过使用多个发射天线来实现。

每种不同类型的攻击，对于 PMU 而言，攻击者都是在力争攻击模型的同时在 GPS 频率范围内传输高斯噪声，使得接收器失去 GPS 锁定的功能，进而有效干扰合法的 GPS 信号的传递。GPS 欺骗攻击的最终目标是攻击者可以操纵 PMU 的同步，造成被攻击者 PMU 的时间参考延迟，进而引起量测值的相位偏移，最后导致错误的系统状态估计。

2.3 GPS 欺骗攻击的系统测量模型

2.3.1 安全状态下系统测量模型

本节考虑一个由 $\mathcal{N}$ 个节点通过 ℓ 条传输线连接的电网系统，该系统由部署在若干个节点上的 M 个 PMU 实现全局观测。假设部署在节点 k 上的 PMU 可以测量节点 k 电压相量和与节点 k 相连的支路的所有电流相量。则节点 k 上 PMU 的测量值集合（在直角坐标系下）的相量表示为 $\boldsymbol{z}_k \in \mathbb{C}^{(2+2l)\times 1}$。$\boldsymbol{z}_k$ 可以表示为

$$\boldsymbol{z}_k = [U_k^r, U_k^i, I_{k1}^r, I_{k1}^i, ..., I_{kl}^r, I_{kl}^i]^T \tag{2-5}$$

其中，U_k^r，U_k^i 分别表示节点 k 处复电压的实部和虚部。I_{kl}^r，I_{kl}^i 分别表示支路 (k,l) 的复电流的实部和虚部，T 为相量转置符。此外，系统的状态 $\boldsymbol{x} \in \mathbb{C}^{2N\times 1}$ 为

$$\boldsymbol{x} = [U_1^r, U_1^i, ..., U_k^r, U_k^i, ..., U_N^r, U_N^i]^T \tag{2-6}$$

因此，利用网络的线路导纳矩阵，$\boldsymbol{z}_k$ 可以写成系统状态 $\boldsymbol{x}$ 的线性函数

$$\boldsymbol{z}_k = \boldsymbol{H}_k \boldsymbol{x} \tag{2-7}$$

其中 $\boldsymbol{z}_k$ 表示部署在节点 k 处的 PMU 的测量值，$\boldsymbol{H}_k$ 是与节点 k 相关的导纳矩阵，这里考虑 $\boldsymbol{z}_k$ 的无噪声形式是便于后续问题的研究。为了有一个简洁的表示，可以将 PMU 的测量值进行垂直堆叠排列以创建一个总体测量相量 $\boldsymbol{z}$。所以，PMU 的总体测量可表示为

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} \tag{2-8}$$

其中，$\boldsymbol{z} = [\boldsymbol{z}_1, ..., \boldsymbol{z}_M]^T$，$\boldsymbol{H} = [\boldsymbol{H}_1, ..., \boldsymbol{H}_M]^T$。

假设在 t 时刻接收到 PMU 的采样值，那么定义节点 k 在 t 时刻的连续电压信

号为

$$\bar{U}_k(t) = U_k(t)\cos(2\pi f_c t + \varphi_k(t)) \tag{2-9}$$

其中 f_c 是频率。$\bar{U}_k$ 可以表示为相量 $U_k(t)e^{j\varphi_k(t)}$，U_k(t) 表示幅度，$\varphi_k(t)$ 表示时刻 t 时的电压相位大小。

由于后续 GPS 欺骗攻击的分析是基于某一时刻采集的数据，因此为了简化符号，在后续公式中省略符号 t。因此，根据其相量形式，可以得到复电压的实部和虚部分别为

$$\begin{aligned} U_k^r &= U_k \cos\varphi_k \\ U_k^i &= U_k \sin\varphi_k \end{aligned} \tag{2-10}$$

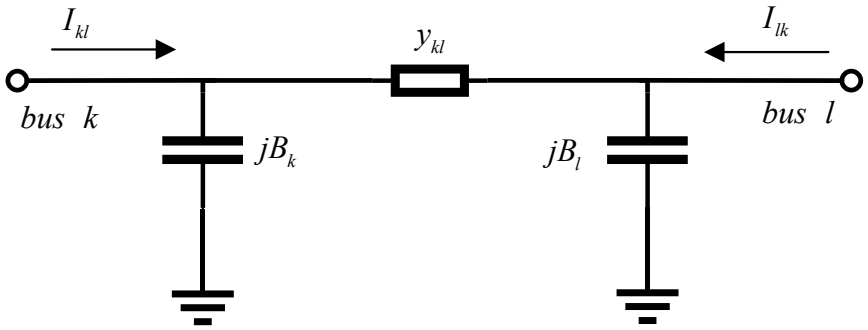


图 2-3 节点分支模型图

节点上的电压与通过支路的电流有关，如图 2-3 所示。记节点 k 处导纳为 B_k，支路 (k,l) 的导纳为 y_{kl}，且

$$y_{kl} = g_{kl} + j \cdot b_{kl} \tag{2-11}$$

其中，g_{kl} 为电导，b_{kl} 为电纳。假设这些节点和线路的参数均是已知且恒定的。那么，支路上的电流的实部和虚部可以由式(2-12)给出。

$$\begin{aligned} I_{kl}^r &= (U_k^r - U_l^r)g_{kl} - (U_k^i - U_l^i)b_{kl} - B_k U_k^i \\ I_{kl}^i &= (U_k^r - U_l^r)b_{kl} + (U_k^i - U_l^i)g_{kl} + B_k U_k^r. \end{aligned} \tag{2-12}$$

为了避免传统 SCADA 估计的时间偏性问题，本文考虑仅使用 PMU 进行状态估计。所以到此为止，通过使用电力系统的拓扑结构的线路参数知识，已经计算出安全条件下线路电压与电路的表达式如式(2-10)和式(2-12)所示。

下面将考虑在 GPS 欺骗攻击下，线路电压与电流的变化情况，方便通过比较攻击前后量测值的变化，找到模型的变化情况进而确定受 GPS 欺骗攻击下的

PMU 的量测模型。

2.3.2 受 GPS 欺骗攻击下的系统测量模型

在 GSA 存在的情况下，攻击者可以操纵 PMU 的同步，造成被攻击 PMU 的时间参考的延迟。对于受到攻击的测量，GSA 会保持相量幅值大小不变的情况下，引起了量测值 z_n 的相位 α_n 发生偏移。因此，可以将被攻击的量测值度量为

$$\boldsymbol{z}_n^{at} = \boldsymbol{z}_n e^{j\alpha_n} \tag{2-13}$$

其中，z_n^{at} 表示受攻击后的测量值。所以受攻击下整个系统的测量值可以表示为

$$\boldsymbol{z}^{at} = (\boldsymbol{z}_1^{at},...,\boldsymbol{z}_k^{at},...\boldsymbol{z}_M^{at})^T = \boldsymbol{z}^{at} \odot \boldsymbol{w} \tag{2-14}$$

其中，$\boldsymbol{w} = (e^{j\alpha_1},...,e^{j\alpha_k},...,e^{j\alpha_M})^T$ 是攻击相量，$\odot$ 为 Hadamard 积。当 PMU 不受攻击时，相位偏移角 $\alpha_n = 0$ 即 $e^{j\alpha_n} = 1$，此时测量值仍然时 $\boldsymbol{z}_n$。PMU 测量包括节点电压相量和连接到该节点的分支的所有电流相量。受 GPS 欺骗攻击后，这两类量测值将发生变化，具体来说，受攻击后电压量测值可以被表示为

$$\bar{U}_k^a = \bar{U}_k \cdot e^{j\alpha_k} = U_k \cdot e^{j\varphi_k} \cdot e^{j\alpha_k} = U_k \cdot e^{j(\varphi_k+\alpha_k)} \tag{2-15}$$

其中，α_k 为攻击引起相位偏移角，可以进一步被表示为

$$\alpha_k = 2\pi f_c t_k \tag{2-16}$$

其中，t_k 是由于攻击导致的第 k 个 PMU 发生的时间延迟。因此，在直角坐标系中对(2-15)进行变换可以得到攻击后的电压测量值的实部和虚部分别为

$$\begin{aligned} \bar{U}_k^{a,r} &= U_k \cos(\alpha_k + \varphi_k) \\ &= U_k \cos\alpha_k \cdot \cos\varphi_k - U_k \sin\alpha_k \cdot \sin\varphi_k \\ &= U_k^r \cos\alpha_k - U_k^i \sin\alpha_k \end{aligned} \tag{2-17}$$

$$\begin{aligned} \bar{U}_k^{a,i} &= U_k \sin(\alpha_k + \varphi_k) \\ &= U_k \sin\alpha_k \cdot \cos\varphi_k + U_k \cos\alpha_k \cdot \sin\varphi_k \\ &= U_k^r \sin\alpha_k + U_k^i \cos\alpha_k \end{aligned} \tag{2-18}$$

另外，由于被攻击后系统节点电压发生了变化，而电路拓扑结构以及电路参数没有发生变化，所以被攻击后电流的实部和虚部的表达式因为同步延时也将发生变化，变化后的表达式分别如式(2-19)和式(2-20)所示。

$$\begin{aligned} I_{kl}^{a,r} &= (U_k\cos(\alpha_k+\varphi_{\mathrm{k}})-U_l\cos(\alpha_k+\varphi_{\mathrm{k}}))g_{kl} \\ &-(U_k\sin(\alpha_k+\varphi_{\mathrm{k}})-U_l\sin(\alpha_k+\varphi_{\mathrm{k}}))b_{kl}-B_kU_k\sin(\alpha_k+\varphi_{\mathrm{k}}) \\ &= U_k^r(g_{kl}\cos\alpha_k-b_{kl}\sin\alpha_k-B_k\sin\alpha_k+U_l^r(-g_{kl}\cos\alpha_k+b_{kl}\sin\alpha_k) \\ &+U_k^i(-g_{kl}\sin\alpha_k-b_{kl}\cos\alpha_k-B_k\cos\alpha_k)+U_l^i(g_{kl}\sin\alpha_k+b_{kl}\cos\alpha_k) \end{aligned} \tag{2-19}$$

$$\begin{aligned} I_{kl}^{a,i} &= (U_k\cos(\alpha_k+\varphi_{\mathrm{k}})-U_l\cos(\alpha_k+\varphi_{\mathrm{k}}))b_{kl} \\ &+(U_k\sin(\alpha_k+\varphi_{\mathrm{k}})-U_l\sin(\alpha_k+\varphi_{\mathrm{k}}))g_{kl}+B_kU_k\cos(\alpha_k+\varphi_{\mathrm{k}}) \\ &= U_k^r(b_{kl}\cos\alpha_k+g_{kl}\sin\alpha_k+B_k\cos\alpha_k)+U_l^r(-b_{kl}\cos\alpha_k-g_{kl}\sin\alpha_k) \\ &+U_k^i(-b_{kl}\sin\alpha_k+g_{kl}\cos\alpha_k-B_k\sin\alpha_k)+U_l^i(b_{kl}\sin\alpha_k-g_{kl}\cos\alpha_k) \end{aligned} \tag{2-20}$$

需要注意的是，由于 GSA 对 PMU 在任何时刻测量的所有信号的影响都是相同的，因此同一时刻下电压和电流的相位角变化都是相同的。

综上，已经分别求解出了一个系统受 GPS 欺骗攻击前后的节点电压和线路电压。而且已知了安全条件下系统的 PMU 测量模型为式(2-7)。因此，通过比较，可以得到攻击之后系统 PMU 的量测模型为

$$\boldsymbol{z}_k^{at}=\boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}+\boldsymbol{e}_k \tag{2-21}$$

其中，$\boldsymbol{\tau}_k$ 是具有以下子矩阵的块对角矩阵，

$$\boldsymbol{G}=\begin{bmatrix}\cos\alpha_k & -\sin\alpha_k\\ \sin\alpha_k & \cos\alpha_k\end{bmatrix} \tag{2-22}$$

矩阵 H_k 可以写成

$$\boldsymbol{H}_{\mathrm{k}}=\begin{bmatrix}I & 0 & \cdots & 0\\ \boldsymbol{\Psi}_{k1} & \tilde{\boldsymbol{\Psi}}_{k1} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{\Psi}_{kl} & 0 & \cdots & \tilde{\boldsymbol{\Psi}}_{kl}\end{bmatrix} \tag{2-23}$$

其中

$$\boldsymbol{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \tag{2-24}$$

$$\boldsymbol{\Psi}_{kl}=\begin{bmatrix}g_{kl} & B_k+b_{kl}\\ -B_k-b_{kl} & g_{kl}\end{bmatrix} \tag{2-25}$$

$$\tilde{\boldsymbol{\Psi}}_{kl}=\begin{bmatrix}-g_{kl} & b_{kl}\\ -b_{kl} & -g_{kl}\end{bmatrix} \tag{2-26}$$

并且 $\boldsymbol{\tau}_k$ 依赖于 α_k，当 $\alpha_k=0$ 即系统中没有 GSA 时，$\boldsymbol{\tau}_k=\boldsymbol{I}_{2l+2}$。

因此，受 GPS 欺骗攻击影响下，系统中所以 PMU 构成的量测模型可以被表示为

$$\boldsymbol{z}^{at} = \boldsymbol{\Gamma H x} + \boldsymbol{e} \tag{2-27}$$

综合上述推导及分析，已经从电路网络的拓扑结构及参数入手，利用 GSA 的影响会导致 PMU 的量测值的相位发生偏移这一特性，通过比较攻击前后电压电流的变化情况以及安全条件下的量测模型推导出受 GSA 下的系统量测模型如式(2-27)所示。有了受攻击下的系统模型，就可以通过对模型的特征分析和处理，这使得对 GSA 的缓解以及防御策略的提出奠定了良好的前期条件。

2.4 模型分析

上一小节中，通过求解并比较出安全条件下和受攻击影响后的系统中节点电压以及支路电流的变化，得到了系统受攻击下的 PMU 量测模型如式(2-27)所示。

对于受欺骗攻击下的 PMU 量测模型 $\boldsymbol{z}^{at} = \boldsymbol{\Gamma H x} + \boldsymbol{e}$，可以认为其中的 $\boldsymbol{Hx}$ 表示系统 PMU 上没有发生 GSA 的时的无噪声测量相量，它表示在安全条件下获得的测量值。然而，受欺骗攻击影响的 PMU 测量模型引入了状态变量 $\boldsymbol{x}$ 与由攻击导致的攻角参数矩阵 $\boldsymbol{\Gamma}$ 产生耦合关联，这种耦合关系使得攻击对系统状态估计的影响难以直接分离和量化。在构建受攻击下 PMU 测量模型时，需要充分考虑这种耦合关系，并寻找合适的方法对其进行处理，以准确反映攻击对系统状态估计的影响。因此，如何有效处理这种非线性关系，分别估计出状态变量 $\boldsymbol{x}$ 以及攻角 α 是解决该问题的一个关键难点。

传统的处理参数耦合的估计方法可以采用交替最小化算法（Alternating Mnimization, AM），AM 算法是一种迭代优化算法，主要用于解决最小化多元函数的问题。该算法的基本原理是通过交替更新两个或多个变量来逐步优化目标函数。在每个迭代步骤中，算法会先固定其中一个变量，然后通过求解另一个变量的最优解来更新当前变量的值，这个过程会持续进行，直到目标函数收敛到最优解为止。AM 算法的一个显著优点是其收敛速度相对较快，并且对于大规模问题也能有效地求解。不过，该方法也有一些缺点，首先 AM 算法对初始值的选择较为敏感，不恰当的初始值可能导致算法陷入局部最优解而非全局最优解，这在实

际应用中可能需要进行多次尝试以获得更好的结果。此外，当参数之间的耦合关系复杂时，交替最小化方法可能难以充分探索整个解空间，从而难以得到准确的解。另外，该方法的稳定性也存在问题，特别是在数据存在噪声或异常值的情况下，可能会产生不稳定的解。

所以，综上所述，对于系统受攻击下的 PMU 量测模型的待估参数耦合的处理需要寻求新的有效解决方法，合理的解耦方法能够大大提高参数的估计精准度。

2.5 本章小结

本章首先分析 PMU 受 GPS 欺骗攻击的原理，显示了该攻击对于系统实现实时状态估计的巨大挑战，该攻击会轻易修改 PMU 获得的系统实时的量测值，并通过给出错误的指令造成大规模的电网事故，了解其攻击方式和机理为进一步研究该攻击的检测与防御提供前期准备。随后介绍了 PMU 的部署对于系统全局可观测的影响，明确了系统全局可观测性是研究系统状态估计的必要部分。最后通过比较攻击前后电压电流的变化情况以及安全条件下的量测模型推导出受 GSA 下的系统量测模型。有了攻击下的系统量测模型，就能更好的提出相应的对策进行攻击的检测和防御，为进一步的研究提供了可操作的空间和清晰研究方向。

第 3 章 基于测量残差的 GPS 欺骗攻击检测和系统状态估计方法

3.1 引言

随着电力系统的数字化和智能化程度的提升，其安全性和可靠性面临着新的挑战，尤其是对于 GPS 欺骗攻击（GPS Spoofing Attack, GSA）的威胁。在电力网中，常用测量残差来检测不良数据，然而，传统的残差分析方法假设坏数据具有可加性，而 GSA 引入的是乘法性质的不良数据。这种攻击形式使得一些加性噪声不会增加残差范数，从而使得基于残差的检测算法无法有效检测。因此，对于 GSA 攻击下的测量残差分析成为当前电力系统安全研究中的重要课题。本章针对 GSA 攻击下的测量残差进行了深入研究与分析，并推导出了在此情况下测量残差范数增加的必要条件。研究发现，在 GSA 攻击影响下，测量的残差会产生明显偏差，因此通过分析受攻击前后残差的情况来区分安全场景和攻击场景变得合理而有效。此外，基于残差的分析还进一步探讨了 GSA 攻击检测、受攻击数据校正以及安全状态估计的算法原理和实现，为电力系统的安全性提供了重要参考。

3.2 GPS 欺骗攻击下测量残差分析

系统未受攻击情况下，可以利用可用的量测值 $\boldsymbol{z}$ 来确定状态变量 $\boldsymbol{x}$。在系统完全可观测的条件下，可根据最小二乘准则建立出目标函数为

$$J(\boldsymbol{x})=[\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}]^T[\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}] \tag{3-1}$$

令目标函数 $J(\boldsymbol{x})$ 最小即可得到状态估计值 $\hat{\boldsymbol{x}}$，即求解目标函数式(3-2)。

$$\min_{x} J(\boldsymbol{x})=\min_{x}\{[\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}]^T[\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}]\} \tag{3-2}$$

要使目标函数最小，可对 $J(\boldsymbol{x})$ 求偏导并令为零，即

$$\frac{\partial J(\boldsymbol{x})}{\partial \boldsymbol{x}}=-2\boldsymbol{H}^T\boldsymbol{z}+2\boldsymbol{H}^T\boldsymbol{H}\boldsymbol{x}=0 \tag{3-3}$$

通过求解式(3-3)可得到状态估计向量 $\hat{\boldsymbol{x}}$ 为

$$\hat{\boldsymbol{x}} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{z} \tag{3-4}$$

其中，$\hat{\boldsymbol{x}}$是电网系统的估计状态。

在安全状态下，系统中没有任何一个 PMU 受到攻击，此时系统 PMU 的测量残差为

$$\begin{aligned}\boldsymbol{r} &= \boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} \\ &= \boldsymbol{z} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{z} \\ &= \boldsymbol{z} - \boldsymbol{H}\boldsymbol{H}^{\dagger}\boldsymbol{z}\end{aligned} \tag{3-5}$$

其中，$\boldsymbol{H}^{\dagger} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T$，$\boldsymbol{r}$为 PMU 测量残差。

由式(2-8)可知，$\boldsymbol{z}$的期望为$\boldsymbol{Hx}$。可以这一已知条件，对式(3-5)两边同时取期望，可以得到

$$\begin{aligned}E[\boldsymbol{r}] &= E[\boldsymbol{z}] - \boldsymbol{H}\boldsymbol{H}^{\dagger}E[\boldsymbol{z}] \\ &= \boldsymbol{Hx} - \boldsymbol{H}\boldsymbol{H}^{\dagger}\boldsymbol{Hx} \\ &= \boldsymbol{Hx} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{Hx} \\ &= 0\end{aligned} \tag{3-6}$$

其中，$E[\cdot]$为期望运算符。

因此，由式(3-6)可知，在 PMU 未受 GSA 情况下测量残差向量的的期望为 0。

当系统中一个或多个 PMU 受 GSA 影响时的系统 PMU 的测量残差为

$$\begin{aligned}\boldsymbol{r}^{at} &= \boldsymbol{z}^{at} - \boldsymbol{H}\hat{\boldsymbol{x}}^{at} \\ &= \boldsymbol{z}^{at} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{z}^{at} \\ &= \boldsymbol{\Gamma z} - \boldsymbol{H}\boldsymbol{H}^{\dagger}\boldsymbol{\Gamma z}\end{aligned} \tag{3-7}$$

其中，$\boldsymbol{r}^{at}$为 GSA 下 PMU 测量的残差矢量。

为了进行简化表示，这里使用m_{us}表示没有受攻击影响的 PMU 的集合，使用m_s表示受攻击的 PMU 的集合。所以，被攻击的测量值可以被改写为

$$\boldsymbol{z}^{at} = \begin{bmatrix}\boldsymbol{I}_{m_{us}} & 0 \\ 0 & \boldsymbol{\gamma}_{m_s}\end{bmatrix}\boldsymbol{z} = \begin{bmatrix}\boldsymbol{z}_{m_{us}} \\ \boldsymbol{\gamma}_{m_s}\boldsymbol{z}_{m_s}\end{bmatrix} \tag{3-8}$$

其中，$\boldsymbol{z}_{m_{us}}$表示所有未受攻击的 PMU 所对应的原始测量值，$\boldsymbol{z}_{m_s}$表示受攻击的 PMU 所对应的原始测量值。因此，式(3-7)可以被简化表示为

$$\begin{aligned}\boldsymbol{r}^{at} &= \begin{bmatrix} \boldsymbol{z}_{m_{us}} \\ \boldsymbol{\gamma}_{m_s}\boldsymbol{z}_{m_s} \end{bmatrix} - \boldsymbol{H}\boldsymbol{H}^{\dagger}\begin{bmatrix} \boldsymbol{z}_{m_{us}} \\ \boldsymbol{\gamma}_{m_s}\boldsymbol{z}_{m_s} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{z}_{m_{us}} \\ \boldsymbol{\gamma}_{m_s}\boldsymbol{z}_{m_s} + \boldsymbol{z}_{m_s} - \boldsymbol{z}_{m_s} \end{bmatrix} - \boldsymbol{H}\boldsymbol{H}^{\dagger}\begin{bmatrix} \boldsymbol{z}_{m_{us}} \\ \boldsymbol{\gamma}_{m_s}\boldsymbol{z}_{m_s} + \boldsymbol{z}_{m_s} - \boldsymbol{z}_{m_s} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{z}_{m_{us}} \\ \boldsymbol{z}_{m_s} \end{bmatrix} - \boldsymbol{H}\boldsymbol{H}^{\dagger}\begin{bmatrix} \boldsymbol{z}_{m_{us}} \\ \boldsymbol{z}_{m_s} \end{bmatrix} + \begin{bmatrix} 0 \\ (\boldsymbol{\gamma}_{m_s} - \boldsymbol{I}_{m_s})\boldsymbol{z}_{m_s} \end{bmatrix} - \boldsymbol{H}\boldsymbol{H}^{\dagger}\begin{bmatrix} 0 \\ (\boldsymbol{\gamma}_{m_s} - \boldsymbol{I}_{m_s})\boldsymbol{z}_{m_s} \end{bmatrix} \\ &= \boldsymbol{r} + \begin{bmatrix} -\boldsymbol{H}_{m_{us}}\boldsymbol{H}_{m_s}^{\dagger}(\boldsymbol{\gamma}_{m_s} - \boldsymbol{I}_{m_s})\boldsymbol{z}_{m_s} \\ (\boldsymbol{I}_{m_s} - \boldsymbol{H}_{m_s}\boldsymbol{H}_{m_s}^{\dagger})(\boldsymbol{\gamma}_{m_s} - \boldsymbol{I}_{m_s})\boldsymbol{z}_{m_s} \end{bmatrix}\end{aligned} \tag{3-9}$$

其中，矩阵 $\boldsymbol{H}_{m_{us}}$ 和 $\boldsymbol{H}_{m_s}$ 分别矩阵 $\boldsymbol{H}$ 相对应未受攻击和受攻击的 PMU 的行，矩阵 $\boldsymbol{H}_{m_s}^{\dagger}$ 表示受攻击 PMU 相对应的矩阵 $\boldsymbol{H}^{\dagger}$ 的列。

同样地，对式(3-9)两边同时取期望，可以得到

$$\begin{aligned}E[\boldsymbol{r}^{at}] &= E[\boldsymbol{r}] + \begin{bmatrix} -\boldsymbol{H}_{m_{us}}\boldsymbol{H}_{m_s}^{\dagger}(\boldsymbol{\gamma}_{m_s} - \boldsymbol{I}_{m_s})E[\boldsymbol{z}_{m_s}] \\ (\boldsymbol{I}_{m_s} - \boldsymbol{H}_{m_s}\boldsymbol{H}_{m_s}^{\dagger})(\boldsymbol{\gamma}_{m_s} - \boldsymbol{I}_{m_s})E[\boldsymbol{z}_{m_s}] \end{bmatrix} \\ &= \begin{bmatrix} -\boldsymbol{H}_{m_{us}}\boldsymbol{H}_{m_s}^{\dagger}(\boldsymbol{\gamma}_{m_s} - \boldsymbol{I}_{m_s})E[\boldsymbol{z}_{m_s}] \\ (\boldsymbol{I}_{m_s} - \boldsymbol{H}_{m_s}\boldsymbol{H}_{m_s}^{\dagger})(\boldsymbol{\gamma}_{m_s} - \boldsymbol{I}_{m_s})E[\boldsymbol{z}_{m_s}] \end{bmatrix} \\ &\neq 0\end{aligned} \tag{3-10}$$

因为 $E[z_{m_s}]$ 是非零的，所以受攻击下残差的期望是非零的。因此可以证明 PMU 受 GSA 影响下测量的残差会产生偏差。所以，可以初步认定通过分析受攻击前后测量残差的情况来区分安全场景和攻击场景是合理。并且，通过进一步的分析发现发生这一攻击后，测量的残差范数是增大的，即当矩阵 $(\boldsymbol{I} - \boldsymbol{H}\boldsymbol{H}^{\dagger})$ 是半正定矩阵时，有 $\|\boldsymbol{r}^{at}\|^2 \geq \|\boldsymbol{r}\|^2$。具体证明过程如下。

证明：为了方便表示和计算，设 $b = \begin{bmatrix} 0 \\ (\boldsymbol{\gamma}_{ms} - \boldsymbol{I}_{ms})\boldsymbol{z}_{ms} \end{bmatrix}$，

所以式(3-9)可以被改写为

$$\begin{aligned}\boldsymbol{r}^{at} &= \boldsymbol{r} + (\boldsymbol{I} - \boldsymbol{H}\boldsymbol{H}^{\dagger})\boldsymbol{b} \\ &= (\boldsymbol{I} - \boldsymbol{H}\boldsymbol{H}^{\dagger})\boldsymbol{z} + (\boldsymbol{I} - \boldsymbol{H}\boldsymbol{H}^{\dagger})\boldsymbol{b}\end{aligned} \tag{3-11}$$

对式(3-8)两边取范数可以得到

$$
\begin{aligned}
\|\boldsymbol{r}^{at}\|^2 &= \|\boldsymbol{r}\|^2 + \|(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{?})\boldsymbol{b}\|^2 \\
&\quad + 2\boldsymbol{z}^T(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})^T(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})\boldsymbol{b} \\
&= \|(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})\boldsymbol{b}\|^2 + 2\boldsymbol{z}^T(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})^T\boldsymbol{b} \\
&\quad -2\boldsymbol{z}^T(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})^T\boldsymbol{b} + \|\boldsymbol{r}\|^2 \\
&= \|(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})\boldsymbol{b}\|^2 + 2\boldsymbol{z}^T(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})^T\boldsymbol{b} \\
&\quad -2\boldsymbol{z}^T(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})^T\boldsymbol{b} + \|\boldsymbol{r}\|^2 \\
&= \|\boldsymbol{r}\|^2 + \|(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})\boldsymbol{b}\|^2 + 2\boldsymbol{z}^T(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})^T\boldsymbol{b}
\end{aligned}
\tag{3-12}
$$

因为 $\boldsymbol{H}\boldsymbol{H}^{\dagger}=\boldsymbol{H}\boldsymbol{H}^{\dagger}\boldsymbol{H}\boldsymbol{H}^{\dagger}$，由于伪逆矩阵的结构的存在且 $(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})$ 是半正定的，所以最后一项是正数，那么可以得出

$$\|\boldsymbol{r}^{at}\|^2 > \|\boldsymbol{r}\|^2 \tag{3-13}$$

上述证明表明，GSA 下的残差范数将大于安全条件下的残差范数。但是需要注意的是，这里矩阵 $(\boldsymbol{I}-\boldsymbol{H}\boldsymbol{H}^{\dagger})$ 的半正定是保证 GSA 下残差范数增加的必要条件，而不是一个充分条件，即残差范数的增加并不一定就意味着存在 GSA。

3.3 基于测量残差的欺骗检测及系统状态估计方法

3.3.1 GPS 欺骗攻击检测方法

在上一节中，针对系统受 GSA 前后的量测值进行了详尽的残差分析。经过细致的对比与计算，可以发现，当系统中存在 GSA 这种攻击时，PMU 所获取的量测值的测量残差会显著增大。这一发现为我们提供了一个有效的手段来识别数据是否受到 GSA 的影响。因此，可以通过给测量数据设置残差阈值 ε 的方法来识别某些数据是否受到 GSA 的影响。当测量的残差大于给定的阈值 ε 时，算法认为测量该数据的 PMU 受到了攻击，否则数据就是安全的。对于如何设定这个关键的阈值需要继续深入探究 GSA 攻击对测量残差的影响。在之前的分析中，已经明确了 GSA 攻击会导致测量残差增加。基于这一认识，在安全的电力系统条件下进行了细致的蒙特卡罗模拟。通过模拟，能够获取到一系列安全场景下的测量残差数据。在这些数据中，选取了最大的测量残差作为阈值 ε，以此来区分安全场景和可能受到 GSA 攻击的场景。

具体的仿真过程如下：首先，利用 MATPOWER 这一专业的电力系统仿真软

件，对电力系统进行精确的建模与仿真。随后，根据式(2-8)，生成 PMU 的稳态测量值。接着，利用最小二乘估计法对电力系统的状态进行了准确的估计。在这一基础上，可以计算出了这些安全测量条件下的测量值的残差 $\boldsymbol{r}$，并从中挑选出了最大的残差。为了确保阈值的准确性，实验进行了多次模拟，并对每次模拟得到的最大残差进行了记录与比较。最终，确定了最大残差范数 $\boldsymbol{r}_{\max}$，并将其记录为阈值即 $\boldsymbol{r}^{\max}=\varepsilon$。这一阈值将作为判断 PMU 数据是否受到 GSA 攻击的重要依据。

3.3.2 GPS 欺骗攻击测量校正及系统状态估计

经过 GSA 检测算法步骤后，测量数据可以被区分为两类：一类是未受攻击影响的安全数据，这类数据可以正常的进行系统的状态估计，另一类是残差大于给定阈值的数据即受攻击影响的数据，这些数据将被记录并进行数据校正后再被使用。

本节，从攻击模型本身的未知参数矩阵的特性出发提出了特定的测量校正算法来估计攻角并校正被攻击的数据，使得这些测量值也可用于状态估计。

为了方便分析，首先只考虑当个 PMU 受攻击情况。此时包含攻角的参数矩阵 $\boldsymbol{\Gamma}$ 的子矩阵 G 可以被表示为

$$\boldsymbol{G}=\begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix} \tag{3-14}$$

其中，α 表示由攻击导致的相位偏移角。根据矩阵 **G** 的特殊性以及三角函数 $\cos^2\theta+\sin^2\theta=1$ 的性质，可以得到

$$\boldsymbol{G}^T\boldsymbol{G}=\begin{bmatrix}\cos\alpha & \sin\alpha\\ -\sin\alpha & \cos\alpha\end{bmatrix}\begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \tag{3-15}$$

因此，对于整个系统而言，被攻击测量引入的攻角矩阵，可以得到

$$\boldsymbol{\Gamma}^T\boldsymbol{\Gamma}=\boldsymbol{I} \tag{3-16}$$

其中，$\boldsymbol{I}$ 为单位矩阵。

所以，结合式(2-27)可以得到被攻击数据的校正方法可以由下式给出。

$$\boldsymbol{z}_{new}=\boldsymbol{\Gamma}^T\boldsymbol{z}^{at} \tag{3-17}$$

其中，$\boldsymbol{z}_{new}$表示校正后可正常被用作系统状态估计的新值。校正后的新值接近真实值，可以用来后续的 LSE 进而估计系统的状态，即

$$\hat{\boldsymbol{x}} = (\boldsymbol{H}^T \boldsymbol{H})^{-1} \boldsymbol{H}^T \boldsymbol{z}_{new} \tag{3-18}$$

当 PMU 被检测到受到攻击时，即其测量的残差超过给定的阈值，可以使用迭代方法最小化这些残差，并将这组数据恢复到可以执行安全状态估计的水平。为此，这个问题的目标是

$$\underset{\alpha}{minimize} \| r_{max}^{at} \| \tag{3-19}$$

该问题的难点在于当估计攻角α时目标函数$r_{\max}^{at}$中的状态估计相量$\boldsymbol{x}$也是未知的，这会导致目标函数成为非凸函数。求出的结果也会存在多个局部最优解，影响估计精度。由于攻角估计是数据校正的基础，所以，本方法将先给出未知参数矩阵$\boldsymbol{x}$的一个先验估计，这样目标函数即变成只含有一个未知量的凸优化问题，可利用梯度下降法进行求解。

具体校正被攻击测量值以及安全状态估计过程的具体步骤如下：

1）残差范数比较与数据安全性判断：计算当前测量数据的总体残差范数，这是衡量测量数据与预期值之间差异的关键指标。将这个计算得到的残差范数与之前设定的的阈值进行比较。如果$\| \boldsymbol{r}^{at} \|^2 \leq \| \boldsymbol{r} \|^2$，则可以认为这组数据是安全数据，没有受到 GSA 的影响，而如果$\| \boldsymbol{r}^{at} \|^2 > \| \boldsymbol{r} \|^2$，则数据受到 GSA 攻击影响即数据是不良数据。

2）攻角估计与不良数据校正：当确定测量值受到了攻击时，需要通过求解目标函数(3-19)来估计攻角。最小化该目标函数的具体步骤如下：

a）首先选取残差范数最大的 PMU，计算其具体残差值，这个残差反映了测量值与预期值之间的偏差；

b）基于当前的电力系统状态给出一个先验状态估计$\boldsymbol{x}$。然后，通过相对于攻角来最小化目标函数，就可以估计出攻角的大小。这个攻角估计值是对攻击影响的量化表示；

c）得到攻角估计值后，可以利用式(3-17)对受攻击的 PMU 测量的相位角进行校正。这一步的目的是消除攻击对测量数据的影响，使得校正后的数据更接近真实值。校正完成后，更新电力系统的状态估计值$\boldsymbol{x}$。然后，重复这个过程，不

断迭代优化，直到状态估计值收敛；

3）重复残差范数比较与收敛性判断：重复步骤 1，直到测量的残差范数满足 $\| \boldsymbol{r}^{at} \|^2 \leq \boldsymbol{\varepsilon}$。

通过先着手对参数矩阵 $\boldsymbol{\Gamma}$ 的处理之后，可以初步估计出攻角的大小，这样以来，两个未知参数耦合下目标函数(2-27)为非凸函数的难题就变得相对简单了。这使得所提的攻击检测、被攻击数据校正和安全状态估计的整个算法更加高效和准确。

整个算法的原理和实现过程流程被清晰地展示在图 3-1 中。从图中可以看到，算法从残差范数的计算开始，经过攻角估计和数据校正，最终通过重复迭代达到收敛状态。

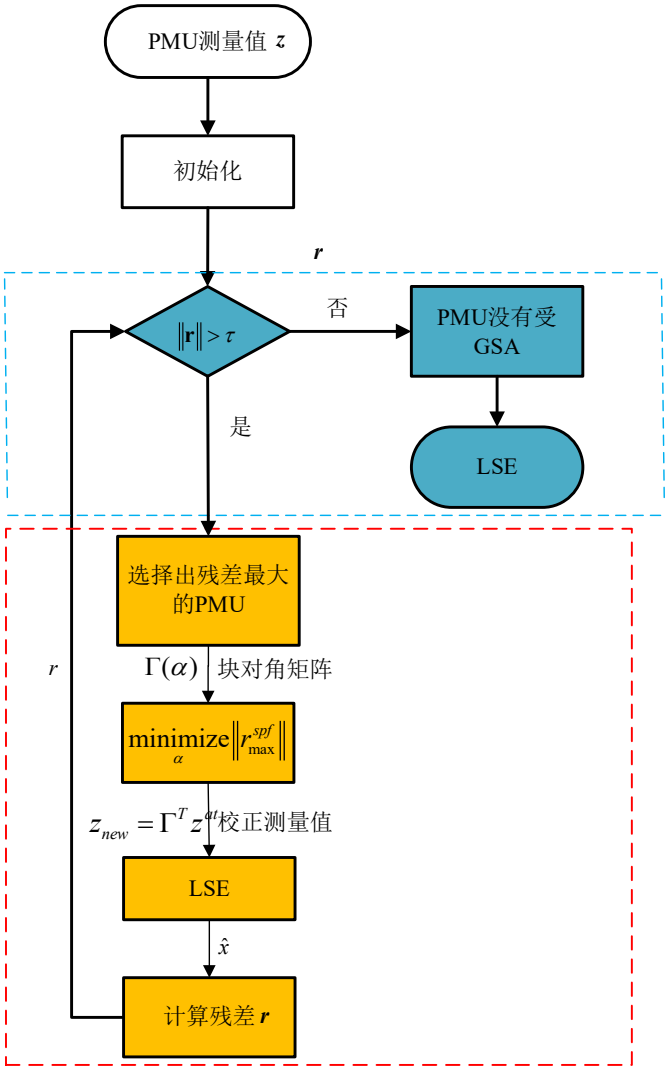


图 3-1 基于测量残差的 GPS 欺骗攻击检测和系统状态估计方法流程图

3.4 仿真结果与分析

3.4.1 仿真环境选择及参数设置

本节将针对上节所提出的 GSA 检测、数据校正和系统状态估计方法进行详细的数值实验，旨在全面验证所提方法的性能与可靠性。实验的仿真工作主要依托 IEEE-14 节点系统，IEEE-14 节点测试系统（如图 3-2 所示）是业界公认的、用于评估电力系统潮流计算和算法性能的标准系统。该系统基于 IEEE-14 标准节点参考模型构建，每个节点、每条线路以及每台发电器的数据都严格遵循 IEEE 标准的定义与规范，确保了测试环境的准确性和一致性。由于 IEEE-14 节点系统具有高度的代表性和通用性，它被广泛用于验证和比较各种潮流计算算法、优化算法以及其他电力系统分析方法。

在实验中，本章充分利用了 IEEE-14 节点系统的各项数据，模拟了多种电力系统运行状态，包括正常状态和各种潜在的 GSA 攻击场景。通过对这些场景进行仿真，可以全面评估所提方法在不同条件下的性能表现。同时，还采用了多种性能评价指标，如检测准确率、校正效果以及状态估计的精度等，以确保对方法性能的全面评估。此外，还特别关注了实验的可比性和通用性。通过使用 IEEE 标准测试系统作为基准，将本章提出的算法研究结果可以与其他研究进行直接比较，从而验证所提方法的优越和有效性。

现实生活中没有政府部门的许可欺骗攻击实验是不被允许进行的。以 GPS 信号频率传播任何信号都是违法的。此外，使用 PMU 和电网进行实际实验的成本很高。因此，本节使用 MATPOWER 进行模拟，它可以为 IEEE-14、IEEE-30 等测试节点网络生成稳态 PMU 测量值。此外，所建立的模型中不同网络创建导纳矩阵 所需的参数在 MATPOWER 中也可以被提供。模型测试的噪声协方差是一个对角矩阵，节点电压和线路电流的标准差均被设置为 0.01。

在模拟中，假设系统网络是可观察的。表 3-1 给出了不同测试场景下 PMU 的部署位置。对于安全场景下，通过执行潮流分析生成 PMU 稳态测量值，为了模拟欺骗环境，使用式(2-27)来修改安全的 PMU 测量值进而来模拟 GSA 发生的情况。

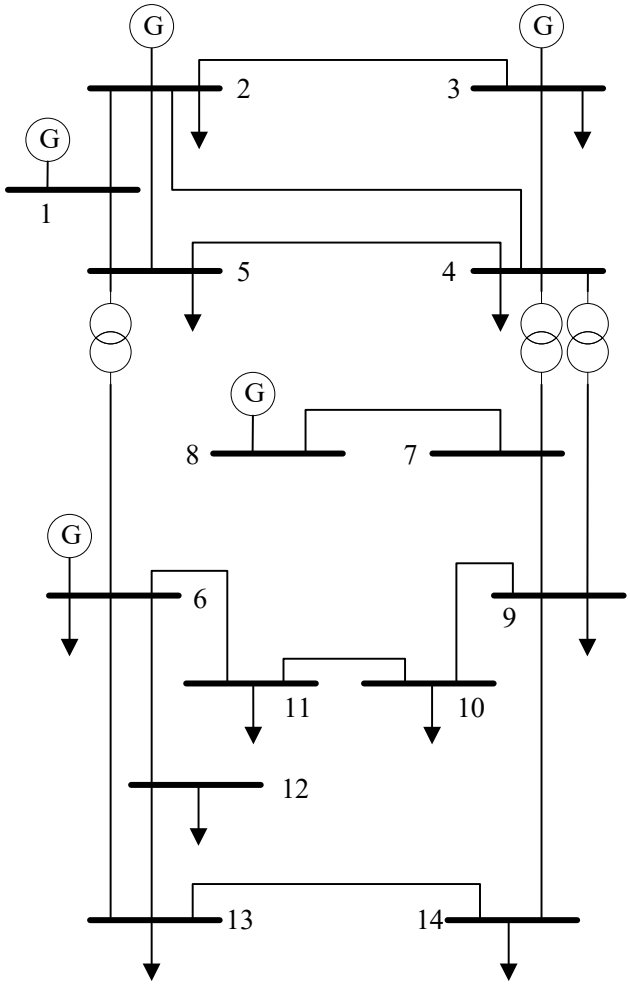


图 3-2 IEEE-14 节点标准系统拓扑结构

表 3-1 不同节点网络 PMU 的部署个数及位置情况

测试网络	PMU 部署个数	PMU 部置在节点的位置
IEEE-14	6	2，4，6，7，10，14
IEEE-30	12	1，3，5，9，10，12，18，24，25，27，28
IEEE-118	54	1，3，4，5，6，8，9，11，12，15，17，19，21，23，25，26，28，30，34，35，37，40，43，45，46，49，52，54，56，59，62，65，68，70，71，75，76，77，78，80，83，85，86,89，90，92，94，96 ，100，105，108，110，114

3.4.2 测量残差阈值ε的确定

在仿真环境及模型参数得到设定之后，就可以通过模拟安全和欺骗场景来精准地呈现 GSA 的发生。为了有效应对这种攻击，本章采用了基于测量残差的 GPS 欺骗攻击检测与系统状态估计算法。

在该算法中，测量残差扮演着至关重要的角色，它不仅是判断数据是否遭受攻击的关键依据，同时也是后续进行数据校正和系统状态估计的重要参考。具体来说，首先利用预设的阈值对测量残差进行筛选，以此区分数据是否被 GSA 攻击。这一阈值的选择并非随意，而是经过反复测试得出的。它关乎能否最大程度上将安全数据与不良数据进行有效分类，进而影响到后续数据校正的准确性和系统状态估计的精度。一旦阈值确定，便可以利用它来筛选出可能遭受 GSA 攻击的数据。对于这部分数据，将进一步分析其残差特性，以确认攻击的存在并评估其严重程度。随后，将根据攻击的特性采取相应的校正措施，以恢复数据的真实性并提高系统状态估计的精度。

对于阈值的确定，本仿真通过进行 2000 次蒙特卡罗模拟，全面考虑了安全和欺骗两种场景。在安全场景中，严格保持 PMU 测量值的原始性，未进行任何修改。在这些安全场景的模拟过程中，特别关注了静态估计中获得的测量残差，并记录下每一次模拟中的最高残差值以最大限度地保证安全数据和受攻击数据的区分度。模拟结果发现，在超过 2000 次的安全情景模拟中，估计达到这一最大残值的实例并不多，其发生率稳定在千分之二至千分之三之间。这一结果不仅验证了所设定阈值的合理性，更显示了其异常出色的鲁棒性。这意味着，在实际应用中，该阈值能够有效地抵御各种潜在的干扰和误差，准确地区分安全数据和受攻击的不良数据。

在模拟被攻击场景下，仿真过程是对 IEEE-14 节点网络上的 PMU 分别采用攻角为30°、45°、60°的攻击模型修改了节点 2 和节点 6 上的 PMU 的测量值来作为实验数据以模拟不同攻击强度下的情况。在每个蒙特卡罗模拟中，使用 LSE 估计系统状态并计算出数据的残差。

图 3-3 显示了不同模拟场景下的残差范数分布，图 3-3 中的结果清楚地表明，GSA 的存在导致 PMU 的测量残差增加，并且这种对于残差的偏移是非常明显，

在正常的安全条件下，系统的测量残差范数分布主要集中在 0.02 以下，这表明系统处于稳定状态，测量值与估计值之间的偏差较小。然而，在 GSA 攻击下，残差范数分布却发生了明显的偏移，达到了 0.12 左右，甚至有些偏移明显大于 0.12。这一显著的差异进一步证实了 GSA 对系统状态估计的破坏作用，也进一步验证了使用一组残差阈值来区分受攻击和未受攻击系统的可行性。

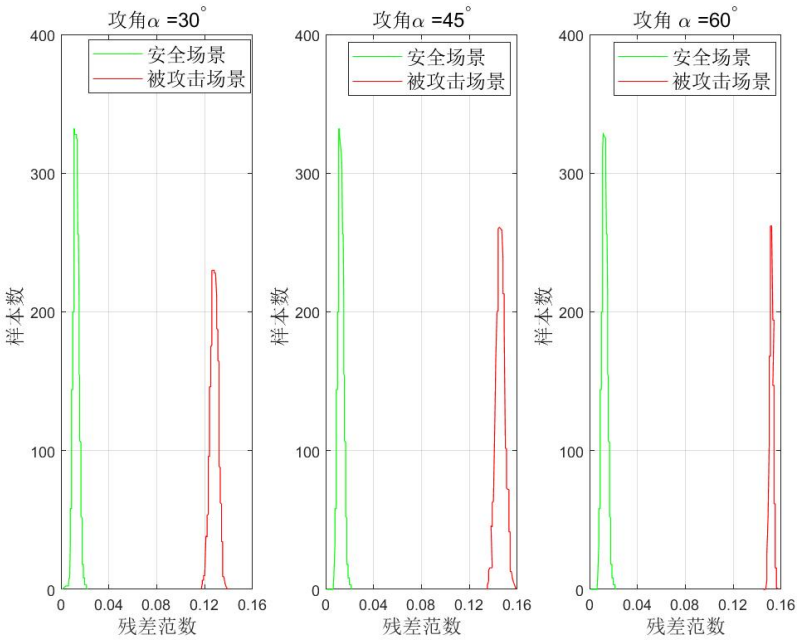


图 3-3 安全和被攻击场景下残差范数分布图

3.4.3 单个 GSA 下算法性能结果及分析

由于 GSA 的实施过程复杂且要求苛刻，它不仅需要专业的设备支持，还耗费大量的时间。更为复杂的是，电网的实际覆盖范围广阔，特别是在某些区域，相邻变电站之间的距离尤为遥远。这种地理分布上的特点，使得在多个位置或 PMU 上协同进行 GSA 变得异常困难。

因此，本仿真首先考虑系统上只有一个 PMU 受 GSA 的情况。对于单个 GSA，假设节点 2 上的 PMU 测量相位由于 GSA 而偏移 30°、60°。分别在图 3-4 和图 3-5 中记录了系统安全条件下以及这两种攻击产生相位偏移影响下系统中所有的 PMU 测量值。

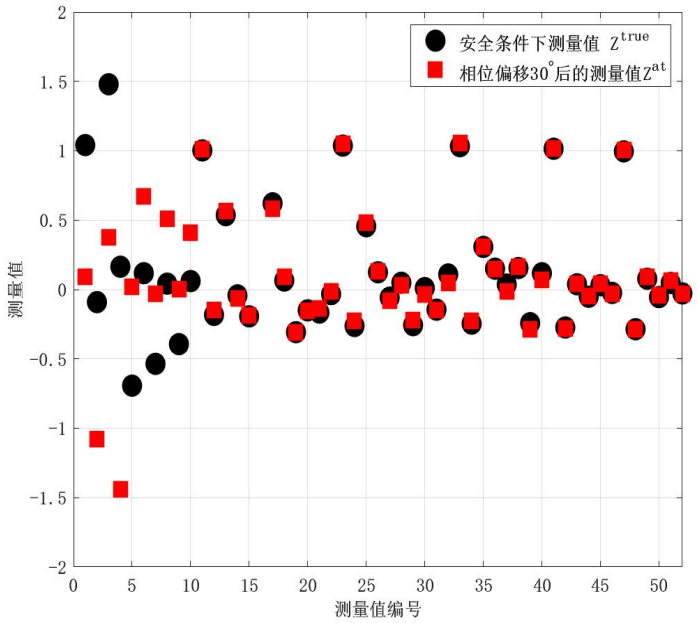


图 3-4 安全条件下和节点 2 上的 PMU 由于 GSA 产生 30° 相移后的系统测量

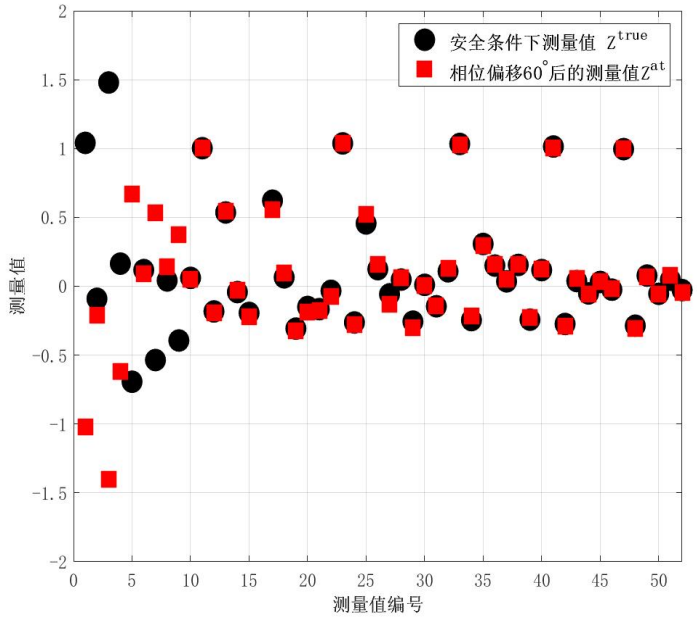


图 3-5 安全条件下和节点 2 上的 PMU 由于 GSA 产生 60° 相移后的系统测量

从图 3-4 和图 3-5 中，可以清晰地观察到 GSA 对电力系统状态估计的影响。当部署在节点 2 上的 PMU 遭受 GSA 攻击，其测量相位发生不同程度的偏移时，导致这些测量值显著偏离了真实值。这种偏差不仅影响了受攻击的 PMU 本身的测量准确性，而且通过电力系统的网络结构，对整体的系统状态估计结果产生了

恶化效应。另一方面，从有明显的偏差数据的位置以及对应的测量值编号，也可以准确的实现对于受到攻击的 PMU 的定位。这是因为受到攻击的 PMU 的测量值会表现出明显的异常，如测量值的突变或持续的偏移。这种异常模式可以便于迅速识别出受到攻击的 PMU，从而采取相应的措施进行防御和校正。同时该结果再一次验证了本文使用最大偏差范数阈值对一定范围内的安全和被攻击数据进行分类的合理性。

接下来，将采用所提出的算法对遭受 GSA 攻击下的测量值进行校正。校正的结果分别如图 3-6 和图 3-7 所示，从图 3-6 和图 3-7 中，可以清晰地看到算法对不良数据的强大校正能力。经过算法的精细处理，原本受到 GSA 攻击而偏离真实值的测量数据得到了显著的改善。校正后的测量值不仅消除了大部分的偏移，而且已经非常接近于真实值的水平。这一结果充分展示了算法在不良数据校正方面的有效性。为了进一步验证校正效果，计算了校正后的测量数据的总体残差范数。结果显示，残差范数保持在一个稳定的低水平。这一算法不仅能够准确识别并校正受到攻击的测量数据，还能够显著提升后续系统状态估计的有效值和数据冗余度。通过消除不良数据的影响，可以大大提高系统状态估计的精度和鲁棒性，为电力系统的安全稳定运行提供有力保障。

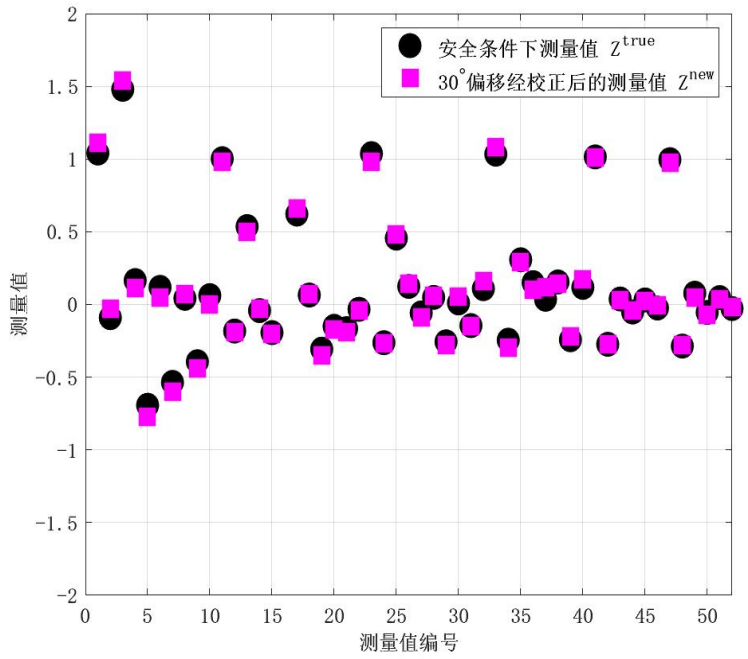


图 3-6 安全条件下和 30° 相移下测量值经校正算法后的系统测量

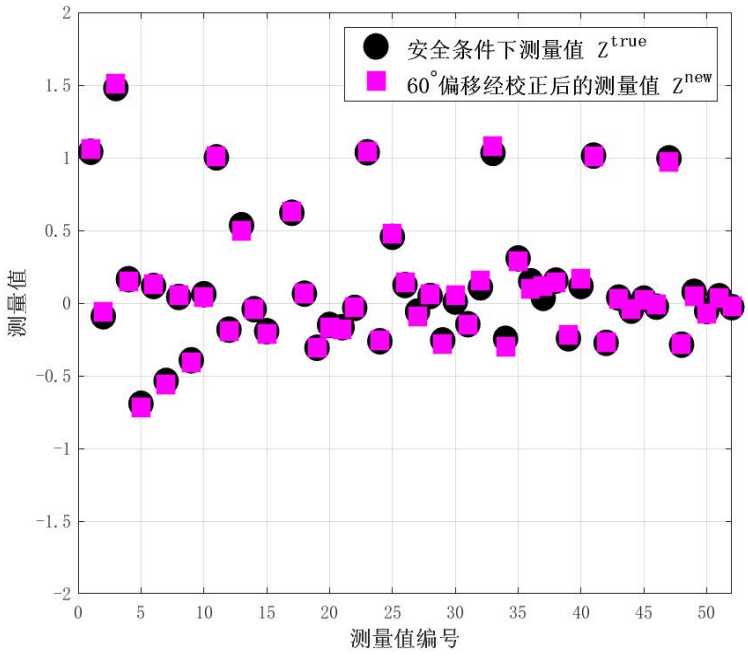


图 3-7 安全条件下和 60° 相移下测量值经校正算法后的系统测量

3.4.4 多个 GSA 下算法性能结果及分析

针对系统同时受到多个 GSA 影响的情况，在 IEEE-14 测试系统上进行了详尽的检测和校正实验。假设攻击者同时对部署在节点 2 和节点 7 上的 PMU 进行了欺骗攻击，意图通过篡改数据来干扰电力系统的正常运行。这种攻击导致节点 2 和节点 7 上的 PMU 测量相位分别发生了 45° 和 60° 的偏移。图 3-8 清晰地记录了系统在安全条件下以及这两个攻击同时发生时的 PMU 测量值。从图中可以明显看出，当系统受到多个 GSA 影响时，测量值相较于真实值发生了众多且显著的偏移。这些偏移不仅数量多，而且幅度大，严重恶化了状态估计的精度。

为了验证所提算法在应对多个 GSA 存在时的性能，将同时受到两个 GSA 影响的系统测量值输入到了所提的数据校正算法中。经过算法的处理，校正结果如图 3-9 所示。从图中可以看出，即使面对多个 GSA 的情况，所提的算法在校正测量值方面仍然展现出了出色的性能效果。校正后的测量值非常接近于真实值，几乎除了 GSA 攻击带来的影响。为了进一步验证校正效果，计算了校正后测量值的均方根误差（Root Mean Square Error，RMSE）。结果显示，RMSE 值保持在

0.015 以下，这充分说明了所提算法在应对多个 GSA 攻击时具有极高的校正精度和稳定性。

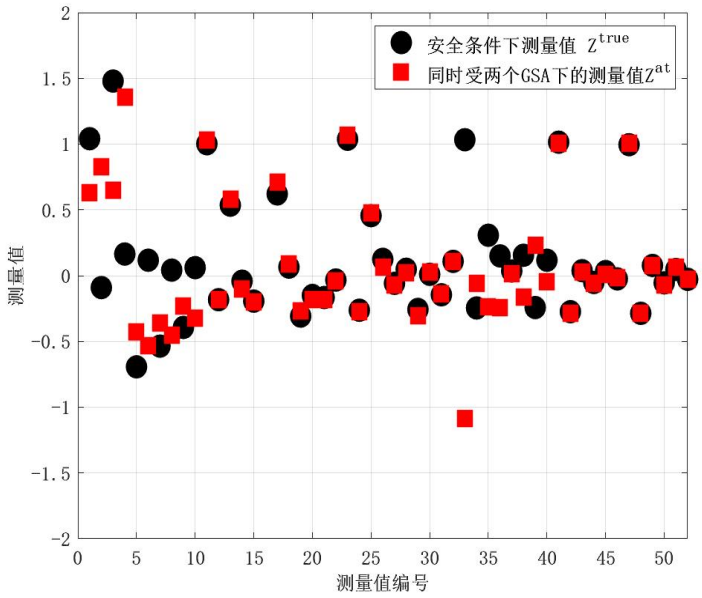


图 3-8 安全条件下和节点 2、节点 7 上 PMU 同时受两个 GSA 下的系统测量

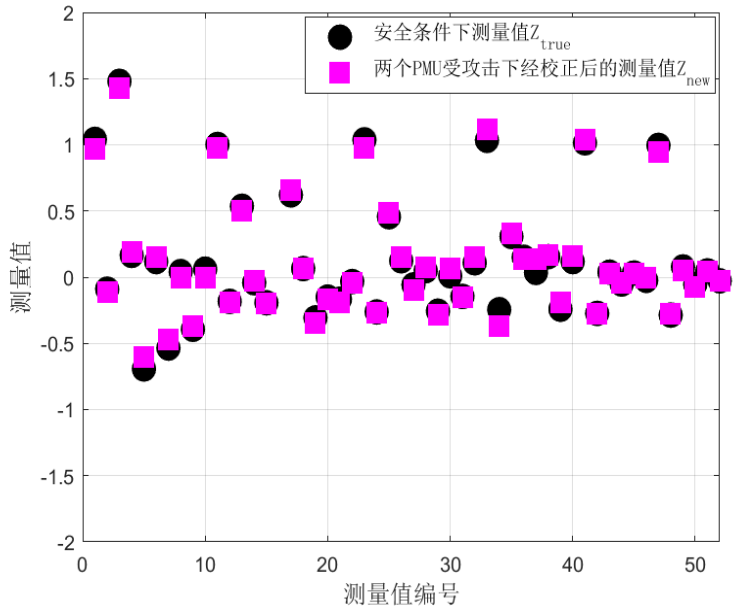


图 3-9 安全条件下和节点 2、节点 7 上 PMU 同时受两个 GSA 下经校正后的系统测量

此外，仿真还通过在 IEEE-14 节点系统中施加了 1-3 个 GSA 来研究算法在面对不同个数 GSA 攻击时的性能。仿真结果是使用多次校正的测量值进行状态

估计的 RMSE 的平均值作为性能指标，RMSE 定义为$\sqrt{\frac{1}{n}(x-\hat{x})}$，其中 n 表示数据样本数，表示$\hat{x}$估计值，$x$为实际值。仿真结果如图 3-10 所示。图 3-10 说明了在 IEEE-14 节点系统上进行不同 GSA 个数的测试时，所提的算法校正后测量值进行系统状态估计的总 RMSE 较低，并且随着 GSA 个数的增加，算法也具有较好的鲁棒性。即使系统中同时有 3 个 PMU 受到 GSA 的影响时，校正后的的测量值在进行状态估计的 RMSE 的均值也仍然低于 0.02。

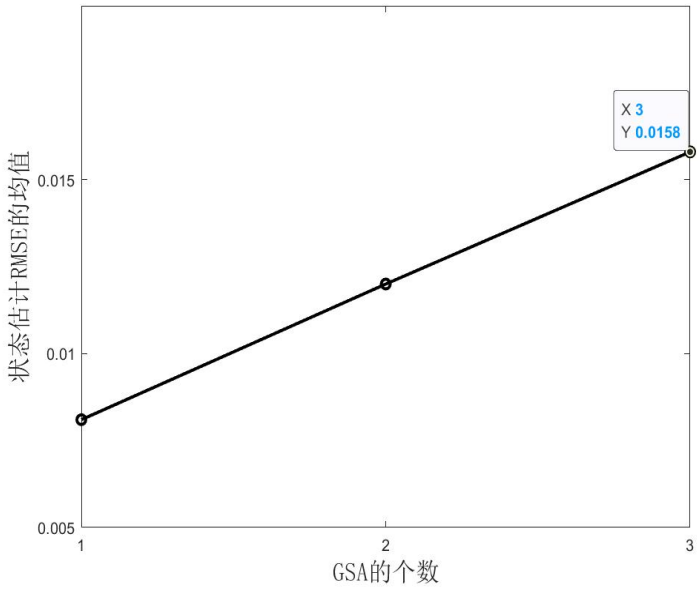


图 3-10 不同 GSA 下测量值校正后的系统状态估计的均方根误差均值

3.4.5 不同 GSA 下算法攻角估计结果及分析

在算法的校正过程中，首先也是重点的目标是通过最小化目标函数的方法估计出在系统受到攻击导致的相位偏移即攻角的大小，攻角估计的精准度关系着校正算法的好坏，关系着校正后的测量值与真实值的接近水平，进而影响着状态估计的精确度。因此，本节通过比较所提算法与传统算法在面对不同 GSA 时对于攻角的估计，来明确所提算法的性能表现。

为了全面评估所提算法的性能表现，本节设计了对比实验，将所提算法与传统算法在面对不同 GSA 攻击时对攻角的估计能力进行了深入比较。实验结果显示，相较于传统算法，所提算法在攻角估计方面展现出了更高的精度和稳定性。无论面对单一 GSA 攻击还是多个 GSA 同时作用的情况，所提算法都能更为准确

地估计出攻角的大小。

仿真实验分别在受到单个 GSA 和多个 GSA 的场景下进行。仿真结果被呈现在图 3-11 和图 3-12 中。在图 3-11 中，模拟了单个 GSA 导致 PMU 量测值相位偏移30°的场景。在这种情境下，所提算法展现出了良好的性能。它对于攻角30°的估计达到了29.43°的水平，充分证明了所提算法在单个 GSA 攻击下的高精度估计能力。相比之下，SpM 算法的估计偏差值达到了1.01°，而 AM 算法的偏差度更是接近1.45°，其性能明显逊色于所提算法。当面对更为复杂的多个 GSA 场景时，所提算法同样展现出了良好的性能。在图 3-12 中，模拟了两个 PMU 量测值分别受到45°和60°相位偏移的情况。在这种情境下，所提算法对于两个攻角的估计偏差分别仅为0.73°和0.86°。这一结果表明，即使在面对多个 GSA 攻击时，所提算法的估计精度也没有发生较大恶化，依然能够保持较高的准确性。这一特性使得所提算法在系统面临多个 GSA 威胁时能够发挥重要的作用，为电力系统的安全稳定运行提供有力的保障。

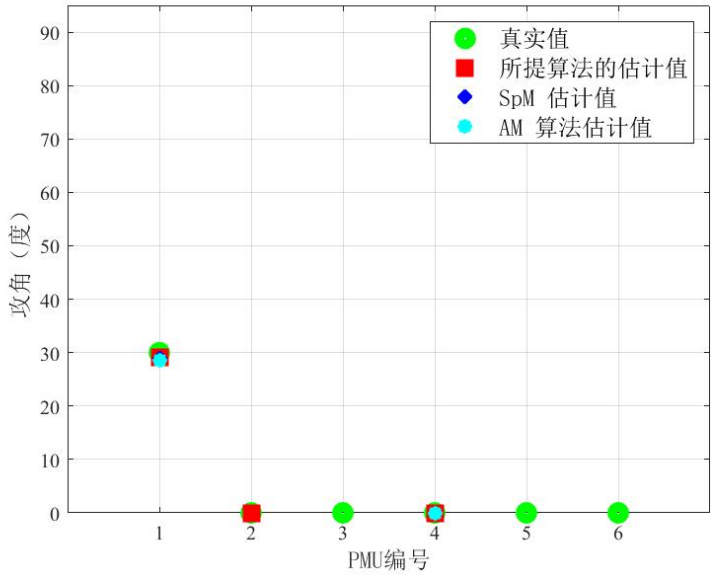


图 3-11 单个 PMU 受 GSA 攻击时不同算法对于攻角的估计与真实攻角的比较

另一方面，为了全面评估所提算法在更大规模网络中的适用性和性能表现，进一步在在 IEEE-14、IEEE-57 和 IEEE-118 这些不同规模的节点测试用例上进行实验以验证了所提算法在更广泛网络场景下的有效性和可靠性。为了确保实验的

准确性和全面性，采用了蒙特卡罗模拟方法，这种方法能够通过大量重复随机实验来评估算法的稳定性和性能。在模拟过程中，我们还考虑了不同数量的 GSA 攻击情况，从单一的 GSA 攻击到多达三个 GSA 同时作用，以模拟实际电力系统中可能遭遇的复杂攻击场景。

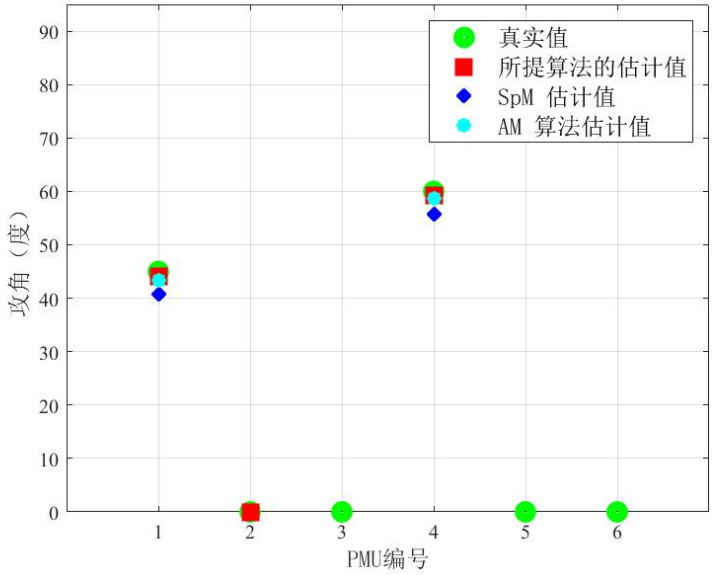


图 3-12 多个 PMU 受 GSA 攻击时不同算法对于攻角的估计与真实攻角的比较

对于每个 GSA 攻击情况，执行了 100 次蒙特卡罗模拟，以充分反映算法在各种随机条件下的性能表现。在每次模拟中，随机选择了一定数量的 PMU 节点作为攻击目标，并设定随机的攻击角度，以模拟 GSA 攻击的不确定性和随机性。实验结果表明，在无论是单一 GSA 攻击还是多个 GSA 同时作用的场景下，所提算法都展现出了良好的性能。如表 3-2 所示，从与 AM 算法和所提算法中获得的校正测量结果的 RMSE 对比中，可以清晰地看到，所提算法校正后的测量值的 RMSE 始终小于 AM 算法。这一结果充分证明了所提算法在更大规模网络中的适用性和性能优势，无论面对何种数量和强度的 GSA 攻击，它都能够有效地校正测量值，提高状态估计的精确度。

此外，为了全面评估所提算法在计算效率方面的表现，还针对 100 次蒙特卡罗模拟中两种算法的计算时间进行了详细的记录与对比。从表 3-2 中的数据可以明显看出，在所有测试用例中，所提算法的计算时间都显著小于 AM 算法，这充分展示了所提算法在计算效率上的优势。此外，由于所提算法采用了迭代估计的方式，其计算时间会随着 GSA 数量的增加而相应增长。然而从表 3-2 可以发现，

即使是在面对同时 3 个 GSA 攻击的场景时，所提算法在 IEEE-118 节点测试系统中的最大计算时间也仅为 0.0068 秒。这一极短的计算时间充分证明了所提算法在处理复杂攻击场景时的高效性，即使在大规模网络中也能够实现快速而准确的计算。更为重要的是，所有模拟试验都是在实时计算环境中进行的，这意味着所提算法不仅具有高效的计算能力，还能够满足实时监控系统对于数据处理速度的要求。这一特性使得所提算法在电力系统的实时监控中具有广泛的应用前景。

表 3-2 不同系统下所提算法与 AM 算法的计算时间及状态估计的 RMSE 结果的均值对比

测试系统	场景	所提算法状态估计 RMSE	所提算法计算时间（秒）	AM 算法状态估计 RMSE	AM 算法计算时间（秒）
IEEE-14	1 GSAs	0.0093	0.0294	0.0413	8.4909
	2 GSAs	0.0120	0.1144	0.0429	14.6323
	3 GSAs	0.0158	0.2830	0.0522	21.3417
IEEE-30	1 GSAs	0.0026	0.1426	0.0193	87.98559
	2 GSAs	0.0219	0.2421	0.0396	94.3241
	3 GSAs	0.0413	0.3029	0.0641	107.4123
IEEE-118	1 GSAs	0.0033	0.1487	0.0137	91.3233
	2 GSAs	0.0057	0.4023	0.0366	122.4132
	3 GSAs	0.0068	0.7011	0.0539	129.5605

3.5 本章小结

本章提出了一种用于检测和校正电力系统中 PMU GSA 引起的测量数据偏差的算法，并使用校正后的数据估计系统状态。通过对 IEEE-14 节点等系统的仿真测试，证明了该算法能够检测出受 GSA 攻击的 PMU 的位置，并且校正后的数据与原始实际测量值非常接近。校正后数据的系统状态估计的均方根误差也非常小，大大提高了估计精度。在广义仿真中，还发现该算法在规模更大的网络中也适用。这对于工程的上的应用具有实际意义。

第 4 章 基于 JMAP-ML 算法的 GPS 欺骗攻击检测和系统状态估计

4.1 引言

传统的对抗 GPS 欺骗攻击的方法通常采用基于同步相量数据的欺骗匹配算法，旨在将被篡改的数据还原为其原始状态。尽管此类方法在一定程度上具备一定的防御性，但其存在着诸多限制，如计算复杂度高、准确性不足，且对智能电网的基础设施要求较高。此外，这些传统的防御手段往往只针对特定类型的攻击有效，难以在攻击发生后迅速且有效地减轻其对智能电网的影响。相较之下，利用估计理论方法则能够进行数据预测，并利用其恢复篡改数据至原始状态，其预测准确性较高。本章针对此，本文研究了电力系统中未知 GSA 的安全状态估计和攻击检测问题。针对推导的 PMU 量测模型的公式化问题中，所涉及的未知参数是耦合的，目标函数是非凸的，这给寻找最优解带来了很大的挑战。为了解决这些问题，提出了一种联合最大后验和最大似然算法来安全地估计 PMU 混合测量中的状态变量和检测 GSA。

4.2 GPS 欺骗攻击下 PMU 测量的混合模型建立

第二章介绍了 PMU 部署运行在安全状态下的测量模型及其在节点受攻击后的测量。在现实中，系统从安装在节点 k 上的 PMU 获得测量值，而无法事先知道节点上的 PMU 是否受到攻击。所以可以将量测模型分为攻击场景和安全场景，以便更好地表示。因此，节点 k 的测量值 $\boldsymbol{z}$ 可表示为:

$$\boldsymbol{z}_k = \begin{cases} \boldsymbol{H}_k \boldsymbol{x} + \boldsymbol{e}_k & \alpha_k = 0 \\ \boldsymbol{\tau}_k \boldsymbol{H}_k \boldsymbol{x} + \boldsymbol{e}_k & \alpha_k \neq 0 \end{cases} \tag{4-1}$$

其中，$\boldsymbol{\tau}_k \in \mathbb{C}^{(2l+2)\times(2l+2)}$ 其取决于 α_k，$\boldsymbol{e}_k$ 服从高斯分布 $\boldsymbol{e}_k \sim \mathcal{N}(0, \boldsymbol{\Sigma})$。

在本章中，利用双模混合分布来表示 PMU 混合测量中的误差，从而简化了这个问题。双模混合分布可表示为

$$p(\boldsymbol{e}_k \mid \boldsymbol{\Sigma}) = \alpha_1 \mathcal{N}(\boldsymbol{z}_k - \boldsymbol{\tau}_k \boldsymbol{H}_k \boldsymbol{x} \mid \boldsymbol{\Sigma}) + \alpha_2 \mathcal{N}(\boldsymbol{z}_k - \boldsymbol{H}_k \boldsymbol{x} \mid \boldsymbol{\Sigma}) \tag{4-2}$$

其中，2 表示混合测量的种类数，即安全测量和受攻击测量，其对应的权重 α_l 必须满足一个概率条件，即

$$\sum_{l=1}^{2}\alpha_l = 1, \alpha_l \geq 0 \tag{4-3}$$

其中，α_l 为未知参数，表示各组分的比例。假设 M 个 PMU 中有 S 个受到攻击导致相位角发生偏移。那么 $\alpha_1 = S/M$ ， $\alpha_2 = (M-S)/M$ 。各部分分布由对应的均值 0 和方差 $\boldsymbol{\Sigma}$ 决定。双模混合分布的主要挑战是估计每个部分分布的单个参数 $\boldsymbol{\theta}_m = [\alpha_1, \alpha_2, \boldsymbol{\Sigma}^T]^T$ ，针对该模型特点可以应用 JMAP-ML 准则来实现这一目标。

4.3 联合最大后验和最大似然算法和系统状态估计

4.3.1 基于联合最大后验和最大似然算法的参数估计

基于式(4-1)的量测模型和式(4-2)的双模混合分布，未知参数 $\theta = [\alpha_1, \alpha_2, \boldsymbol{\Sigma}^T, \boldsymbol{\Gamma}^T]^T$ （其中 $\boldsymbol{\Gamma} = [\boldsymbol{\tau}, \boldsymbol{x}]^T$ ）的对数似然函数为

$$\begin{aligned} \mathcal{J}_I(\boldsymbol{\theta};\boldsymbol{e}) &= \ln(p(\boldsymbol{e};\boldsymbol{\theta})) \\ &= \sum_{k=1}^{M}\left(\ln(\alpha_1 \mathcal{N}(\boldsymbol{z}_k - \boldsymbol{\tau}_k \boldsymbol{H}_k \boldsymbol{x} \mid \boldsymbol{\Sigma}) + \alpha_2 \mathcal{N}(\boldsymbol{z}_k - \boldsymbol{H}_k \boldsymbol{x} \mid \boldsymbol{\Sigma}))\right) \end{aligned} \tag{4-4}$$

通过求解下式可以得到对数似然函数的参数 $\boldsymbol{\theta}$ 最大似然估计 $\hat{\boldsymbol{\theta}}_{\mathrm{ML}}$ 。

$$\begin{cases} \arg\max\limits_{\boldsymbol{\theta}} \quad \mathcal{J}_I(\theta;e) \\ \text{s.t.} \ \sum\limits_{l=1}^{2}\alpha_l = 1 \\ \alpha_l \geq 1 \end{cases} \tag{4-5}$$

式(4-4)中的代价函数过于复杂而难以求解。这里引入了一个隐变量 $\boldsymbol{v}$ 来表示数据属于哪一类别，从而可以大大降低最大似然估计的计算复杂度。$\boldsymbol{v}$ 被表示为

$$\boldsymbol{v} = \begin{bmatrix} \boldsymbol{v}_{11} & \cdots & \boldsymbol{v}_{k1} & \cdots & \boldsymbol{v}_{M1} \\ \boldsymbol{v}_{12} & \cdots & \boldsymbol{v}_{k2} & \cdots & \boldsymbol{v}_{M2} \end{bmatrix}^T \tag{4-6}$$

隐变量 $\boldsymbol{v}$ 中包含 $2M$ 个潜在变量，其值表示测量误差 $\boldsymbol{e}_k$ 的误差分布。其中，

$\boldsymbol{v}_k$ 的表示第 k 个测量的误差指标，定义为

$$\boldsymbol{v}_k=(\boldsymbol{v}_{k1},\boldsymbol{v}_{k2})=\begin{cases}(1,0) & k\in M_a\\(0,1) & k\in M_b\end{cases} \tag{4-7}$$

其中，$|M_a|=S$，$|M_{\mathrm{b}}|=M-S$。

在引入隐藏变量后，完整数据的对数似然函数可以很容易地表示为

$$\begin{aligned}\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{e})&=\ln[p(\boldsymbol{v},\boldsymbol{e};\boldsymbol{\theta})]\\&=\ln\left(\prod_{k=1}^{M}p(\boldsymbol{v}_k,\boldsymbol{e}_k;\boldsymbol{\theta})\right)\\&=\ln\left(\prod_{k=1}^{M}[\alpha_1\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})^{\nu_{k1}}+\alpha_2\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})^{\nu_{k2}}]\right)\\&=\sum_{k=1}^{M}\ln\left([\alpha_1\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})^{\nu_{k1}}+\alpha_2\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})^{\nu_{k2}}]\right)\end{aligned} \tag{4-8}$$

为避免歧义，将原始对数似然函数(4-4)中的 $\mathcal{J}_I(\boldsymbol{\theta};\boldsymbol{e})$ 称为不完全数据对数似然函数。引入隐藏变量的对数似然函数 $\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{e})$ 称为完整数据。那么对于式(4-5)的求解就变为

$$\begin{cases}\arg\max\limits_{\boldsymbol{\theta}} & \mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{e})\\ \text{s.t.} & \sum\limits_{l=1}^{2}\alpha_l=1\\ & \alpha_l\geq 1\end{cases} \tag{4-9}$$

联合最大后验和最大似然方法是对最大化似然估计的近似值，并直接针对未知参数 $\boldsymbol{\theta}$ 和 $\boldsymbol{v}$ 进行最大化操作。此近似问题可以表述为

$$\arg\max_{\boldsymbol{\theta},\boldsymbol{v}}\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{e})=\arg\max_{\boldsymbol{\theta}}\left\{\arg\max_{\boldsymbol{v}}\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{e})\right\}. \tag{4-10}$$

综上所述，联合最大化后验和最大化似然算法是一个包含最大化后验和最大似然这两个标准的迭代算法。

4.3.2 最大后验步骤

在最大后验步骤中，主要完成的是对于参数 $\boldsymbol{v}$ 的估计。首先把似然函数变化成

$$\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{e}) = \ln p(\boldsymbol{v},\boldsymbol{e};\boldsymbol{\theta}) = \ln p(\boldsymbol{v}\,|\,\boldsymbol{e};\boldsymbol{\theta}) + \ln p(\boldsymbol{e};\boldsymbol{\theta}) \tag{4-11}$$

其中，$\ln p(\boldsymbol{e};\boldsymbol{\theta})$ 是独立于隐藏变量 $\boldsymbol{v}$ 的概率函数，因此，式(4-11)的最大化可以用式(4-12)概率函数的最大化替代。

$$\arg\max_{\boldsymbol{v}} \quad \ln p(\boldsymbol{v}\,|\,\boldsymbol{e};\boldsymbol{\theta}) \tag{4-12}$$

通过将 η 次的迭代结果 $\boldsymbol{\theta}^{(\eta)}$ 代替 $\boldsymbol{\theta}$，隐藏变量 $\boldsymbol{v}$ 的最大后验估计可以被重新表述为

$$\boldsymbol{v}^{(\eta+1)} = \arg\max_{\boldsymbol{v}} \quad \ln p(\boldsymbol{v}\,|\,\boldsymbol{e};\boldsymbol{\theta}^{(\eta)}) \tag{4-13}$$

其中，$p(\boldsymbol{v}\,|\,\boldsymbol{e};\boldsymbol{\theta}^{(\eta)})$ 被定义为

$$p(\boldsymbol{v}_k\,|\,\boldsymbol{e};\boldsymbol{\theta}^{(\eta)}) = \frac{\alpha_1\mathcal{N}(\boldsymbol{z}_k - \boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma}) + \alpha_2\mathcal{N}(\boldsymbol{z}_k - \boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})}{p(\boldsymbol{e};\boldsymbol{\theta}^{(\eta)})} \tag{4-14}$$

$p(\boldsymbol{e};\boldsymbol{\theta}^{(\eta)})$ 的概率表达式为

$$\ln p(\boldsymbol{e};\boldsymbol{\theta}^{(\eta)}) = \sum_{k=1}^{M} \ln\left(\alpha_1\mathcal{N}(\boldsymbol{z}_k - \boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma}^{(\eta)}) + \alpha_2\mathcal{N}(\boldsymbol{z}_k - \boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma}^{(\eta)})\right) \tag{4-15}$$

因此，式(4-13)的最大后验估计可以被重新表述为

$$v_{kl}^{(\eta+1)} = \arg\max_{\boldsymbol{v}_{kl}} \ln\left(\alpha_1\mathcal{N}(\boldsymbol{z}_k - \boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma}^{(\eta)}) + \alpha_2\mathcal{N}(\boldsymbol{z}_k - \boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma}^{(\eta)})\right) \tag{4-16}$$

通过定义

$$\gamma_{kl}^{(\eta)} = \ln\left(\alpha_1^{(\eta)}\mathcal{N}(\boldsymbol{z}_k - \boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma}^{(\eta)}) + \alpha_2^{(\eta)}\mathcal{N}(\boldsymbol{z}_k - \boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma}^{(\eta)})\right) \tag{4-17}$$

那么，最后的最大后验估计即对于 v_{kl} 的估计可以描述为

$$v_{kl}^{(\eta+1)} = \begin{cases} 1 & \gamma_{kl}^{(\eta)} = \max\{\gamma_k^{(\eta)}\} \\ 0 & otherwise \end{cases} \tag{4-18}$$

综上所述，完成了最大化后验估计的关键步骤。在这一过程中，充分发挥了后验概率的优势，实现了对安全和受到攻击的不良数据的精准分类。同时，利用数据的对应关系，进一步完成了对受攻击 PMU 的精准定位。这一步骤至关重要，它能够帮助迅速锁定受到攻击的具体节点，为后续的防御和应对措施提供了明确的目标。在定位到不良数据后，紧接着展开了数据处理的关键环节。在这一阶段，采用了最大似然估计的方法，通过不断优化数据模型，使得处理后的数据更加接

近真实情况。

4.3.3 最大似然步骤

在最大似然步骤中，主要完成对于参数$\boldsymbol{\theta}$的估计，通过将$\nu_{kl}^{(\eta+1)}$代入完全对数似然函数$\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{e})$得到新的对数似然函数为

$$\begin{aligned}\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v}^{(\eta+1)},\boldsymbol{e}) &= \sum_{k=1}^{M}\ln\left(\alpha_1\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})+\alpha_2\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})\right)\\ &= \underbrace{\sum_{k=1}^{M}\left(\nu_{k1}^{(\eta)}\ln\alpha_1+\nu_{k2}^{(\eta)}\ln\alpha_2\right)}_{\mathcal{J}_{c1}^{(\eta)}(\alpha_1,\alpha_2)}\\ &\quad+\underbrace{\sum_{k=1}^{M}\left(\nu_{k1}^{(\eta)}\ln\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})+\nu_{k2}^{(\eta)}\ln\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{H}_k\boldsymbol{x}\,|\,\boldsymbol{\Sigma})\right)}_{\mathcal{J}_{c2}^{(\eta)}(\boldsymbol{\Sigma},e)}\end{aligned} \tag{4-19}$$

所以，可以得到参数$\boldsymbol{\theta}$的第$(\eta+1)$次迭代估计为

$$\boldsymbol{\theta}^{(\eta+1)}=\arg\max_{\boldsymbol{\theta}}\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v}^{(\eta+1)},\boldsymbol{e}) \tag{4-20}$$

根据文献[60]中的技术路线，可以得到以下拉格朗日方程

$$\frac{\partial}{\partial\alpha_l}\left[\mathcal{J}_{C1}^{(\eta)}(\alpha_1,\alpha_2)+\lambda\left(\sum_{l=1}^{2}\alpha_l-1\right)\right]=0 \tag{4-21}$$

其中，λ是拉格朗日算子，

$$\frac{\partial}{\partial\boldsymbol{\Sigma}}\left[\mathcal{J}_{C2}^{(\eta)}(\boldsymbol{\Sigma},\tau^{(\eta)},\boldsymbol{x}^{(\eta)})\right]=0 \tag{4-22}$$

通过求解式(4-21)和式(4-22)，参数α_l和$\boldsymbol{\Sigma}$的估计可以由式(4-23)和式(4-24)所示。

$$\alpha_l^{(\eta+1)}=\frac{1}{M}\sum_{k=1}^{M}\nu_{kl}^{(\eta)} \tag{4-23}$$

$$\boldsymbol{\Sigma}^{(\eta+1)}=\frac{\sum_{k=1}^{M}\left(\nu_{k1}^{(\eta)}(\boldsymbol{z}_k-\boldsymbol{\tau}_k^{(\eta)}\boldsymbol{H}_k\boldsymbol{x}^{(\eta)})^T(\boldsymbol{z}_k-\boldsymbol{\tau}_k^{(\eta)}\boldsymbol{H}_k\boldsymbol{x}^{(\eta)})+\nu_{k2}^{(\eta)}(\boldsymbol{z}_k-\boldsymbol{H}_k\boldsymbol{x}^{(\eta)})^T(\boldsymbol{z}_k-\boldsymbol{H}_k\boldsymbol{x}^{(\eta)})\right)}{M} \tag{4-24}$$

接下来，可以通过式(4-23)和式(4-24)更新参数变量$\boldsymbol{\Gamma}=[\boldsymbol{\tau},\boldsymbol{x}]^T$。

$$\boldsymbol{\tau}^{(\eta+1)}=\arg\max_{\boldsymbol{\tau}}\mathcal{J}_{C2}^{(\eta)}(\boldsymbol{\Sigma}^{(\eta+1)},\boldsymbol{\tau}) \tag{4-25}$$

$$\boldsymbol{x}^{(\eta+1)}=\arg\max_{\boldsymbol{x}}\mathcal{J}_{C2}^{(\eta)}(\boldsymbol{\Sigma}^{(\eta+1)},\boldsymbol{x}) \tag{4-26}$$

对式(4-25)和式(4-26)的未知变量求导并令其为零，可得到式(4-27)和式(4-28)所示的关于 $\boldsymbol{\tau}$ 和 $\boldsymbol{x}$ 的表达式。进而完成了对于系统的安全状态估计。

$$\boldsymbol{\tau}^{(\eta+1)}=\frac{\sum_{k=1}^{M}\boldsymbol{z}_k}{\sum_{k=1}^{M}\left(\boldsymbol{H}_k\boldsymbol{x}^{(\eta+1)}\right)} \tag{4-27}$$

$$\boldsymbol{x}^{(\eta+1)}=\frac{\sum_{k=1}^{M}\left(\nu_{k1}^{(\eta)}(\boldsymbol{\tau}_k^{(\eta+1)}\boldsymbol{H}_k)^T\boldsymbol{\Sigma}^{(\eta+1)}\boldsymbol{z}_k+\nu_{k2}^{(\eta)}\boldsymbol{H}_k^T\boldsymbol{\Sigma}^{(\eta+1)}\boldsymbol{z}_k\right)}{\sum_{k=1}^{M}\left(\nu_{k1}^{(\eta)}(\boldsymbol{\tau}_k^{(\eta+1)}\boldsymbol{H}_k)^T\boldsymbol{\Sigma}^{(\eta+1)}\boldsymbol{\tau}_k^{(\eta+1)}\boldsymbol{H}_k+\nu_{k2}^{(\eta)}\boldsymbol{H}_k^T\boldsymbol{\Sigma}^{(\eta+1)}\boldsymbol{H}_k\right)} \tag{4-28}$$

基于上面所述的算法的迭代估计过程，可以归纳出来对于 GPS 欺骗攻击中参数的联合最大后验和最大似然估计的算法流程如表 4-1 所示。

表 4-1 基于 JMAP-ML 算法的状态估计和 GSA 检测

步骤	流程
1.	输入：PMU 的量测数据 $\boldsymbol{z}$
2.	初始化：设置算法收敛阈值 ε_x=10^{-6}、最大迭代次数 $N_{itr}^{\max}$、初始估计 $\hat{\boldsymbol{\theta}}^{(0)}=(\boldsymbol{\theta}_m^{(0)},\boldsymbol{\tau}^{(0)},\boldsymbol{x}^{(0)})$ 和迭代指数 $\eta=0$
3.	**while** $\mathcal{J}_C^{(\eta)}(\boldsymbol{\theta}^{(\eta+1)};\boldsymbol{v}^{(\eta+1)},\boldsymbol{e})-\mathcal{J}_C^{(\eta)}(\boldsymbol{\theta}^{(\eta)};\boldsymbol{v}^{(\eta)},\boldsymbol{e})\mid>\varepsilon$ **or** $N_{itr}<N_{itr}^{\max}$ **do**
4.	$\eta=\eta+1$
5.	计算 ν_{kl}：$\nu_{kl}^{(\eta+1)}=\arg\max_{\boldsymbol{v}_{kl}}\ln\left(\alpha_1\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{\tau}_k\boldsymbol{H}_k\boldsymbol{x}\mid\boldsymbol{\Sigma}^{(\eta)})+\alpha_2\mathcal{N}(\boldsymbol{z}_k-\boldsymbol{H}_k\boldsymbol{x}\mid\boldsymbol{\Sigma}^{(\eta)})\right)$
6.	更新 $\boldsymbol{\theta}_m^{(\eta+1)}$：$\arg\max_{\boldsymbol{\theta}_m}\mathcal{J}_C^{(\eta)}(\boldsymbol{\theta}_m,\boldsymbol{v}^{(\eta+1)},\boldsymbol{\tau}^{(\eta)},\boldsymbol{x}^{(\eta)};\boldsymbol{e})$
7.	更新 $\boldsymbol{\Gamma}^{(\eta+1)}=[\boldsymbol{\tau}^{(\eta+1)},\boldsymbol{x}^{(\eta+1)}]^T$：$\arg\max_{\boldsymbol{\tau}/\boldsymbol{x}}\mathcal{J}_C^{(\eta)}(\boldsymbol{\theta}_m^{(\eta+1)},\boldsymbol{\tau},\boldsymbol{x};\ \boldsymbol{e})$
8.	**end while**
9.	输出：$\boldsymbol{\tau}$、$\hat{\boldsymbol{x}}$

4.4 算法收敛性分析

从上一小节的分析过程中知道 JMAP-ML 算法是一个迭代算法。因此，算法最终能否收敛也是一个有必要讨论的问题。针对这个问题，作了如下的分析。

本章提出的算法收敛性是指 JMAP-ML 算法单调收敛于完整数据对数似然函数 $\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{\Gamma})$ 的某个点 $\mathcal{J}^*$。在 JMAP-ML 算法的第一步，对于给定的先验参数估计 $\boldsymbol{\theta}^{(\eta)}$ 使得 $\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{\Gamma})$ 相对于 $\boldsymbol{v}$ 最大化，因为 $\boldsymbol{v}^{(\eta+1)}$ 是全局最优解，所以可以保证下式对于任何情况下的参数估计都是成立的，即

$$\mathcal{J}_C(\boldsymbol{\theta}^{(\eta)};\boldsymbol{v}^{(\eta+1)},\boldsymbol{\Gamma}) \geq \mathcal{J}_C(\boldsymbol{\theta}^{(\eta)};\boldsymbol{v}^{(\eta)},\boldsymbol{\Gamma}) \tag{4-29}$$

在第二步中，相对于未知参数矩阵 $\boldsymbol{\theta}$ 最大化似然函数 $\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v}^{(\eta+1)},\boldsymbol{\Gamma})$。这里，借助类似于期望最大化（Expectation Maximization，EM）算法中的 Q 函数的思想，假设

$$Q(\boldsymbol{\theta};\boldsymbol{\theta}^{(\eta)}) = \sum_{\boldsymbol{v}} \ln(p(\boldsymbol{v},\boldsymbol{e};\boldsymbol{\theta}))\cdot p(\boldsymbol{v}\,|\,\boldsymbol{e};\boldsymbol{\theta}^{(\eta)}) \tag{4-30}$$

接下来先证明对于任何 $\boldsymbol{\theta}^{(\eta)}$ 参数空间下，都有下式成立。

$$Q(\theta^{(\eta+1)};\theta^{(\eta)}) \geq Q(\theta^{(\eta)};\theta^{(\eta)}) \tag{4-31}$$

证明：

对于一个给定的先验参数 $\boldsymbol{\Gamma}^{(\eta)}$，文献[61]和[62]证明了高斯分布更新后的估计 $\boldsymbol{\alpha}_1^{(\eta+1)},\boldsymbol{\alpha}_2^{(\eta+1)},\boldsymbol{\mu}_1^{(\eta+1)},\boldsymbol{\sigma}_1^{2,(\eta+1)},\boldsymbol{\mu}_2^{(\eta+1)}$ 和 $\boldsymbol{\sigma}_2^{2,(\eta+1)}$ 是相应最大化问题的全局最优解。因此，由此结论可以得到

$$Q(\boldsymbol{\theta}_m^{(\eta+1)},\boldsymbol{\Gamma}^{(\eta)};\boldsymbol{\theta}^{(\eta)}) \geq Q(\boldsymbol{\theta}_m^{(\eta)},\boldsymbol{\Gamma}^{(\eta)};\boldsymbol{\theta}^{(\eta)}) \tag{4-32}$$

上式的右侧即 $Q(\boldsymbol{\theta}^{(\eta)};\boldsymbol{\theta}^{(\eta)})$。

下一步，通过最小化下面的 g 函数求出一个新的估计 $\boldsymbol{\Gamma}^{(\eta+1)}$，其中给定的先验参数 $\boldsymbol{\Gamma}^{(\eta)}$ 是通过拟牛顿法得到的。

$$g(\boldsymbol{\tau},\boldsymbol{x}) = \sum_{i=1}^{M}\sum_{l=1}^{2} \frac{(\boldsymbol{z}_i - \boldsymbol{\tau}_i\boldsymbol{H}_i\boldsymbol{x} - \boldsymbol{\mu}_l^{(\eta+1)})^2}{\boldsymbol{\Sigma}_l^{(\eta+1)}}\cdot \boldsymbol{v}_{il}^{(\eta)} \tag{4-33}$$

通过拟牛顿法得到的先验估计 $\boldsymbol{\Gamma}^{(\eta)}$ 保证了在每个牛顿步中向局部最小值的下坡步进，因此在第 $(\eta+1)$ 步迭代中，新的估计 $\boldsymbol{\Gamma}^{(\eta+1)}$ 不会再使 $Q(\boldsymbol{\theta}^{(\eta)};\boldsymbol{\theta}^{(\eta)})$ 减小，即

$$Q(\boldsymbol{\theta}_m^{(\eta+1)},\boldsymbol{\Gamma}^{(\eta+1)};\boldsymbol{\theta}^{(\eta)}) \geq Q(\boldsymbol{\theta}_m^{(\eta+1)},\boldsymbol{\Gamma}^{(\eta)};\boldsymbol{\theta}^{(\eta)}) \tag{4-34}$$

上式的左边即是 $Q(\boldsymbol{\theta}^{(\eta+1)};\boldsymbol{\theta}^{(\eta)})$。因此，式(4-31)可以被证明。

有了式(4-31)，可以即可得到

$$\mathcal{J}_C(\boldsymbol{\theta}^{(\eta+1)};\boldsymbol{v}^{(\eta+1)},\boldsymbol{\Gamma}) \geq \mathcal{J}_C(\boldsymbol{\theta}^{(\eta)};\boldsymbol{v}^{(\eta+1)},\boldsymbol{\Gamma}) \tag{4-35}$$

式(4-35)说明 $\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{\Gamma})$ 的值在迭代过程中式单调递增的，又由于 $\mathcal{J}_C(\boldsymbol{\theta};\boldsymbol{v},\boldsymbol{\Gamma})$ 函数是有界的，由单调有界定理，可以保证其收敛到某个不动点 $\mathcal{J}^*$。

4.5 仿真结果与分析

4.5.1 仿真参数设置及性能评估指标

在本节中，将执行数值测试来评估第三节中描述的欺骗攻击检测和系统状态估计方法的性能。以 IEEE-14 节点电网系统为例，进行了不同场景下的仿真。表 4-2 提供了整个仿真过程中使用的模拟参数的汇总。

表 4-2 算法过程的仿真参数

参数	数值
α_1	0.5
α_2	0.5
u_1	0
u_2	0.0217
ε	10^{-6}
$N_{itr}^{\max}$	50

此外，在仿真过程中还指定了一些性能指标。具体表示如下

1）假设 PMU 安装在 IEEE-14 节点系统的节点 2、4、6、7、9 和 13 上，PMU 编号顺序规定为从 1 到 6。

2）使用均方根误差（RMSE）作为度量算法性能的指标。RMSE 定义为

$\sqrt{\frac{1}{n}(\hat{x}-x)^2}$，其中$n$表示数据样本数，$\hat{x}$表示估计值，$x$表示实际值。

3) 相对状态估计误差可以定义为$\frac{\|\hat{\boldsymbol{x}}-\boldsymbol{x}\|_2}{\|\boldsymbol{x}\|_2}$，其中$\hat{\boldsymbol{x}}$表示算法估计的状态向量，$\boldsymbol{x}$表示状态的实际值。

4.5.2 不同 GSA 下算法的系统状态估计性能结果及对比分析

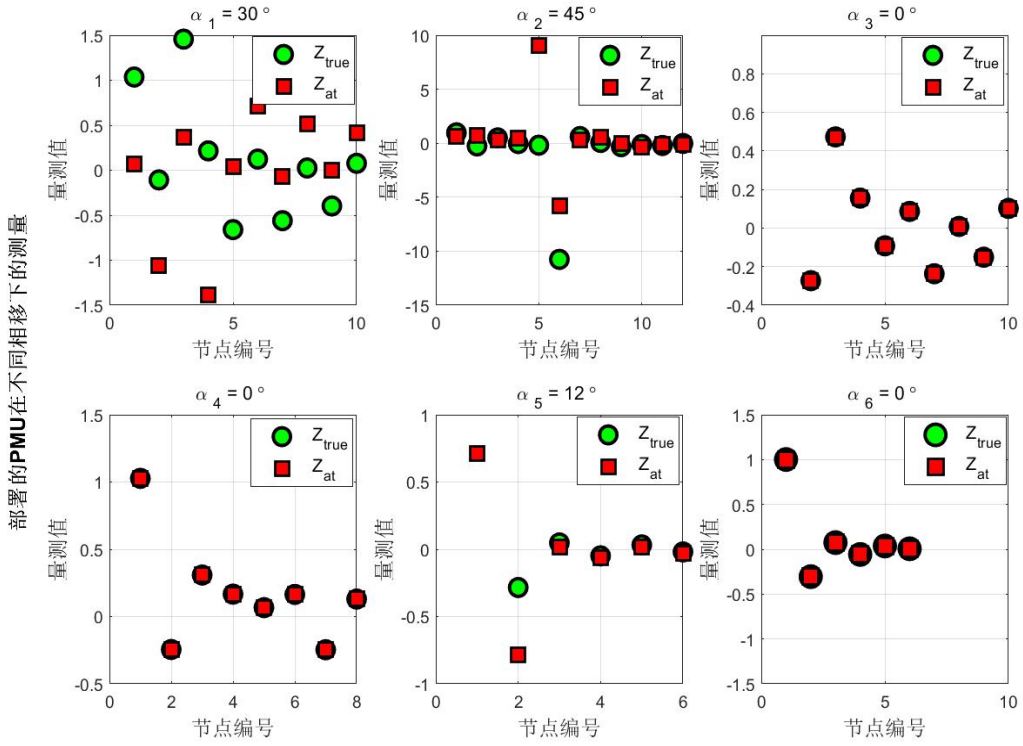


图 4-1 系统所部署 PMU 发生不同相位偏移时的 PMU 量测值

在场景 1 中，首先考虑一个只有一个 PMU 受到 GSA 影响的系统。仿真使得 PMU-2 受到恒定的相移攻击，即$\alpha_2 = 45^{\circ}$。假设这些 PMU 的测量标准差为 0.01，可以得到 PMU-2 受到攻击后的测量值和实际值，如图 4-1 所示。

从图 4-1 可以看出，当 PMU-2 受到 GSA 攻击时，测量值明显偏离真实值，足以降低状态估计结果。这也表明 GSA 产生的相移最终改变了 PMU 的测量。图 4-2 和图 4-3 显示了在单个 GSA 下系统状态的实部和虚部的 RMSE 估计。值得注意的是，在单个 GSA 存在的情况下，所提提出的 JMAP-ML 算法实现了与传统估计方法（即 WLSE 和 SpM）相当的 RMSE 性能。尽管如此，JMAP-ML 算

法表现出优越的鲁棒性，因为 RMSE 始终低于 0.025 的阈值。

在场景 2 中，PMU-1 和 PMU-5 受到 GSA 攻击，导致相移30°和12°（即$\alpha_1 = 30^{\circ}$、$\alpha_5 = 12^{\circ}$），相应的测量偏移量如图 4-1 所示。文献[59]验证了 SpM 算法在面对多个 GSA 时的估计性能显著下降。因此，在面对多个 GSA 时，将该算法与 SpM 和 AM 算法进行了比较，仿真结果如图 4-4 和图 4-5 所示。图 4-4、图 4-5 显示了在 PMU-1 和 PMU-5 受到攻击时，由 SpM、AM 和 JMAP-ML 算法估计的每个节点状态变量的实部和虚部的 RMSE。也证实了 SpM 算法在面对多个 GSA 时的估计性能比面对单个 GSA 时明显下降。与 SpM 算法相比，AM 算法显著提高了状态估计的 RMSE。然而，所提的 JMAP-ML 算法显示出更好的总体估计精度。

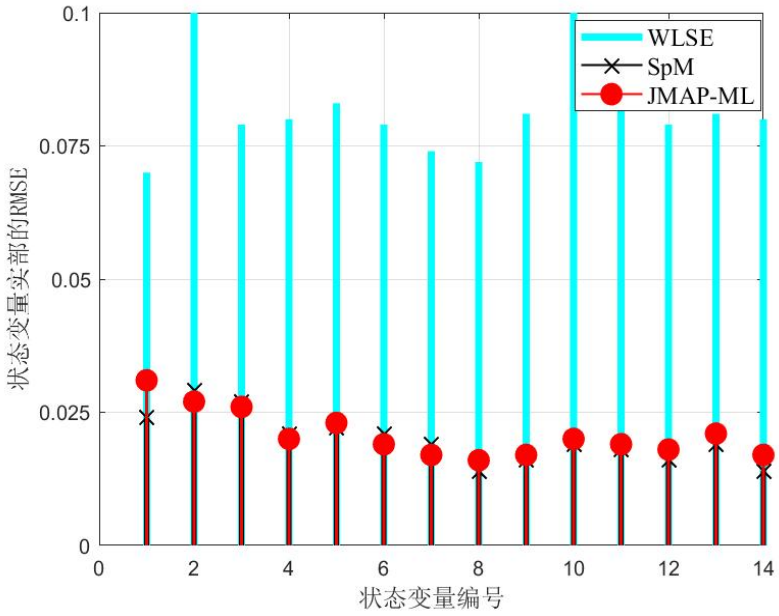


图 4-2 单个 GSA 时不同算法在估计状态变量实部时的均方根误差

此外，在仿真中，通过对于隐变量 的估计可以确定被攻击数据进而确定被攻击 PMU 的位置，并且还估计了欺骗攻击的相角偏移，如表 4-3 和表 4-4 所示。结果表明，当只有一个 GSA 时，SpM 算法和 JMAP-ML 算法对攻击的响应是相似的。但是，一旦存在多个 GSA，SpM 算法的性能就会明显下降。在这一点上，JMAP-ML 和 AM 算法可以有效地减轻 GSA 的影响，特别是 JMAP-ML 算法在估计偏移角时更准确，更接近真实值。因此，本章提出的算法总体上优于其他比较算法。

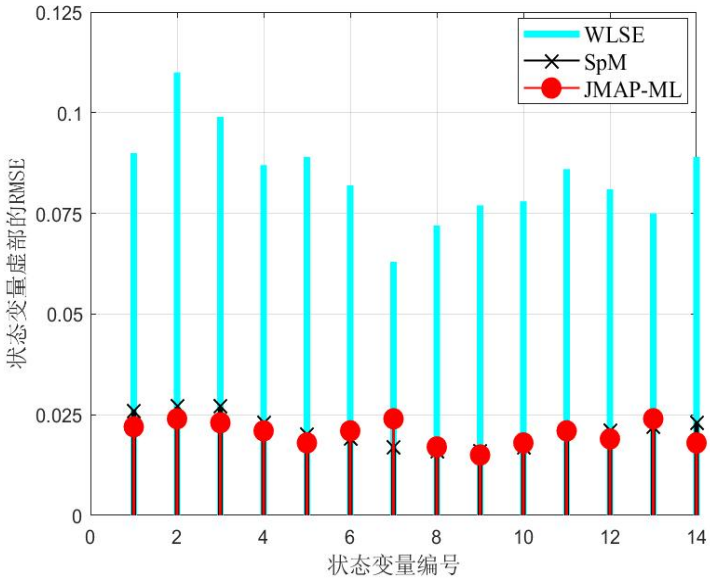


图 4-3 单个 GSA 时不同算法在估计状态变量虚部时的均方根误差

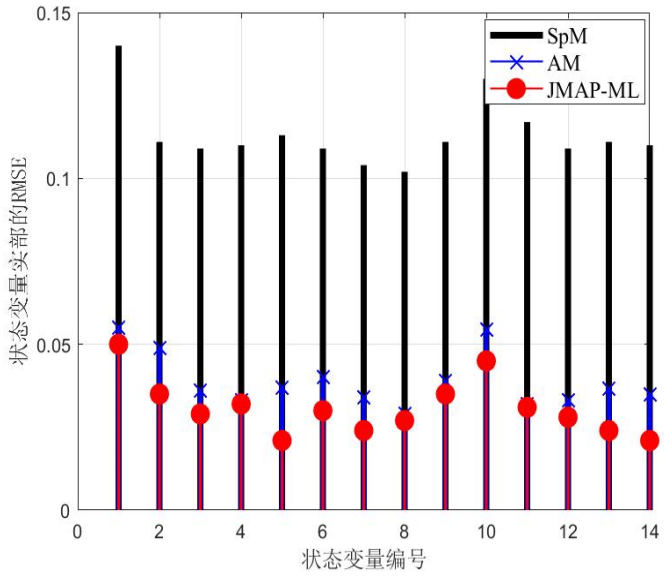


图 4-4 多个 GSA 时不同算法在估计状态变量实部时的均方根误差

为了更好地比较不同算法的性能，还记录了整个采样过程中系统状态变量的 RMSE 结果，如表 4-4 和表 4-5 所示。从这些表中可以看出，JMAP-ML 算法在性能上优于其他比较算法。无论是在面对单个 GSA 还是多个 GSA 时，JMAP-ML 算法对于状态变量估计的精度上都具有很大的提升，尤其是面对系统中多个 GSA 存在的情况下。

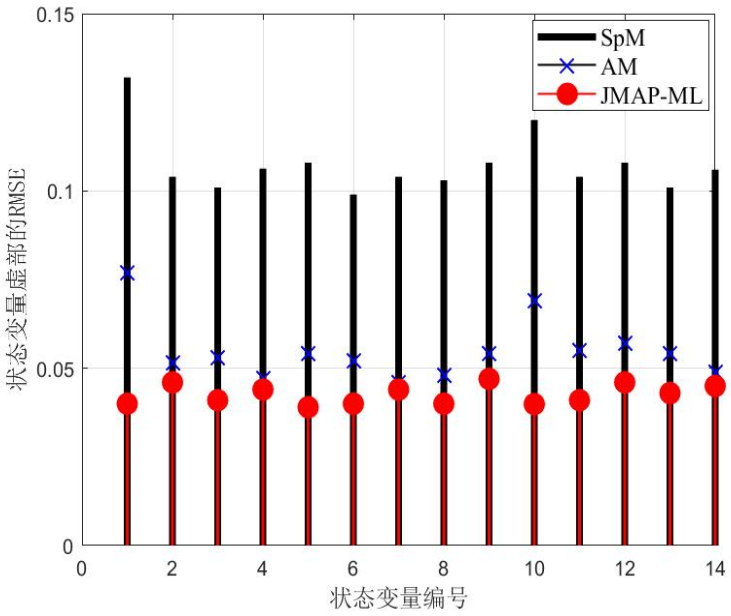


图 4-5 多个 GSA 时不同算法在估计状态变量虚部时的均方根误差

表 4-2 单个 GSA 下单一相位偏移时不同算法估计结果

偏移角	实际偏移角	SpM 算法	JMAP-ML 算法
α^{at}	45°	44.42°	44.59°

表 4-3 多个 GSA 下多相位偏移时不同算法估计结果

偏移角	实际偏移角	SpM 算法	AM 算法	JMAP-ML 算法
α_1^{at}	30°	25.93°	28.16°	29.53°
&	&	&	&	&
α_2^{at}	12°	7.32°	11.09°	12.19°

表 4-4 单个 GSA 下不同算法的均方根误差

算法	估计量实部的 RMSE	估计量虚部的 RMSE
WLS	1.33e-01	8.41e-02
SpM	1.99e-02	2.11e-02
JMAP-ML	2.08e-02	2.04e-02

表 4-5 多个 GSA 下不同算法的均方根误差

算法	估计量实部的 RMSE	估计量虚部的 RMSE
SpM	1.225e-01	1.41e-01

AM	4.19e-02	4.65e-02
JMAP-ML	3.09e-02	4.26e-02

4.5.3 GSA 在不同 PMU 部署下的系统状态估计结果分析

上一小节的仿真结果发现了一个现象：当系统中部署了 6 个 PMU，且节点 2 上的 PMU 受到攻击时，对于节点 1 上状态变量的估计却出现了较大的 RMSE。通过分析发现这主要是由于节点 2 上的 PMU 是唯一一个能够观测到节点 1 的 PMU。因此，在节点 2 的 PMU 遭受攻击时，关于节点 1 的数据冗余度大大降低，导致状态估计的准确度显著下降。这一问题可以通过优化 PMU 的部署来提升系统对攻击的抵抗能力。毕竟，电力系统的稳定运行在很大程度上依赖于状态估计的准确性，而 PMU 的部署策略则是影响状态估计准确性的关键因素之一。

为了验证这一思路，本研究在 IEEE-14 节点系统上进行了深入的仿真分析。IEEE-14 节点系统作为一个典型的电力系统模型，其 PMU 的部署策略已经得到了广泛的研究。这些研究涵盖了从成本最小化到系统全局可观测性的多个方面，包括考虑零注入节点和分支故障的最佳放置策略等[63]。

在本次仿真中，考虑了三种不同的 PMU 部署方案。这些方案都是在确保系统全局可观测性的前提下，根据不同的优化目标和约束条件制定的。通过在这些方案下进行仿真，可以更全面地评估算法在不同 PMU 部署情况下的性能表现。表 4-6 详细列出了这三种不同的部署方案。这些方案不仅展示了 PMU 在系统中的具体位置，还反映了不同部署策略对系统状态估计和攻击抵抗能力的影响。

表 4-6 IEEE-14 节点系统 PMU 的不同部署方式

PMU 数量	PMU 部署在节点的位置
6	2，4，6，7，9，13
8	1，2，4，6，7，9，10，13
12	1，2，3，4，5，6，7，8，9，10，11，13

在本仿真测试中，采用了 JMAP-ML 算法来估计特定的攻击情况，即攻击目标锁定在节点 2 和节点 9 的 PMU 上。当系统中部署了 6 个 PMU 时，该算法的

表现通过图 4-6 和图 4-7 得到了直观的展示。图中显示了算法对状态变量实部和虚部的估计的 RMSE 的情况。为了深入探究 PMU 部署数量对算法估计性能的影响，在保持攻击位置不变的前提下，分别模拟了部署 8 个和 12 个 PMU 的场景，并对算法的估计性能进行了细致的分析。通过对比分析不同部署数量下的估计结果发现随着 PMU 部署数量的增加，JMAP-ML 算法对状态变量实部和虚部的估计的 RMSE 呈现出明显的减小趋势。特别是在系统部署了 12 个 PMU 后，状态估计的 RMSE 有了显著的下降。这一结果表明，随着 PMU 数量的增加，算法在面临 GPS 欺骗攻击时能够更好地利用冗余数据，从而实现对状态变量的更准确估计。几乎可以说，算法的优化可以使得其能够忽略 GPS 欺骗攻击对状态估计的干扰。

更直观的结果被展示在图 4-8 中，图 4-8 说明里在相同攻击条件下，估计的 RMSE 如何随着 PMU 部署数量的增加而逐渐减小。此外，实验还对不同 PMU 部署方案下 JMAP-ML 算法对状态变量实部和虚部的 RMSE 进行了详细的计算，并将结果记录在表 4-7 中。通过对比这些数值数据，可以发现当系统受到相同的 GSA 影响时部署 12 个 PMU 估计的实部和虚部的 RMSE 相对于部署 6 个时分别提高 74.9%和 75.1%，这说明了数据冗余度对于系统状态估计的精度有很大的影响。

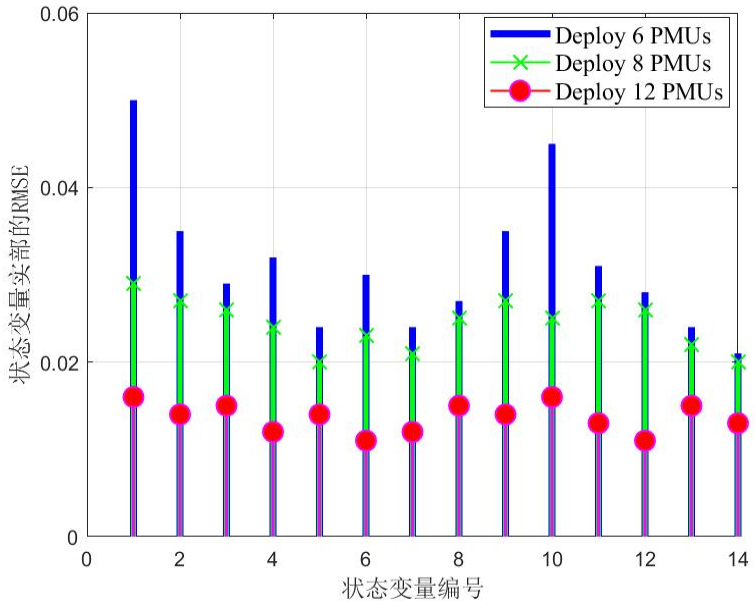


图 4-6 不同 PMU 部署下估计状态变量实部时的均方根误差

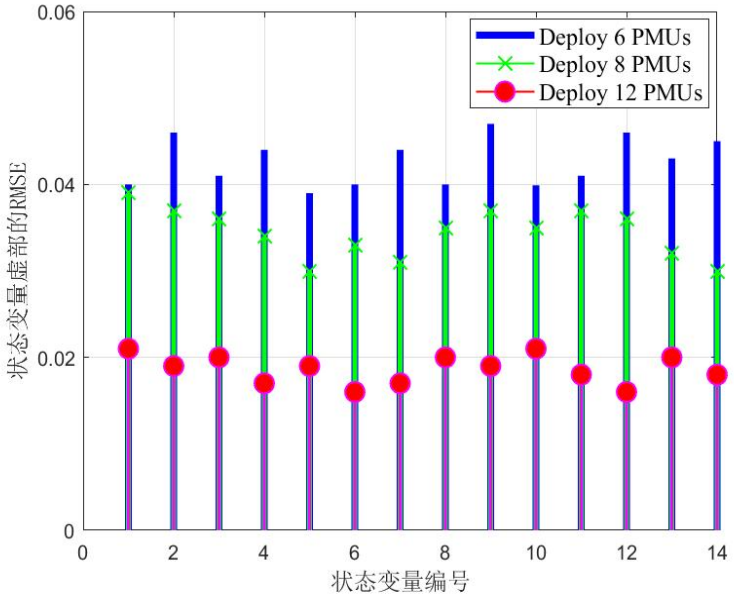


图 4-7 不同 PMU 部署下估计状态变量虚部时的均方根误差

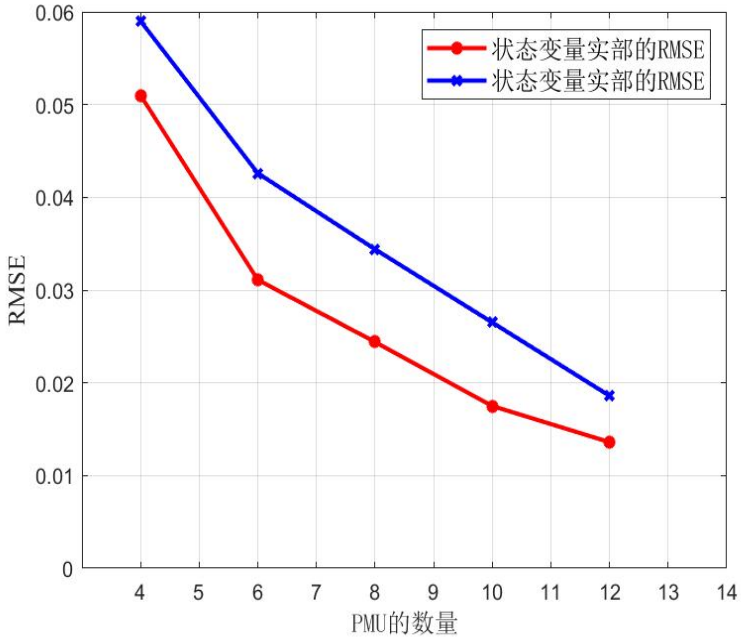


图 4-8 IEEE-14 节点系统上部署不同数量 PMU 时的系统状态变量估计的 RMSE

表 4-7 不同的 PMU 部署下 JMAP-ML 算法的均方根误差

PMU 数量	估计量实部的 RMSE	估计量虚部的 RMSE
6	3.11e-02	4.26e-02
8	2.44e-02	3.44e-02
12	0..78e-02	1.06e-02

4.5.4 GSA 攻击比例增加时不同算法性能比较

在前期仿真研究中，主要探究了系统中两个 PMU 受到攻击时算法性能的表现。然而，在本节中，将注意力转向了更为复杂的情境，即考虑了 12 个 PMU 的系统部署，并在不同攻击比例下对算法性能进行了深入研究。对 1 至 4 个 PMU 受到攻击时的算法状态估计相对误差进行了广泛的仿真，并对各算法的优缺点进行了详尽的比较。所有仿真结果的综合呈现如图 4-9 所示。

从图 4-9 中可以明显观察到，随着攻击比例的增加，WLS 和 SpM 算法的状态估计相对误差呈逐渐扩大的趋势，暴露出了其在面对多重 PMU 攻击时的不足之处。图 4-9 可以清晰地观察到，随着攻击比例的增加，传统的 WLS 和 SpM 算法的状态估计相对误差呈现出逐渐扩大的趋势。这表明，在面对多重 PMU 攻击时，这两种算法的性能受到了严重的影响，无法保持稳定的估计精度。然而，与这两种算法不同的是，AM 和 JMAP-ML 算法在不同攻击率下展现出了相对稳定的性能表现。特别是本章所提出的 JMAP-ML 算法，即便在 30%的 PMU 受到攻击的情况下，其相对误差仍能保持在 0.02 以下，相较于 AM 算法有了显著的提升。这一结果充分证明了 JMAP-ML 算法在面对多个 PMU 受到攻击的复杂情境时，不仅表现出了良好的鲁棒性，而且在估计精度上也具有显著优势。

4.5.5 算法收敛性能分析

本次仿真实验，深入探索所提出的迭代 JMAP-ML 算法的收敛性表现，并通过对算例的细致分析，观察到了一个引人注目的现象：当系统部署了 6 个 PMU，且位于节点 2 的 PMU 遭受攻击，导致其相位角偏移逐渐增大时，状态变量的实部和虚部均方根误差随着迭代次数的递增，展现出了稳健且稳定的收敛趋势。具体结果 bei1 记录在图 4-10 和图 4-11 中，两张图表显示了算法收敛的动态过程。值得注意的是，在状态变量的更新过程中，可以发现，该算法仅需进行最多不超过 5 次的迭代，便能实现收敛。这不仅证明了算法的高效性，更突显了其在处理复杂数据时的强大能力。并且随着攻击引起的偏差不断增大，算法所需的迭代次数却呈现出减少的趋势。这一特性表明，在面对更为严重的攻击时，算法反而能够更快地收敛。迭代次数的减少不仅意味着计算效率的提升，更为实时在线的数

据处理提供了强有力的支持。在电力系统的实时监控和数据分析中，算法的快速收敛特性显得尤为重要。它能够确保在有限的时间内，对大量数据进行准确、高效的处理，从而为电力系统的稳定运行提供及时、有效的决策支持。即使在面对大规模网络时，迭代 JMAP-ML 算法依然能够保持其高效、稳定的收敛性能，为电力系统的安全、稳定运行提供有力保障。

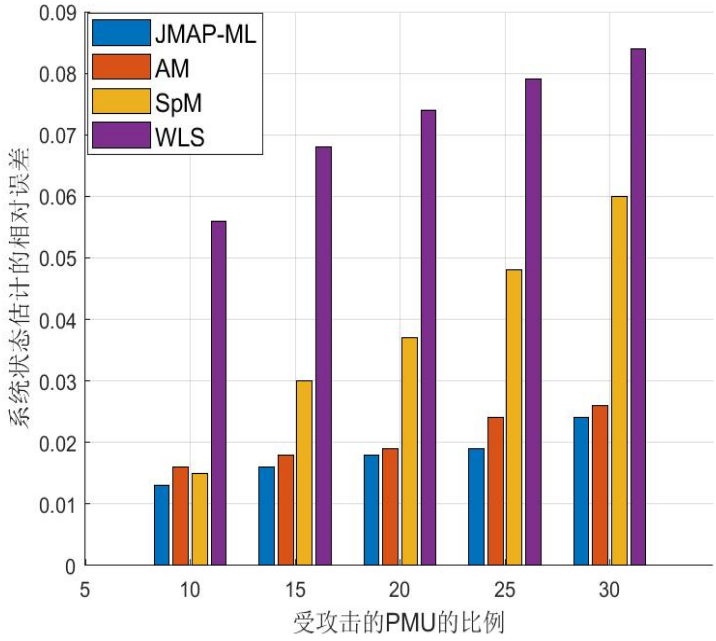


图 4-9 IEEE-14 节点系统上部署的 PMU 受攻击比例不同下的系统状态估计的相对误差

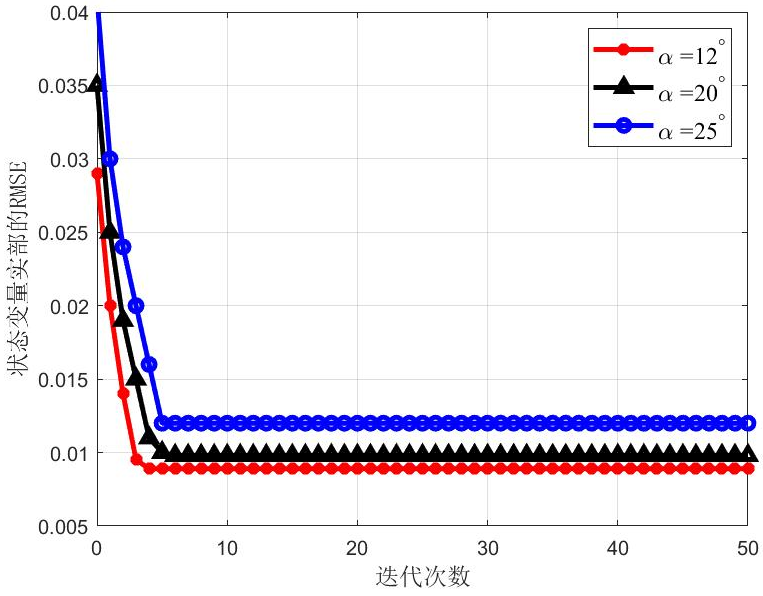


图 4-10 不同相位偏移下状态变量的实部均方根误差与迭代次数的关系

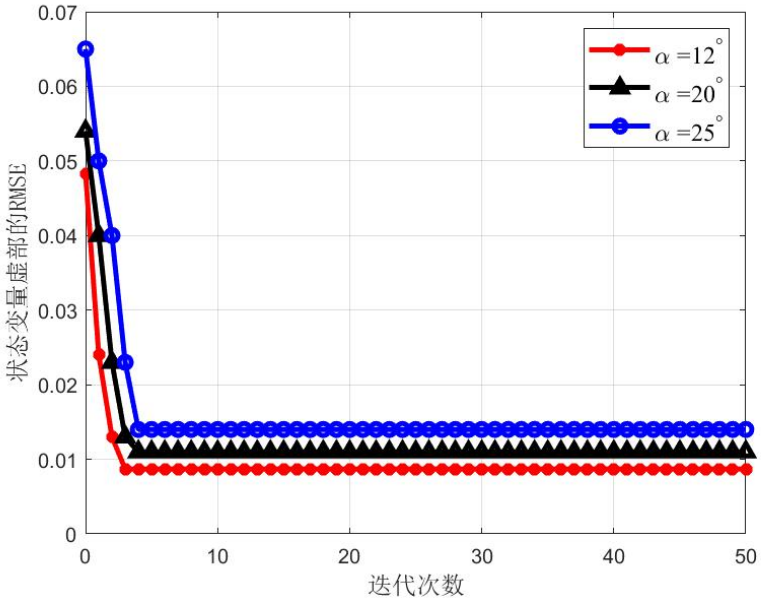


图 4-11 不同相位偏移下状态变量的虚部均方根误差与迭代次数的关系

4.6 本章小结

本章提出了一种基于联合最大后验和最大似然算法的 GPS 欺骗攻击检测和系统状态估计的方法。推导了基于 PMU 的 GSA 量测模型用于系统状态估计问题，并将其表述为混合极大似然问题。在公式化问题中，所涉及的未知参数是耦合的，目标函数是非凸的，这给寻找最优解带来了很大的挑战。为了解决这些问题，提出了一种 JMAP-ML 算法来安全地估计 PMU 混合测量中的系统状态并检测 GSA。通过对 IEEE-14 节点系统中进行不同测试场景的仿真，验证了该算法在 GSA 检测和状态估计方面的性能。从数据冗余度角度，分析了 PMU 布置对于 GSA 的影响。

第 5 章 总结与展望

5.1 全文总结

电网安全和电网智能化的发展日益受到人们的关注，PMU 在电力系统状态估计中的作用越来越重要。传统的电力系统监测方法依赖于 SCADA 系统进行稳态运行，但在预测电网状态、低频振荡、故障分析和实时安全监测方面的作用有限。相比之下，PMU 可以提供同步测量并生成可用于系统状态估计的线性模型。此外，它们的采样率远快于 SCADA，可以实时估计电力系统的状态，并对异常情况做出快速反应。通过为每个单元配备一个利用民用信号进行同步的 GPS 接收机，可以实现 PMU 的高采样率和准确的时间同步。然而，民用 GPS 接收机容易受到产生虚假信号的网络攻击，即 GPS 欺骗攻击。GPS 欺骗攻击会导致 PMU 与控制中心不同步，导致 PMU 的时间延迟和采样相位失配，从而阻碍了对电网状态的实时准确估计，导致状态估计误差很大。本文从电力系统安全人员角度使用估计理论等方法对该攻击对电网系统的造成的影响进行研究分析，提出相应的检查和缓解方法并进行仿真实验以验证方案的有效性。本文主要完成以下几方面工作：

1）研究了 PMU 受 GPS 欺骗攻击的原理，分析了该攻击对于系统实现实时状态估计的巨大挑战。

2）通过比较攻击前后电压电流的变化情况以及安全条件下的量测模型推导出受 GSA 下的 PMU 量测模型。

3）为了检测和缓解 GSA，从量测模型中矩阵特殊性质角度入手，提出了一种新的基于残差的电网欺骗检测与测量校正算法，该算法可以检测和缓解不同攻击角度的多个 GSA。算法由两个关键子算法组成：欺骗检测算法通过监测测量残差的欧几里得范数，以区分安全和欺骗攻击场景。在安全场景中，没有任何 PMU 被欺骗，而在欺骗场景中，有一个或多个 PMU 被不同的攻击角度欺骗。并且将校正后的数据进行正确的系统状态估计。最后在不同测试系统进行了仿真实验，并且与其他研究方法进行了对比分析，仿真结果表明该方法对于检测和缓解 GSA 尤其是多个 GSA 存在时具有明显的效果。

（4）从整个参数耦合的模型出发，为了检测和缓解 GSA，采用一种基于混合建模的测量模型，引入双模混合分布来表示 PMU 混合测量中的误差，该模型提供了 PMU 中测量误差的更准确表示，并且提出了一种联合最大后验和最大似然（JMAP-ML）算法来安全地估计 PMU 混合测量中系统的正确状态和检测 GSA。最后在不同测试系统进行了仿真实验，与其他研究方法进行了对比分析的仿真结果表明所提算法对于检测和缓解 GSA 都具有良好的效果。

5.2 工作展望

本文主要针对电力系统中部署的 PMU 受 GPS 欺骗攻击的问题进行了初步研究，尽管取得了一些研究成果，但有待进一步研究：

（1）在面对 GPS 欺骗攻击时，目前采用的检测和防御方法都是在攻击已经发生后才启动的，这使得防御者处于一种被动的状态。为了更有效地保障智能电网的安全运行，迫切需要转变策略，从被动防御转向主动防御。通过采用主动防御措施在攻击发生之前就采取行动，阻断潜在攻击的源头，从而彻底消除安全隐患。具体而言，可以研究针对智能电网 GPS 欺骗攻击的主动防御方法。通过实施这些方法，可以在攻击者能够发动实际攻击之前，识别并阻止其欺骗行为。这种前瞻性的安全策略将为智能电网的可靠性和安全性提供更为坚实的保障。在未来的研究中，将致力于发展创新性的技术和系统，以实现对电网安全的主动保护。这包括但不限于利用先进的监测技术、强化网络安全协议以及实施智能化的反欺骗机制。通过这些努力，希望能够彻底改变我们在电网安全方面的角色，从而更加主动地确保智能电网的稳健运行。

（2）以往的大多数研究都着眼于软件层面开展 GSA 的检测和防护，后续可以针对 GPS 欺骗攻击，着重于构建多层次的防御策略，这一策略的精髓在于它的全方位性。未来将不仅仅侧重于单一层面的防护，而是通过在硬件、网络通信和应用层面综合运用安全措施，验证机制以及智能算法，打造一个层层设防、多重护盾的安全体系。在硬件层面，可以考虑采用物理安全措施，例如加密模块和安全认证芯片，以防止未经授权的访问或信息篡改。同时，强化设备防护、实施安全启动程序等措施也将成为提高整体系统安全性的重要步骤。

参考文献

[1] 董朝阳, 赵俊华, 文福拴, 薛禹胜. 从智能电网到能源互联网: 基本概念与研究框架[J]. 电力系统自动化, 2014, 38(15): 1-11.

[2] 王博，吴舟婷，吴倩等. 关键信息基础设施 ICT 供应链安全风险评估指标体系研究[J]. 信息安全与通信保密, 2020(12): 103-111.

[3] 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.

[4] Adhikari U, Morris T, Pan S.WAMS Cyber-Physical test bed for power system cybersecurity study, and data mining[J]. IEEE Transactions on Smart Grid, 2017, 8(6): 2744-2753.

[5] 朱鹏程，柳劲松，范士雄等.考虑混合量测的配电网二次约束二次估计方法[J]. 电网技术, 2019，43(3): 841-847.

[6] Siamak S, Dehghani M, Mohammadi M. Dynamic GPS spoofing attack detection, localization, and measurement correction exploiting PMU and SCADA[J]. IEEE Systems Journal, 2020,6(4): 1-10.

[7] Zonouz S, Davis M C, Davis R D, et al. SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures[J]. IEEE Transactions on Smart Grid, 2014, 5(1): 3-13.

[8] Phadke A G. Synchronized phasor measurements in power systems[J]. IEEE Computer Applications in Power, 1993, 6(2): 10-15.

[9] Risbud P, Gatsis N, Taha A, et al. Vulnerability analysis of smart grids to GPS spoofng[J]. IEEE Transactions on Smart Grid, 2019, 10(4): 3535-3548.

[10] Do C B, Stacchini S C. Forecasting-aided state estimation—part I: panorama[J]. IEEE Transactions on Power Systems, 2009, 24(4): 1667-1677.

[11] Benedito, Raphael A S. Power system state estimation: undetectable bad data[J]. European Transactions on Electrical Power, 2014, 24(1): 91-107.

[12] Yu Y, Wang Z, Lu C. A joint filter approach for reliable power system state estimation[J]. IEEE Transactions on Instrumentation and Measurement,

2019,68(1): 87-94.

[13] Schweppe F C, Wildes J. Power system static-state estimation, part I: Exact model[J]. IEEE Transactions Power Apparatus and Systems 1970, PAS-89: 120-125.

[14] Schweppe F C, Rom D. Power system static-state estimation, part II: Approximate model[J]. IEEE Transactions Power Apparatus and Systems, 1970, PAS-89: 125-130.

[15] Couch G H. Improved power system state estimation with constant gain matrices[J]. Proceedings of the IEEE, 2016, 64(11): 1641-1643.

[16] Irving M R, Owen R C, M. Sterling J H. Power-system state estimation using linear programming[J]. Proceedings of the Institution of Electrical Engineers, 2008, 25(9): 879-885.

[17] Brameller A, Karaki S H. Power-system state estimation using linear programming[J]. Electrical Engineers Proceedings of the Institution, 2019, 126(3): 246-247.

[18] Ferreira I M, Barbosa F P M. A square root filter algorithm for dynamic state estimation of electric power systems[C]// Electrotechnical Conference, Antalya, Turkey, 1994: 877-880.

[19] Zanni L, Le Boudec J Y, Cherkaoui R, Paolone M. A prediction-error covariance estimator for adaptive Kalman filtering in step-varying processes: Application to power-system state estimation[J]. IEEE Transactions on Control Systems Technology, 2017, 25(5): 1683-1697.

[20] Kwon S J. Robust Kalman filtering with perturbation estimation process for uncertain systems[J]. IEEE Proceedings Control Theory and Applications, 2006, 153(5): 600-606.

[21] Manda S, Balakrishna K, Sriharibabu A. Linear programming method to find the minimal placements of phasor measuring units for power system state estimation[C]// 2017 International Conference on Power and Embedded Drive Control (ICPEDC), Chennai, India, 2017: 360-364.

[22] Emami K, Fernando T, Nener B. Power system dynamic state estimation using particle filter[C]// IECON 2014 40th Annual Conference of the IEEE Industrial Electronics Society, Dallas, TX, USA, 2014: 248-253.

[23] Emami K, Fernando T, Iu C, Trinh H, Wong K P. Particle filter approach to dynamic state estimation of generators in power systems[J]. IEEE Transactions on Power Systems, 2015, 30(5): 2665-2675.

[24] De Oliveira-De Jesus P M, Rodriguez N A, Celeita D F, et al. PMU-based system state estimation for multigrounded distribution systems[J]. IEEE Transactions on Power Systems, 2020, 36(2): 1071-1081.

[25] Yaghoti A A, Moghaddam M P, Haghifam M R, et al. A new formulation IPCA based method for branch-current estimation in distribution networks[C]// CIRED Seminar 2008: SmartGrids for Distribution, Frankfurt, 2008: 73-73.

[26] Yohanandhan R V, Elavarasan R M, Manoharan P. Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications[J]. IEEE Access, 2020, 8: 151019-151064.

[27] Wang S, Liu G. State estimation for active distribution networks based on multisource hybrid measurements[C]// 2016 China International Conference on Electricity Distribution (CICED), Xi'an, China, 2016: 1-6.

[28] Kong X, Yan Z, Guo R, Xu X, Fang X. Three-Stage distributed state estimation for AC-DC hybrid distribution network under mixed measurement environment[J]. IEEE Access, 2018, 6: 39027-39036.

[29] Li Y. Method for extracting patterns of coordinated network attacks on electric power CPS based on temporal-topological correlation[J]. IEEE Access, 2020, 8: 57260-57272.

[30] Jahromi A A, Kemmeugne A, Kundur D. Cyber-Physical attacks targeting communication-assisted protection schemes[J]. IEEE Transactions on Power Systems, 2020, 35(1): 440-450.

[31] Kim J, Kang J H, Bae J, Lee W. Distributed moving horizon estimation via operator splitting for automated robust power system state estimation[J]. IEEE

Access, 2021, 9: 90428-90440.

[32] Zhong W, Liu W, Yao Y, Yu. State estimation of new distribution network based on deep neural network[C]// 2023 International Conference on Power System Technology (PowerCon), Jinan, China, 2023: 1-6.

[33] Muscas C, Pegoraro P A, Sulis S, Pau M, Ponci F, Monti A. New Kalman filter approach exploiting frequency knowledge for accurate PMU-based power system state estimation. IEEE Transactions on Instrumentation and Measurement, 2020, 69(9): 6713-6722.

[34] Ascari B, Costa A S. A bad data resilient multisensor fusion framework for hybrid state estimation[J]. IEEE Transactions on Power Systems, 2024, 39(1): 132-146.

[35] Zhao J B, Gómez-Expósito A. Power system dynamic state estimation: Motivations, definitions, methodologies, and future work[J]. IEEE Transactions on Power Systems, 2019, 34(4): 3188-3198.

[36] Chitsazan M A, Fadali M S, Trzynadlowski A M. State estimation for large-scale power systems and FACTS devices based on spanning tree maximum exponential absolute value. IEEE Transactions on Power Systems, 2020, 35(1): 238-248.

[37] Zhao J B, Marcos N, Huang Z Y. Roles of dynamic state estimation in power system modeling, monitoring and operation[J]. IEEE Transactions on Power Systems, 2021, 36(3): 2462-2472.

[38] Abolmasoumi A H, Farahani A, Mili L. Robust particle filter design with an application to power system state estimation[J]. IEEE Transactions on Power Systems, 2024, 39(1): 1810-1821.

[39] 闫童. 电力系统状态估计并行加速研究[J]. 上海电气技术, 2023, 16(01): 1-5.

[40] Song W, He J, Lin J, Ye H, Ling X, Lu C. Bias analysis of PMU-based state estimation and Its linear bayesian improvement[J]. IEEE Transactions on Industrial Informatics, 2024, 20(2): 1607-1617.

[41] Iadarola G, Disha D, Santis A D, Spinsante S, Gambi E. Global positioning system measurements: Comparison of IoT wearable devices[C]// 2022 IEEE 9th International Workshop on Metrology for AeroSpace, Pisa, Italy, 2022: 213-218.

[42] Ioannides R T, Pany T, Gibbons G. Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques[J]. Proceedings of the IEEE, 2016, 104(6): 1-21.

[43] Dempster A G, Cetin E. Interference localization for satellite navigation systems[J] Proceedings of the IEEE, 2016, 104(6): 1318-1326.

[44] Vyskocil P, Sebesta J. Relative timing characteristics of GPS timing modules for time synchronization application[C]// 2009 International Workshop on Satellite and Space Communications, Siena, Italy, 2009: 230-234.

[45] Risbud P, Gatsis N, Taha A. Vulnerability analysis of smart grids to GPS Spooffng[J]. IEEE Transactions Smart Grid, 2019, 10(4): 3535-3548.

[46] Zhang Q, Vittal V, Heydt G, Chakhchoukh Y, Sturgill S. The time skew problem in PMU measurements[C]// 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 2012: 1-6.

[47] Bhamidipati S, Mina T Y. GPS time authentication against spoofing via a network of receivers for power systems[C]// 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 2018:1485-1491.

[48] Psiaki M L, Humphreys T E. GNSS spoofing and detection[J]. Proceedings of the IEEE, 2016, 104(6):1258-1270.

[49] Mina T Y, Bhamidipati S, Gao G X. Detecting GPS spoofing via a multi-receiver hybrid communication network for power grid timing verification[C]// Process 31st International Technical Meeting of the Satellite Division of the institute of navigation, Miami, United States, 2018: 2963-2977.

[50] Bhamidipati S, Gao G X. GPS multireceiver joint direct time estimation and spoofer localization[J]. IEEE Transactions on Aerospace and Electronic Systems, 2019, 55(4): 1907-1919.

[51] Zhu F, Youssef A, Hamouda W. Detection techniques for data-level spoofing in GPS-based phasor measurement units[C]// 2016 International Conference on Selected Topics in Mobile & Wireless Networking, Cairo, Egypt, 2016: 1-8.

[52] Pradhan P, Nagananda K, Venkitasubramaniam P, Kishore S, Blum R S. GPS

spoofing attack characterization and detection in smart grids[C]// 2016 IEEE Conference on Communications and Network Security, Philadelphia, PA, USA, 2016: 391-395.

[53] Ming Z, Centeno V A, Thorp J S, Phadke A G. An alternative for including phasor measurements in state estimators[J]. IEEE Transactions on Power Systems, 2016, 21(4): 1930-1937.

[54] Jain A, Shivakumar N R. Impact of PMU in dynamic state estimation of power systems[C]// 2008 40th North American Power Symposium, Calgary, AB, Canada, 2008: 1-8.

[55] Kekatos V, Giannakis G B. Distributed robust power system state estimation[J]. IEEE Transactions on Power Systems, 2017, 28(2): 1617-1626.

[56] Yang P, Tan Z, Wiesel A, Nehorai A. Power system state estimation uing PMUs with imperfect synchronization[J]. IEEE Transactions on Power Systems, 2019, 28(4): 4162-4172.

[57] Chauhan S, Gao G X. Spooffng resilient state estimation for the power grid using an extended kalman filter[J]. IEEE Transactions on Smart Grid, 2021, 12(4): 3404-3414.

[58] Risbud P, Gatsis N, Ahmad T. Vulnerability analysis of smart grids to GPS spoofing[J]. IEEE Transactions on Smart Grid, 2019, 10(4): 3535-3548.

[59] Fan X, Du L, Duan D. Synchrophasor data correction under GPS spoofing attack: A state estimation-based approach[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4538-4546.

[60] Bilmes J A. A gentle tutorial on the EM algorithm and its application to parameter estimation for Gaussian mixture and hidden Markov models[M], University of California, Berkeley, CA, USA, Technology Reports, 1998.

[61] Gupta M R, Chen Y H. Theory and use of the EM algorithm[J]. Found Trends Signal Process, 2010, 4(3): 223-296.

[62] Boyd S, Vandenberghe L. Convex Optimization[M]. New York, USA: Cambridge University Press, 2004.

[63] Aminifar F, Khodaei A, Fotuhi-Firuzabad M, Shahidehpour M. Contingency-constrained PMU placement in power networks[J]. IEEE Transactions on Smart Grid, 2010, 25(1): 516-523.

攻读硕士期间取得的学术成果

[1] Hua F, Gao W, Li Y, Hu P, Qiao L. Joint Detection and State Estimate with GSAs in PMU-Based Smart Grids. Energies. 2023; 16(15):5731.

[2] Hua F, Gao W, Li Y, Hu P, Qiao L. Optimal PMU Placement and Fault Location Under Single PMU Failure, 2023 38th Youth Academic Annual Conference of Chinese Association of Automation (YAC), Hefei, China, 2023, pp. 40-44,

致谢

行文至此，落笔为终。相聚于秋，离别在夏。此刻回望研究生三年生涯，虽有焦虑艰辛，但更多的还是被身边人的温暖包围，就如同此刻窗外的太阳，让我很是舒服自在。这三年，我结识了一个人、一群人，深交了某个人、某些人，收获了一些不掺杂任何水分的关系，你们总是站在我的身边，给我求学和生活路上披荆斩棘的勇气和方法。在此，我要向你们致以诚挚的感谢！

首先，很是幸运来到了像家一样的实验室，衷心感谢让我跨越对老师刻板印象的导师高文根教授。您会像朋友一样跟我聊天，教我学术，帮助我学会规划我的时间，照顾我的生活。论文从选题到定稿的细节处理上，每一步您都倾注了大量心血。生活上，您教会我做人的道理会让我受益一生。

其次，我要感实验室同门和师弟师妹以及室友们给予我的关心和帮助，让我在整个研究生生涯待的最久的地方收获了知识的同时也度过了如此欢乐的时光。

特别地，还要感谢我的挚友们，包括但不限于郑锐、王志成、陈刚。感谢十年来的陪伴，从高中到本科再到读研，不管是取得成绩时的喜悦还是迷茫混沌时的失意，你们都一直在我身边，用不同形式的陪伴去给我鼓励和支持。你们是我最宝贵的财富。祝愿友谊长存，各自在工作生活中顺利、健康。

最后，我要感谢我的父母，感谢你们对我整个二十多年里的养育和帮助，以及在我做任何选择时的无条件尊重和支持，谢谢你们。

最后，再次感谢你们的存在，让我能够顺利完成这篇论文。愿你们一切都好。