摘要

智能电网在电力系统中使用新兴的物联网技术收集系统数据，以分析电网电力需求和系统状态。随着智能电网的快速发展，海量实时数据需要频繁从智能电表传输至云端服务器处理，推进了基于云计算的智能电网系统的应用和部署。在云层和智能计量设备层之间加入中间雾节点，已成为提高云计算性能的一个重要趋势。然而，雾计算模型带来性能提升的同时，如何在保护智能电网大数据安全和隐私的前提下实现高效收集和处理数据成为基于雾计算智能电网亟需解决的重要问题。

本文研究解决当前基于雾计算的智能电网数据聚合方案容易产生雾节点单点故障、且计算成本和通信开销高等问题。主要工作包括以下方面：

（1）提出了一种针对单点故障的智能电网多维数据聚合方案。基于含有雾群的雾计算智能电网系统模型，设计了一种雾节点分配策略。将一个含有多个雾节点的雾群对应多个智能电表子区域，使用动态优先级方法分配雾群中雾节点进行数据聚合工作，以降低单点故障风险。进而提出了一种隐私保护多维数据聚合方案，支持智能电表一次向控制中心报告多种类型的数据，实现数据高效处理。安全性分析表明本方案可以较好的满足安全性。在性能分析中显示了本方案在计算成本的优势。

（2）基于雾计算的无可信机构智能电网模型，提出了一种高效多维数据聚合方案，既减少通信链路，同时保证数据聚合的安全性。方案采用椭圆曲线加密机制，支持不依赖可信机构的数据加密，降低因密钥分发而产生的大量通信开销；再者，使用批量验证的双线性配对技术实现高效身份验证；通过安全性分析证明无可信机构的智能电网高效多维数据聚合方案的数据隐私和安全；保证用户的个人信息在数据聚合过程中无法被获取。性能分析表明，本方案与现有方案相比具有更低的计算成本与通信开销。

关键词：雾计算；智能电网；数据聚合；隐私保护

Abstract

Smart grid uses emerging Internet of Things technology in the power system to collect system data to analyze grid power demand and system status. With the rapid development of smart grid, massive real-time data needs to be frequently transmitted from smart meters to cloud servers for processing, which promotes the application and deployment of cloud computing-based smart grid systems. Adding intermediate fog nodes between cloud servers and smart meters has become an important trend to improve cloud computing performance. However, while the fog computing architecture brings performance improvement, how to efficiently collect and process data on the premise of protecting the security and privacy of big data in the smart grid has become an important issue that needs to be solved urgently for the smart grid based on fog computing.

This paper studies and solves the problem that the current fog computing-based smart grid data aggregation schemes are prone to single point failure of fog nodes, and has high computation cost and communication overhead. The main work includes the following aspects:

(1) A smart grid multi-dimensional data aggregation scheme for single point of failure is proposed. Based on the fog computing smart grid system model with fog clusters, this paper designs a fog node allocation strategy. A fog group containing multiple fog nodes is corresponding to multiple smart meter sub-areas, and the fog nodes in the fog group are assigned for data aggregation by using the dynamic priority method to reduce the risk of single point failure. Furthermore, a privacy preserving multi-dimensional data aggregation scheme is proposed, which supports smart meters to report multiple types of data to the control center at a time to achieve efficient data processing. Security analysis shows that this scheme can better satisfy the security. The performance analysis shows the advantages of this scheme in computation.

(2) Based on the fog computing smart grid model without trusted authority, this paper proposes an efficient multi-dimensional data aggregation scheme, which not only reduces communication links, but also ensures the security of data aggregation. The scheme adopts the elliptic curve encryption mechanism, supports data encryption without relying on trusted authority, reduces a large amount of communication overhead due to key distribution; Furthermore, the bilinear pairing technology of batch verification is used to achieve efficient identity verification; Security analysis

proves that the smart grid's efficient multi-dimensional data aggregation scheme without trusted authority can achieve data privacy and security; ensure that users' personal information cannot be obtained during the data aggregation. The performance analysis shows that this scheme has lower computational cost and communication overhead compared with the existing scheme.

Keywords: Smart Grid; fog computing; data aggregation; privacy perserving

目录

第1章 绪论

随着电力系统信息化的快速发展，智能电网受重视程度与日俱增。智能电网中的各个实体进行通信，实现信息的传递与数据聚合。

1.1 研究背景与意义

现有电网可靠性不足，易限电、停电，输电损耗大，电能质量差，电力供应不足，不利于分布式能源的整合[1]，缓解这些问题需要对电力输送结构进行彻底的改革。智能电网给现有电网解决存在的问题带来了巨大的可能性。智能电网，即电网的现代化，是各种技术的不断融合，旨在给电网带来巨大变化，从而提高电网性能[2]。

“电网”一般用于发电、输电、配电和功率控制。众所周知，传统的电网是将电力从生产者输送到消费者的网络。电网中的主要阶段是发电、输电、变电、配电和消费。虽然这五个阶段已经成熟，但由于电力节点数量庞大，从分散的电力节点自动收集信息，对传统电网来说是非常困难的。这使得电网对于新的数字化、现代化和基于互联网的基础设施需求越发强烈。智能电网利用新兴通信技术取代传统电网，以实现更高效的管理分布式的电能和电力分配。

“智能电网”是对传统电力电网的增强，它是能源检测、分配和控制装置的现代化。智能电网可以解释为一个电力网络，它结合了智能技术来监控、控制和向消费者供电。智能电网生成了一个用于在网络内观察、分析、调控和通信的平台，用于更高效的控制能源的利用，尽可能地提高电能供应的经济性、可控性与健壮性。智能电网使用先进的物联网信息通信技术，将可再生能源与传统能源相结合，与传统电网相比具有更高的效率和可靠性[3]-[4]。

智能电网将先进的信息和通信技术、自动化、传感和计量技术融入其中，实现对电网信息的高效感知与能源管理。传统电网和智能电网之间的一个最大的区别就是消费者能够直接参与到电网的运行中来，实现了消费者和电力提供商之间的交流。

智能电表周期性提供实时信息，控制中心通过分析聚合用电数据实现电网供需近乎即时的平衡和灵活的管理[5]-[6]。智能电网一个显著的特点就是各个环节大量、高效的信息交换。如果没有处理好高效、快速的信息交换与信息安全之间的矛盾，将大大制约智能电网的发展[7]-[8]。在智能电网中，各个环节传递的数据信息如果遭到不法分子的窃取，将引发严重的隐私安全问题。如个人信息被窃取，

从而影响个人用户的人身和财产安全；智能电网中重要数据被不法分子恶意篡改，将影响智能电网健康、稳定的运行[9]。且随着智能电网的快速部署与应用，海量的数据信息从各类智能电表收集而来，智能电网将更容易遭受各种各样的威胁。因此，智能电网对于一个可靠、稳定、安全且足够及时快速处理能力的智能电表数据收集方案的需求越发强烈。

为了保护用户的隐私和信息安全，同时降低大量数据带来的高计算成本和通信开销，数据聚合的方法受到了许多学者的认可。通过数据聚合方法，可以将智能终端收集到的数据进行聚合，并将聚合结果发送给上级接收者，接收者仅从获取的聚合值分析数据。这样既能保护单个用户的隐私，也降低了计算成本和通信开销。

随着对数据聚合方案研究的深入，在传统的网络模型基础上提出了很多先进的网络模型，如基于云计算的智能电网模型，基于雾计算的智能电网模型等。虽然目前基于云计算的智能电网数据聚合方案解决部分数据聚合的安全和隐私问题，提升电网系统的整体性能，但也带来了新的挑战[10]。云计算的主要问题包括:（1）成本高，因为云计算需要配备大型数据中心。同时，云计算中心的维护是艰巨的，需要高传输带宽。（2）传统的云模型要求高速处理和大规模数据存储能力，没有有效的实时服务。（3）智能电网的云计算中心难以有效、实时地处理和分析海量数据。（4）在实际的智能电网计量系统环境中，当电力网络中的单个节点发生故障时，如何将所有故障设备的数据上传到云端进行分析的问题仍然没有解决。首先，分辨时间长，成本高。其次，需要上传大量的数据，这对通信网络的传输带宽要求很高。

仅靠云计算已无法解决智能电网面临的大多数挑战，例如海量数据带来的高带宽、高延迟和连接性不足等问题[11]-[12]。近年来，针对这些问题，学术界产生了广泛的讨论。2012 年 CISCO 的 Flavio Bonomi 首次提及并定义雾计算[13]。雾计算不是替代云计算，而是在网络的边缘预先处理或者解决一部分问题，以解决因网络带宽和存储空间不足而带来的问题，增强系统实时性和提高系统效率。在实际中，雾计算是一个虚拟的概念，其作为云计算模型中智能电表与云服务器的中间过渡层，提供计算、存储和通信的作用[14]。雾计算这个中间层中由无数个雾节点（Fog Node）组成，雾节点会对智能电表所上传的设备在发送到云服务器前进行预处理和分析[15]。每个雾节点（基站、小型服务器或者计算机）都具有低时延、分布性、可移动性、异构性和互操作性等特点。一般来说，在基于雾计算的智能电网模型中的用电数据由智能电表收集，雾节点初步处理，最终发送给控制中心。在这个数据传递过程中，一旦出现敏感的隐私数据泄露的问题，将给智能电网不可估量的后果。如用户的个人信息泄露，电网数据遭到非法的篡改等。

由此来看，如何解决智能电网在数据收集过程中存在的安全和隐私问题是不可忽视的。

此外，随着智能电网用户数量日益增大，用电类型和用电情况复杂多样，智能电表的功能越发丰富与强大，单一维度的上传数据信息显然有些不切实际。为了实现对智能电网精准的掌控与高效的电力资源分配，通常需要对大量的，多种维度的数据进行分析。现有数据聚合方案大多以高计算成本与通信开销为代价来实现对多维数据的处理，不适用于资源受限的终端采集设备。因此，对多维度用电数据的进行高效处理是智能电网数据聚合重要的研究方向。

综上所述，智能电网数据聚合是现阶段研究的一个热点，为智能电网数据收集与分析问题提供了一种重要解决思路。随着智能电网研究深入与快速部署，智能电网数据的安全性与实时性变得越来越重要，如何设计一种安全且高效的多维数据聚合方案是智能电网数据聚合的热点研究问题。

1.2 国内外研究现状

数据聚合一直被认为是可以解决智能电网隐私和数据处理问题的关键技术之一[16]。数据聚合以其可以显著降低智能电网通信过程中的通信负载，为系统提供丰富多样的聚合结果，是智能电网研究与应用的重要数据来源[17]。在聚合过程中，智能电表可以将采集的包含隐私和机密信息的实时数据通过掩蔽或加密等方法实现隐私保护。随着智能电网信息化的快速发展，攻击者为从电网中获利，利用各种各样的手段来监听、误报或分析用户的初始信息。因此，在数据聚合阶段如何降低数据聚合所占用的资源和确保用户信息在传输、聚合、分析阶段都不被泄露是当前国内外研究的热点。

现有智能电网数据聚合方案按其网络模型可以划分为三种：第一种是以传统的网络模型为基础，实现数据聚合隐私保护；第二种是以云计算为网络的核心的网络模型[18]-[19]，以此提升电网对大数据的收集和处理能力；第三种是以边缘计算，特别是雾计算概念为核心的网络模型[20]-[21]；其将系统中部分计算和存储压力分摊给雾节点，以降低系统延迟和提高智能电网数据处理效率。与前两种网络模型相比，第三种网络模型更适用于对网络带宽和时延有较高要求的智能电网，且能充分发挥网络边缘设备的计算和存储性能。

以雾计算为核心的网络模型所提出的数据聚合方案大致归为三类：第一类为使用假名/匿名的方式，将隐私信息保护起来，使除第三方可信机构的实体即使得到用电数据也无法与其发送者相匹配，进而实现用户的隐私保护；第二类是通过现有的密码学或物联网相关技术加密智能电表收集到的实时用电数据，来实现用户数据的隐私保护；密码学中最常见的加密方法是采用同态加密算法，其以高

效、机密性强等优点受到了许多研究者的青睐。常用的同态加密算法有 BGN（Boneh-Goh-Nissim）加密算法[22]-[23]、Paillier 加密算法[24]-[26]、ECC 加密算法[27]-[29]、ELGamal 加密算法[30]-[31]、RSA 加密算法[32]-[33]和格加密算法[34]等；第三类是将前两类的方法相结合，更全面的保护用户隐私信息。与先前文献相比计算、通信效率和延迟有了显著改善。但在雾层中，现有以雾计算为核心的网络模型所提出的数据聚合方案没有考虑利用多个节点来分配数据聚合的负载，存在容易产生单点故障问题。

从智能电网数据聚合方案中数据维度来看，目前已经提出了许多隐私保护数据聚合方案，但大都是针对低数据维度。Fan[35]将 BGN 加密算法和盲因子相结合，提出了可以实现用户的隐私和实现数据完整性的数据聚合方案，但该方案被证实存在安全漏洞，根本无法满足数据完整性要求。随后 He[36][37]先后提出类似的方案，既保护数据的完整性，也降低了计算成本。Hua[38]提出能抵御恶意数据挖掘攻击的数据聚合方案，而且能输出准确的聚合结果。HE[39]-[40]提出使用 Shamir 秘密共享，允许智能电表在没有可信第三方机构的情况下协商聚合参数，且能满足多功能聚合。Liu[41]提出不带可信第三方机构的实用隐私保护数据聚合方案，通过构造虚拟聚合区来保护单个用户的用电数据，且适合大规模应用。Erkin[42]将中国剩余定理与改进的同态加密相结合，实现了一个简单、高效的方案，该方案适用于动态智能电网环境。Gope[43]提出了一种基于屏蔽的空间数据聚合方案，使用轻量级加密原语，提高智能电网计算效率，此外，该方案提出了一种安全计费方案，实现动态计费。Gope[44]通过逐跳通信提出了一种高效的智能电网数据聚合方案。所提方案仅使用计算成本低的操作，例如散列操作。且该方案支持智能电网的动态计费。Shen[45]提出了一种雾计算中动态组的隐私保护方案，可以实现任何聚合函数的计算，有效防止恶意终端设备，雾节点或云服务器的串通，此外，该方案实现了终端设备的动态连接与退出。Huang[46]提出的数据聚合方案将轻微扰动技术与密码学技术结合起来，使其适用于硬件有限的设备，如智能电表。Li[47]为满足精细的智能电网控制中心需求，将多子集用电数据聚合成单个聚合值，同时引入可信第三方，使用 Paillier 同态加密保证个人隐私。Liu[48]提出一种支持聚合通信与函数查询的隐私保护方案，它支持服务提供商动态控制和分配电力。利用地理上分布的大规模雾节点和集中的云服务器来实现低延迟通信和电力数据存储。通过将加密的数据外包给云，该方案允许服务提供商对加密的使用数据启动各种功能查询，同时允许用户控制自己的数据。Hassan[49]基于分解技术和对称同态方案，提出了一种物联网隐私保护范围查询方案，实现高效范围查询。

随着智能电网发展，多维度的用电数据收集是智能电网对高精度、高效率控

制的必然要求。如何对多维度用电数据进行处理是智能电网数据聚合重要研究方向。2012 年，Lu[50]利用超递增序列批量压缩密文规模，对多维数据结构化处理。该方案还采用批量验证技术来降低认证成本。受此技术的影响，随后 Zuo[51]和 Ming[52]基于 ELGamal 加密算法的超递增序列技术分别提出了两种隐私保的多维数据聚合方案。与传统将每个维度数据分别加密处理的数据聚合方案相比，该方法可以显著降低计算成本。但每多一个维度的数据，智能电表需要多增加一个额外的指数运算，且上述方案不支持容错机制。Shen[53]和 Chen[54]使用霍纳规则将多维数据融入霍纳多项式的系数中，使用 Paillier 加密算法隐藏多项式，从而实现了多维数据聚合。但随着数据维度的增加，需要加入更多的霍纳多项式系数，这将导致计算成本与通信开销的剧增。与霍纳规则的方法相似，Hu[55]提出一个将多维数据嵌入到中国剩余定理公式中的多维数据聚合方案，但该方法效率并不高。Bo[56]提出了一种支持细粒度访问控制的多维数据聚合方案，采用扩展的 BGN 同态加密，将多维电力数据聚合成一个密文，此外该方案还支持细粒度的访问控制。Boudia[57]提出一种使用编码函数来结构化数据的多维数据聚合方案 ESMA。ESMA 还可以适用于其他查询，而不是数据的数值之和，该方案还支持容错。然而，该方案仅支持一些简单的查询，且对智能电表与雾节点的计算能力有较高的要求。

综上所述，许多研究人员对智能电网数据聚合问题进行了深远的研究，并提出了许多具有代表性的研究成果。然而由于智能电网的复杂性以及智能电网对于数据安全、网络功能以及运行效率等方面需求越来越高，现有的工作仍有待进一步改进与完善的地方。对上述智能电网数据聚合方案存在的问题做出如下简要总结：

（1）上述基于雾计算的智能电网数据聚合方案存在容易产生单点故障的问题。

（2）上述智能电网多维数据聚合方案存在计算成本高及通信开销大的问题。

1.3 论文特色与创新

本文主要特色与创新点包括以下方面：

（1）针对上述智能电网数据聚合方案中容易产生单点故障的风险，影响数据安全聚合的问题，基于含有雾群的雾计算智能电网系统模型，设计了一种雾节点分配策略。将一个含有多个雾节点的雾群对应多个智能电表子区域，使用动态优先级方法分配雾群中雾节点进行数据聚合工作，以降低单点故障风险。进而提出了一种隐私保护多维数据聚合方案，支持智能电表一次向控制中心报告多种类型的数据，实现多维数据高效处理。

（2）为降低上述多维数据聚合方案的计算成本和通信开销，提出一种无可信机构的智能电网高效多维数据聚合方案，既减少通信链路，同时保证数据聚合的安全性。具体来说，该方案采用基于雾计算的智能电网模型，使中间层雾节点定期收集智能电网采集的实时数据，并生成细粒度的聚合报告，能有效降低通信开销；同时，本方案采用椭圆曲线加密机制，支持不依赖可信机构数据加密，降低因密钥分发而产生的大量通信开销；再者，使用批量验证的双线性配对技术实现高效身份验证。

1.4 论文结构安排

本论文整体结构安排如图 1-1 所示：

第 1 章 论述研究背景和意义，通过国内外研究现状指出当前研究中存在的问题，最后说明本文的特色与创新点以及论文整体结构安排；

第 2 章 介绍相关理论与技术，其中包括雾计算、智能电网网络模型和密码学相关技术；

第 3 章 针对单点故障的智能电网多维数据聚合；

第 4 章 无可信机构的智能电网高效多维数据聚合；

第 5 章 总结与展望。

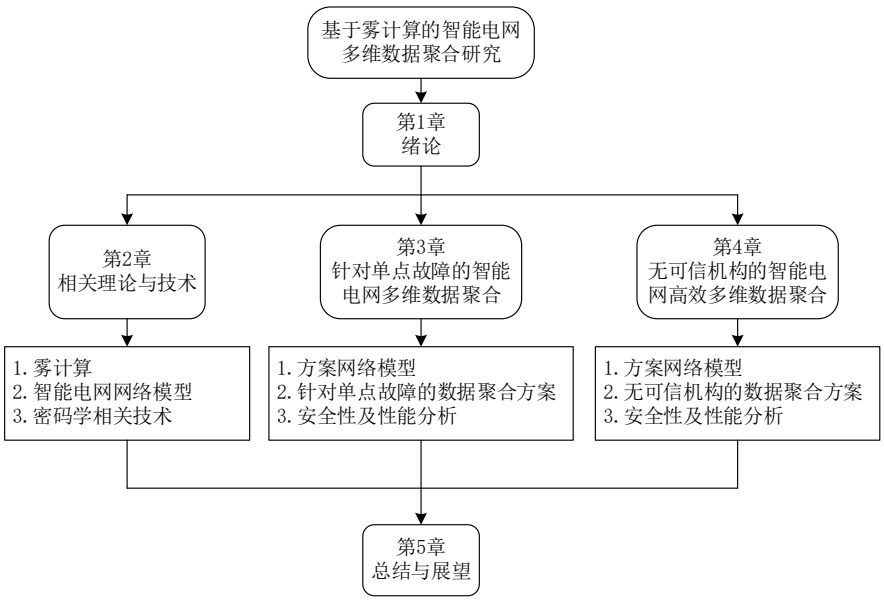

图 1-1　本论文整体结构安排

第2章 相关理论与技术

在本章，我们将介绍本论文相关的理论与技术方面的知识，其中包括雾计算、智能电网网络模型和密码学相关技术。

2.1 雾计算

2.1.1 雾计算概述

物联网的火热研究使公众的注意力转移到去中心化的计算范式上来。由此，边缘计算应运而生，其主要思想是将部分计算、存储和控制功能从云中心转移到更靠近终端用户的雾节点上来，以减轻网络中由大量数据产生的高带宽，高延迟的压力。如今，已提出了边缘计算原理的几种实现方式，其中包括：移动云计算、小云计算、移动边缘计算。

在这种边缘计算竞争中，雾计算脱颖而出，代表了边缘计算思想最先进的形态。事实上，雾计算旨在代表一个完整的架构，该架构沿着云到物的连续体水平和垂直分布资源[58]。因此，它不仅仅是云的扩展，而是与云和物联网交互的新角色，以协助和增强它们的交互。

边缘计算仅利用边缘资源，而雾计算同时利用边缘和云资源。考虑到雾计算的潜力，物联网设备可以通过根据其对服务质量要求将所有或者部分应用程序分摊到雾或云服务器来执行资源匮乏或延迟敏感的应用程序，并提高服务质量。它还可以减少云服务器的拥塞，因为分布式雾服务器可以减轻云服务器来自物联网设备的传入数据处理和存储的负担。

2.1.2 雾计算特点

雾计算的主要特点可以概述为：

（1）认知：雾计算意识到以客户为中心。了解客户需求的雾体系结构可以更好地确定在云到物的连续体中在何处执行计算、存储和控制功能。雾计算中的雾节点更靠近终端用户，可以更细致的获得用户的状态信息与满足用户个性化的需求[60]。

（2）高效：雾计算可以从云一直到终端连续不断的提供各种资源。雾计算可以将计算、存储和控制功能分布在云和端点之间的任何位置，以充分利用这一连续体上可用的资源。它还允许应用程序利用网络边缘和终端用户设备（如平板电脑、笔记本电脑、智能家用电器、连接的车辆、火车以及位于网络边缘小型服务器）上大量可用的闲置计算、存储和通信资源。雾与端点的距离更近，这使其

与终端用户系统联系密切，能提高系统的整体效率和性能。这对于性能关键的网络物理系统尤为重要。

（3）敏捷性：云提供商提供服务通常需要一定的时间与成本，导致新服务的开发通常缓慢且昂贵。雾计算可以更简单的为独立个体和小型团队提供一个应用服务，用户使用开放式应用程序编程接口、开放式软件开发工具包和移动设备的激增来创新、开发、部署和运营新服务。

（4）低延迟：雾计算不仅能对网络终端产生的实时数据进行一系列的分析，而且对于本地网络物理系统的时间控制更敏感。这不仅适用于对于延迟要求高的控制系统，而且对于需要更快反应的嵌入式 AI 的部署与应用至关重要。

（5）效率：雾模型支持在云和物联网之间的任何地方汇集计算、通信、控制和存储功能。基于雾模型的基础设施从云端“推送”功能并从强大的物联网设备“拉取”功能，将它们集成到基于雾模型的基础设施中，提高整体系统性能和效率。

2.1.3 雾计算的安全和隐私问题

在未来十年中，雾计算最基本的问题是沿着从云到物的连续体分布在哪里、何时以及如何将计算、通信、控制和存储。

随着人们安全和隐私保护意识的增强，安全和隐私越来越受到人们的重视。鉴于它与边缘计算的相关性，雾中的许多挑战与边缘计算面临的安全挑战相似[61]。当前雾计算的安全和隐私问题主要有以下几个方面：

（1）身份隐私：雾计算中存在大量分布式设备，不同设备之间的交互也会越来越多，如何实现雾节点中各种设备的相互协作，如何进行身份隐私保护是实现雾计算安全的第一步安全措施。

（2）数据隐私：与云计算相比，雾计算中覆盖了无数终端设备，使得其更容易收集到用户的隐私数据。此外，终端设备的收集到的数据都需要上传到近端雾节点或者远端云服务器上处理，这使得数据暴露的可能性增大。

（3）位置隐私：收集位置信息更适合雾计算分布式的应用场景。终端设备使用靠近边缘节点资源时，很容易被雾节点根据使用资源情况推测出边缘设备的地理位置信息[62]。位置隐私对于确保用户安全来说十分重要。

2.2 智能电网网络模型

2.2.1 传统智能电网网络模型

智能电网有四个主要阶段，发电、输电、配电和消费。在这个过程中，市场、

运营商以及服务提供商通过安全通信接口参与整个过程，从而实现整个智能电网通信交流，如图 2-1 所示。

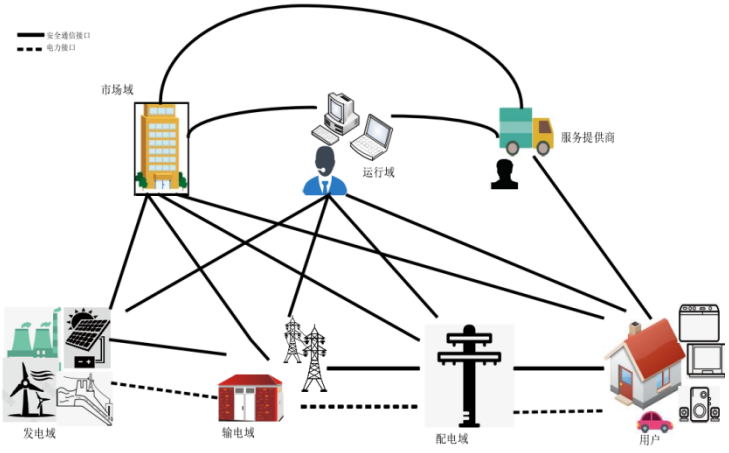

图 2-1　传统智能电网模型

智能电网模型包括三个部分即家庭区域网（HAN）、建筑区域网（BAN）以及领域区域网（NAN）。智能电网包含两种通信类型：局域网络(LAN)和广域网(WAN)。局域网络将屋内的智能设备连接起来，从而形成一个小型网络，其可以通过多种方式进行通信互联[63]。另一方面，广域网是一个天文数字般的巨大网络，它连接着仪表、住宿供应商和电力设施。广域网可以利用 WiMAX、5G/GSM/LTE 或光纤进行通信。智能电表充当内部设备和外部各方之间的门户，提供其所需的信息。电力公司管理着智能电网中的能量分配，从智能电表中按分/小时收集电力实时数据，并在需要时向智能电表发送通知[64]。网关接收来自局域网络内部设备的信息，并将其发送到合适的接收者。图 2-2 显示了智能电网的基本架构。

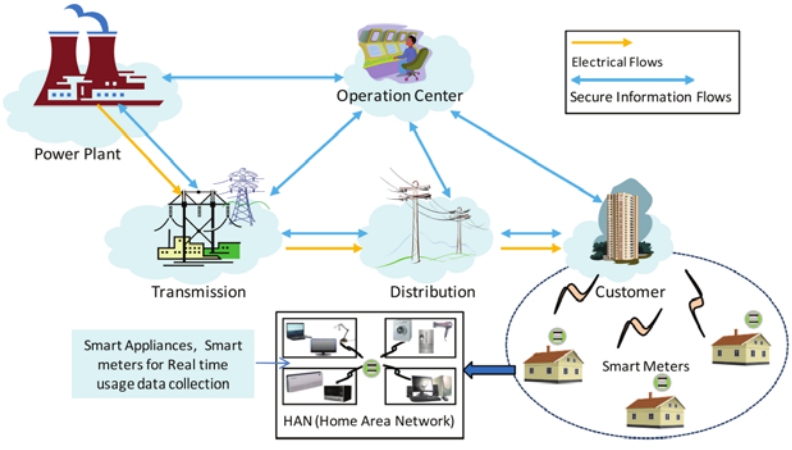

图 2-2　智能电网基本架构

2.2.2　基于云计算的智能电网模型

云计算是一种基于互联网的计算模式，通过共享资源，软件和信息按需提供给计算机和其他设备，如电网。云计算为未来电力系统的巨大计算资源池和存储需求提供了答案。云计算因其在按需自助服务、无处不在的网络访问和与位置无关的资源池方面的主要优势而被认为是下一代计算范式[65]。

基于云计算的智能电网模型如图2-3所示。图2-3中，红色箭头代表能量流的传输，蓝色虚线代表信息流的传输。在该模型中，由能源提供者为所有实体提供其所需的能量。工业用户、商业用户及住宅用户通过智能电表加密数据，并上传至基于云的服务器。利用云计算的集中式处理优势，以降低处理数据所需的成本，提高效率。

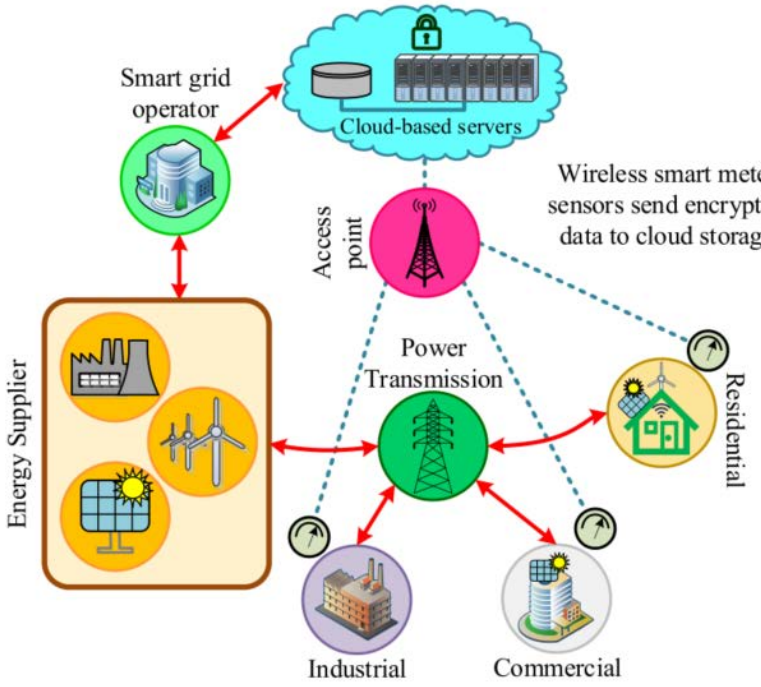

图 2-3　基于云计算的智能电网模型

2.2.3　基于雾计算的智能电网模型

随着网络边缘产生的数据量的增加，给云计算系统的网络带宽和数据传输效率提出了更高的要求。与此同时，现实世界的物联网应用对智能设备提出了更高的要求。一个公开的挑战是如何提高各个环节与云之间的通信效率[66]。遗憾的是，传统的云计算模式对于这些问题有些束手无策，而且云服务也引起了对安全性和隐私的关注。

雾计算通过支持密集分布的数据源，为实时大规模数据分析奠定了良好的基础，并提供卓越的用户体验[67]。雾节点可以是 Intel Edison、Raspberry Pi、Arduino Uno 和一些其他的微控制器板。设想一个智能计量的三级网络模型，如图 2-4 所

示。底层有大量智能电表，中层有雾节点，顶层有云服务器。其设计主要目的是通过利用雾层降低因大量数据传输造成的高带宽与高延迟。因此，雾节点可以通过各种通信机制（如 Wi-Fi、蓝牙、ZigBee、蜂窝网络等）处理/聚合来自附近终端设备的数据，并将结果转发到远程云服务器。由于智能电网对于数据的实时性要求较高，因此基于雾计算的智能电网模型更适于实际应用。

由于所有的测量数据从终端节点传输到远程云服务器的代价要比转发到附近的雾节点的代价高得多，因此可以有效地利用雾节点提供更好的服务。此外，考虑到远程云中心只关心其覆盖范围内的整体的电力数据消耗情况，所以单个终端节点可以将测量的实时数据发送给每个地区附近的雾节点，雾节点对实时的测量数据进行初步处理，然后中间层的雾节点将聚合值转发给云，以节省能源消耗。

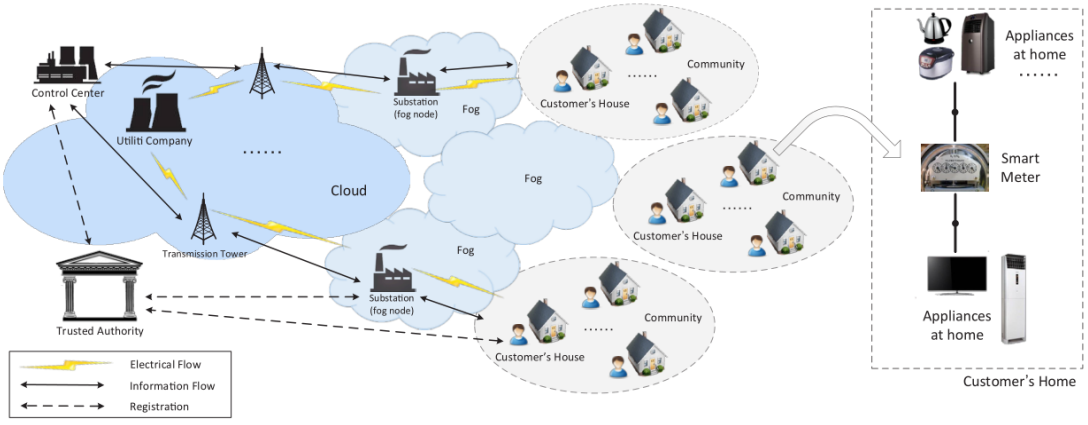

图 2-4　基于雾计算的智能电网模型

2.3　密码学相关技术

2.3.1　Paillier 加密算法

Paillier 加密是一种用于公钥加密的非对称算法。Paillier 加密算法是一种加性同态加密，由公式（2-1）描述，其中 $E(\ )$ 是一个加密函数，$k1$ 是加密密钥，a,b 是两个随机消息。

$$E_{k1}(a)\cdot E_{k1}(b)=E_{k1}(a+b) \tag{2-1}$$

A．密钥生成

给定一个安全参数 k，密钥生成算法会生成两个大素数 p_1,q_1，其中 $|p_1|=|q_1|=k/2$。计算另一个大数 $n=p_1q_1$，$\lambda=lcm(p_1-1,q_1-1)$ 和 $\mu=\left(L\left(g^{\lambda}\bmod n^2\right)\right)^{-1}\bmod n$，其中，$lcm(\bullet)$ 是求最小公倍数操作。然后计算生成 $g\in Z_{n^2}^{*}$ 和 $\gcd\left(L\left(g^{\lambda}\bmod n^2\right),n\right)=1$，其中 $L(u)=u-1/n$。公钥为 (n,g)，私钥为 (λ,μ)。

B．加密

设数据信息为一个整数集$\{0,1,\ldots,n^2-1\}$。为了加密数据信息m，选择一个随机数$r \leftarrow Z_n^*$和计算密文：$c = g^m r^n \bmod n^2$。

C．解密

给定密文$c = g^m r^n \bmod n^2$和私钥(λ,μ)。很容易获得：$m = L\left(c^{\lambda \bmod n^2}\right)\mu \bmod n$。

2.3.2 椭圆曲线加密算法

虽然在数学领域的研究，椭圆曲线已有一百多年的历史，但是椭圆曲线加密在 1985 年才首次引入[68]。ECC 以其高安全性、密钥长度小及速度快等特点，迅速收到了人们的热捧。椭圆曲线安全性是由椭圆曲线离散对数问题（ECDLP）的难解性决定的。根据选择不同椭圆曲线的安全特性，决定 ECC 的安全性。ECC 可以采用不同安全等级、密钥长度及性能的椭圆曲线来满足各种不同的需求。ECC 更适用于网络边缘上一些资源受限的智能设备。椭圆曲线加密过程如图 2-5 所示。

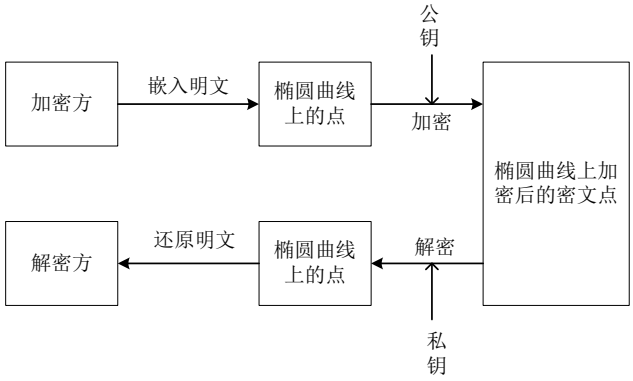

图 2-5　椭圆曲线加密过程

2.3.3 消息认证码

现代信息通信网络在消息传递时，通常需要一种用于防止消息内容被篡改的签名认证技术。消息认证码具有安全性较好和计算成本小的特点，被广泛应用于网络系统中。在消息传递时，发送方将消息认证码附带在发送的消息中，接收方通过检查使用共享密钥生成的消息认证码与接收到的消息认证码是否相等，来确定该消息是否被篡改。在共享密钥没有被泄露的情况下，如果没有接收双方约定的共享密钥，任何第三方都无法从消息认证码中获取加密的消息。因此，消息认证码也可以验证消息来源的真实性。

2.3.4 双线性映射

设G, G_T是同一素数阶q的两个循环乘法群，P 是群G的生成元，假设G和G_T

配对，$e:G\times G\to G_T$，其中$e(P,P)\neq 1$且$e(aP_1,bQ_1)=e(P_1,Q_1)^{ab}\in G_T$，并且其中的元素满足$a,b\in Z_q^*$；$P_1,Q_1\in G$。

（1）双线性性：$\forall g_1\in G,\forall g_2\in G$和$\forall a,b\in Z_N$，$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

（2）非退化性：$\exists g_1\in G$和$\exists g_2\in G_1$，当且仅当$e(g_1,g_2)\neq 1_{G_T}$。

（3）可计算性：$\forall g_1\in G_1$，$\forall g_2\in G$，$e(g_1,g_2)$是可计算的。

2.4 本章小结

本章节主要阐述了本论文涉及的相关背景技术基础理论，包括雾计算、智能电网系统模型和密码学相关技术。首先对雾计算的相关概念、特点和存在的安全和隐私问题进行阐述，其次，对三种智能电网系统模型的概念、组成和特点进行介绍；最后对本论文所涉及的密码学相关技术进行逐一介绍。

第3章 针对单点故障的智能电网多维数据聚合研究

3.1 引言

智能电网是电力工业发展的方向和趋势，它利用物联网的信息和通信技术，实现了电力系统各个环节之间的信息通信。智能电网不仅通过有线/无线网络在各种智能终端设备之间传输数据，还通过互联的云服务器进行数据分析和决策。智能电网根据大量的实时数据和分析模型，可以为电网提供更加智能化的应用。智能电网的快速发展给电力系统产生了大量数据处理开销。数据聚合以降低智能电网传输成本、数据存储成本、数据冗余，同时提高数据分析速度和计算效率受到了人们的青睐。电力供应商将智能电表数据聚合，提高电网基础设施的整体效率和可靠性。然而，有许多因素制约着智能电网的发展。其中一个主要的问题就是数据隐私和安全。在智能电网中，数据所有者担心从智能电表收集的数据信息在数据传输过程中被不法分子窃取，从而引发消费者隐私问题，如暴露消费者的活动规律和对消费者位置跟踪等。

许多研究人员提出了很多相应的解决方法，许多方案实现数据聚合的同时保护了网络内部各实体和运营商的数据隐私，有效抵御外部窃听者。然而，大多数方案以昂贵的计算代价来实现隐私保护，且只适用一维数据。在实际应用中，智能电表通常需要采集多维数据（即多种类型数据，如温度，湿度，位置信息等），以满足智能电网在不同应用中的需求。为实现多维数据聚合，一些方案也被相继提出。虽然它们在一定程度上实现了多维数据的隐私保护，然而，随着电网数据的数量、种类、维度的增加，对传统智能电网云服务器模型造成大量计算负担，可能导致高延迟、低可靠性及可扩展性低的问题。

2012 年，思科研究人员提出了雾计算模式的概念。雾计算将云计算和部分存储功能从云数据中心部分转移到更靠近终端设备的边缘。雾计算较于边缘计算，因其在端与云的连通道路上提供连续化的服务，更契合智能电网的结构特点，受到了极大关注。引入中间雾节点，利用其通信、计算和存储方面的能力，减轻云服务器传输和处理的数据负载，解决传统智能电网框架中云中心可能出现的延迟和带宽问题。

尽管雾计算在数据聚合期间提供了许多帮助，但仍存在容易产生单点故障风险，影响数据安全聚合的问题。因此，我们基于含有雾群的智能电网模型，设计一个雾节点分配策略来降低单点故障风险，以实现高效、安全的数据聚合。具体贡献如下：

（1）基于含有雾群的雾计算智能电网系统模型，设计了一种雾节点分配策

略，使用动态优先级方法分配雾群中雾节点进行数据聚合工作，以降低单点故障风险。

（2）提出了一种基于雾计算的智能电网多维数据聚合方案，支持智能电表一次向控制中心报告多种类型的数据，实现数据高效处理。

（3）通过安全分析表明本方案的安全性。性能分析显示，本方案与其它方案相比在计算成本方面具有优势。

3.2 网络模型

3.2.1 系统模型

本文充分利用雾节点计算资源，构建了一个三级智能电网模型，如图 3-1 所示。第一层为设备层（Device Layer），包含若干个由智能电表（Smart Meter）组成的智能电表子区域；第二层为雾层（Fog Layer），由若干个雾群（Fog Group）组成；第三层为控制中心（Control Center）。此外还有一个实体—可信机构（Trust Authority）负责密钥参数产生、分发和各实体的注册。

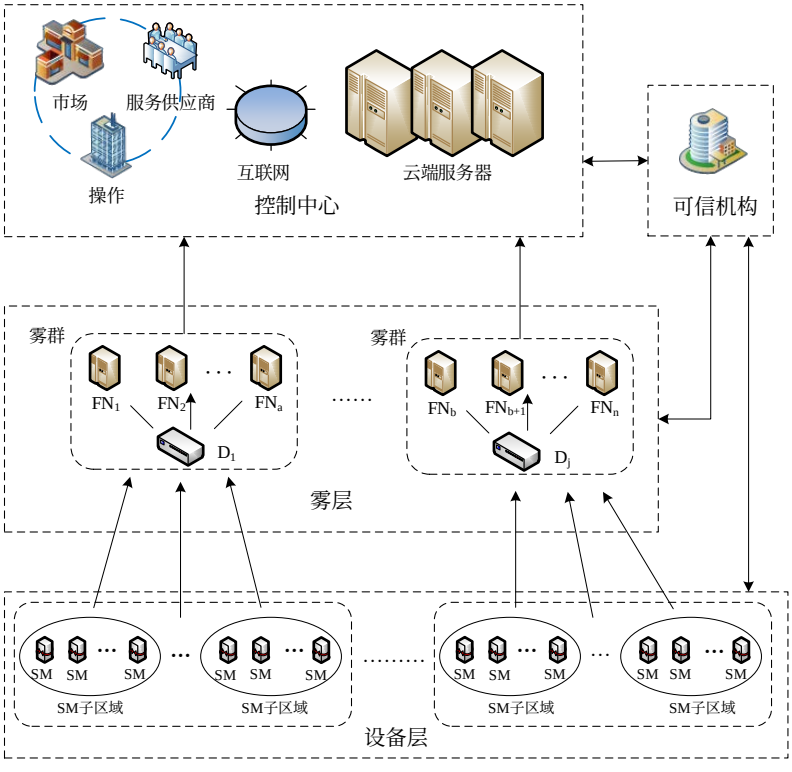

图 3-1　系统模型

（1）可信机构（TA）：可信机构是可信的第三方，其职责是引导系统、管理密钥并为所有智能电表、雾节点和控制中心分配密钥和负责智能电表、雾节点和控制中心的注册。

（2）控制中心（CC）：控制中心通过雾节点（Fog Node）接收所有智能电表数据后，进行多样化的数据分析，以满足智能电网不同需求。

（3）雾层：根据地理位置的不同，将雾节点（FN）分为若干个雾群。每个雾群（FG）中设置一个用于调用雾节点的分配器（Distributor）。分配器（D）按照雾节点分配策略，调用雾节点处理每个智能电表子区域所上传的数据，并发送聚合报告给控制中心。

（4）设备层：设备层中存在大量计算和存储资源受限的智能电表（SM）。由于智能电表位置不同，我们自然地将智能电表分成若干个智能电表子区域。SM 将采集到的实时多维电力数据，进行初步处理后发送给相应的雾群，等待雾群的处理。

雾群分类规则：

规则 1：SM 子区域与分配器在空间上距离很近。

规则 2：基于规则 1，分配器的最短距离内有且不止有一个具有计算资源的雾节点 FN。

3.2.2 问题陈述

假设系统包含一个控制中心和 J 个雾群，每个雾群中含有若干个雾节点和 1 个分配器。单个雾群接收设备层中若干个 SM 子区域内智能电表上传的数据。每次时间间隙，SM 子区域内智能电表上传的数据报告数量是固定且不重复的。

图 3-1 中箭头表示数据流的方向。智能电网产生的多维数据由智能电表负责采集、加密并上传至所属雾群；由雾群中分配器负责分配雾节点的数据聚合任务，并由雾节点将聚合结果上传给控制中心；最后，由控制中心对聚合结果进行解析。

一般来说，负责对智能电表子区域上传数据进行数据聚合的雾节点是固定的。一旦相应雾节点发生故障，例如雾节点数据受到外部攻击者窃听、雾节点与其它实体长时间共谋、恶意雾节点向控制中心发送错误报告等情况，若无法及时发现并解决，将影响相应 SM 子区域安全数据聚合，对智能电网安全运行造成严重威胁。为此，我们在数据聚合方案中设计一种雾节点分配策略用于降低单点故障风险。

3.2.3 安全模型

在本方案中，TA 和分配器为可信任的，控制中心、雾节点和智能电表都是诚实但好奇的，即它们诚实地执行协议，但试图揭露其它实体的隐私。对于智能电表上传的敏感数据，有以下安全要求：

（1）隐私保护：即使攻击者在数据传输过程中截取了传输消息，攻击者得

到的也只是用电数据的密文，无法获得用户的数据明文。此外，方案还需要确保单个用户的数据在雾层和控制中心处理时不会泄露。

（2）源认证：源认证保证了控制中心和雾节点接收到的消息来源于合法的智能电表或雾节点。任何非法的消息报告都会被雾节点或控制中心过滤。任何修改的消息都会被检测出来。

（3）数据完整性：数据完整性能抵御许多对消息的攻击，如篡改攻击，虚假数据注入攻击等。

（4）抵御单点故障：即使发生单点故障，系统也能最大程度保障受单点故障影响的 SM 子区域正常数据聚合过程。

3.3 方案设计

根据网络模型，本节提出一种针对单点故障的智能电网多维数据聚合方案，该方案由系统初始化、注册、智能电表数据采集、雾节点分配、数据聚合及聚合数据解密 6 个部分组成。为了更好的描述，表 3-1 将列出本章使用的相关符号及意义。

表 3-1　相关符号及意义

符号	表示的意义
(n, g)	Paillier 加密公钥
(λ, μ)	Paillier 加密私钥
r_{ij}	用于加密的随机数
s_{ij}	附加秘密参数
s_j	附加秘密参数之和
w_1	智能电表子区域内智能电表的数量
w_2	控制中心覆盖范围内雾节点数量
h	安全的哈希函数
sk_{ij}	智能电表与雾节点之间的共享密钥
pk_j	雾节点与控制中心之间的共享密钥
m_{ik}	智能电表采集到的 k 维用电数据
k	数据类型的数量

3.3.1 系统初始化

对于基于雾计算的智能电网系统，可信机构 TA 协助整个系统运行并负责系统参数生成。具体步骤如下：

步骤 1：TA 首先选择两个随机且独立的大素数 p 和 q，计算 $n=p\cdot q$ 作为同态加密的公钥，同时定义函数 $L(x)=(x-1)/n$。计算 $\lambda=lcm(p-1,q-1)$，$\mu=\left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod \mathrm{n}$，其中 $g\in Z_{n^2}^{*}$，保证 $\gcd\left(L\left(g^{\lambda} \bmod n^2\right),n\right)=1$。由此获得 Paillier 同态加密的公钥 (n,g)，私钥 (λ,μ)。TA 选择一个用于加密的随机数 $r_{ij}\in Z_n^{*}$。

步骤 2：TA 使用伪随机数生成器生成 $w_1\cdot w_2$ 个附加秘密参数 $s_{ij}\in Z_n^{*}$，（$i=1,\ldots,w_1, j=1,\ldots,w_2$），并且计算 s_j：

$$s_j=\sum_{i=1}^{w_1} s_{ij} \bmod n \tag{3-1}$$

步骤 3：TA 选择一个安全的加密哈希函数：$h:\{0,1\}^{*}\rightarrow\{0,1\}^{h}$。

步骤 4：TA 生成智能电表和雾节点之间用于签名验证的共享密钥 sk_{ij} 以及雾节点和控制中心之间用于签名验证的共享密钥 pk_j。

3.3.2 注册

所有的 SM_{ij}，FN_j，CC 都需要向 TA 进行注册，我们对此阶段说明如下：

SM_{ij} 注册：SM_{ij}（$i\in\{1,2,\ldots,w_1\}$）通过安全信道向 TA 发送注册信息 m_{ij}（注册信息包含智能电表 ID，用户信息，位置信息等），TA 为 SM_{ij} 选择一个身份 id_{ij}，TA 发送 $\{r_{ij},g,sk_{ij},id_{ij},s_{ij}\}$ 给 SM_{ij}。

FN_j 注册：FN_j（$j\in\{1,2,\ldots,w_2\}$）通过安全信道向 TA 发送注册信息 m_j（注册信息包含雾节点 ID，用户信息，位置信息等），TA 为 FN_j 选择一个身份 id_j，TA 发送 $\{pk_j,id_j\}$ 给 FN_j。

CC 注册：CC 首先选择一个身份 ID_{cc}。然后，TA 发送 $\{\lambda,\mu,pk_j,s_j\}$ 给 CC。

在上述 SM_{ij}，FN_j，CC 注册之后，TA 发送共享密钥 $\{sk_{ij}\}$ 给分配器 D_j 并公布系统参数 $\{n,h\}$。

3.3.3 智能电表数据采集

用户的用电信息会定期向 FN 报告，例如每 15 分钟报告一次。为了保护用户隐私，智能电表需要加密此类隐私信息。每个智能电表 SM_{ij} 对采集到的 k 种类型用电数据 $(m_{i1},m_{i2},\cdots,m_{ik})$ 初步处理，具体步骤如下：

步骤 1：将 k 种类型的电力数据编码为：

$$d_{ix}=(m_{ix})_2 \,\|\, 0^{\alpha}, x=1,\ldots,k \tag{3-2}$$

式（3-2）中：$\alpha=\left(\left[\log_2\left(w_1\right)\right]+z\right)\cdot\left(x-1\right)$。$z$ 表示一种数据类型 m 的最大位数。

编码后，SM_{ij} 计算 D_{ij}：

$$D_{ij}=\sum_{j=1}^{k}d_{ix} \tag{3-3}$$

并加入附加秘密参数 s_{ij}：

$$M_{ij}=D_{ij}+s_{ij}\bmod n \tag{3-4}$$

步骤 2：SM_{ij} 将编码后的电力数据 D_{ij}，使用公钥 $\left(n,g\right)$，运行 Paillier 同态加密算法得到：

$$C_{ij}=g^{M_{ij}}\cdot r_{ij}^{n}\bmod n^2 \tag{3-5}$$

步骤 3：SM_{ij} 使用共享密钥 sk_{ij} 生成密文签名：

$$\sigma_{ij}=h\left(C_{ij}\parallel id_{ij}\parallel T_p\right)^{sk_{ij}} \tag{3-6}$$

式（3-6）中 T_p 表示当前时间戳，能有效防止重放攻击。

步骤 4：SM_{ij} 发送包含 $\left\{C_{ij},id_{ij},T_p,\sigma_{ij}\right\}$ 报告给相应的雾群。

3.3.4 雾节点分配

受文献[69]启发，根据动态优先级调度算法思想，设计一种雾节点分配策略，如图 3-2 所示。根据分配策略，分配器将各个 SM 子区域上传的消息报告分配给雾群中雾节点处理，避免单一雾节点长期负责某个 SM 子区域的数据聚合工作，降低雾节点单点故障的风险。具体分配策略如下：

步骤 1：雾节点优先级初始化：对雾群中空闲的雾节点 $\left\{FN_q\right\}$（$q\in\left\{1,2,\cdots,m\right\}$），分配器用随机数产生 FN 优先级，并按优先级大小生成就绪队列 $PList=\left\{p_j\right\}$，p_j 表示 FN_q 的优先级，$p_j\geq 0$（优先级数值越大，优先级越高）。

步骤 2：分配器接收到某个 SM 子区域发送的消息报告。

步骤 3：分配器判断该消息报告所属 SM 子区域是否安排 FN。如果否，分配器转入步骤 4。如果是，分配器转入步骤 5。

步骤 4：分配器按优先级选择最大优先级雾节点 FN_i。分配器发送该 SM 子区域对应的共享密钥 $\left\{sk_{ij}\right\}$ 给 FN_i，就绪队列 FN 优先级 p_j+1。

步骤 5：FN_i 继续接收该子区域中所有 SM 消息报告。

步骤 6：判断是否有 SM 上传消息报告。如果否，结束。如果是，转入步骤

7。

步骤 7：FN_i 任务执行结束后，判断 FN_i 是否收到投诉消息，如果是，FN_i 优先级 p_i=0，如果否，FN_i 优先级 $p_i = p_i - 3$。

步骤 8：FN_i 按优先级 p_i 大小插入就绪队列 $PList$。转入步骤 3。

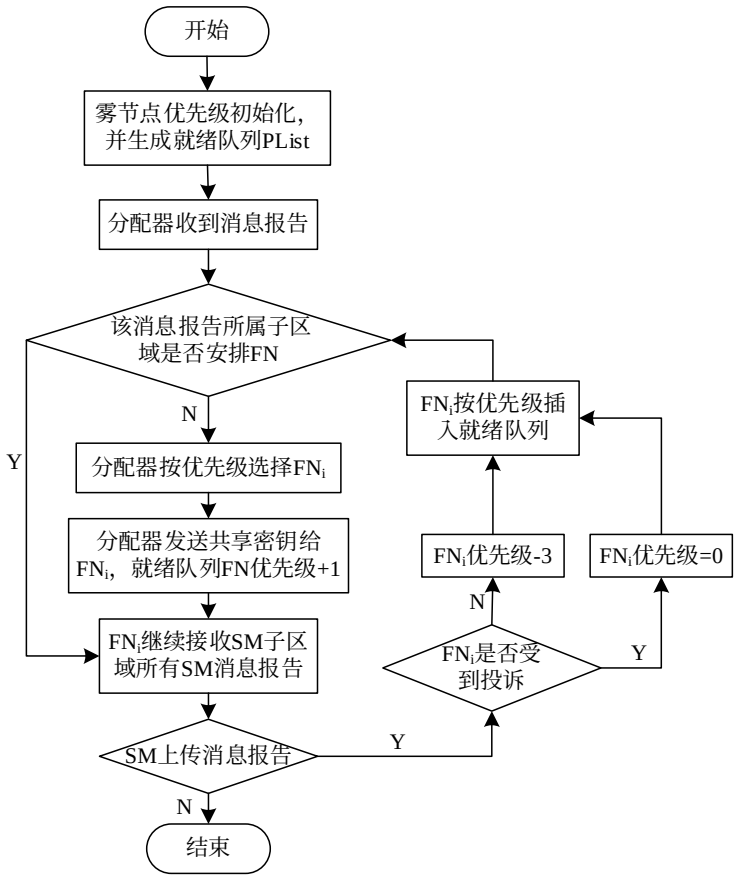

图 3-2　雾节点分配策略流程图

3.3.5　数据聚合

当 FN_j 接收到分配器分配的报告后，FN_j 具体操作步骤如下：

步骤 1：FN_j 首先检查报告的当前时间戳 T_p 和身份 id_{ij}，FN_j 验证密文签名。如：

$$\sigma_{ij} = \sigma'_{ij} = h\left(C_{ij} \| id_{ij} \| T_p\right)^{sk_{ij}} \tag{3-7}$$

如时间戳、身份及签名三者都正确则继续下一步，如错误则拒绝接收。以这种方式，FN 可以确保接收到隐私数据密文来源的可靠性，同时过滤掉外部攻击者的注入的错误数据。

步骤 2：FN_j 聚合加密的密文：

$$
\begin{aligned}
C_j &= \prod_{i=1}^{w_1} C_{ij} \bmod n^2 \\
&= \prod_{i=1}^{w_1} g^{M_{ij}} \cdot r_{ij}^n \bmod n^2 \\
&= g^{\sum_{i=1}^{w_1} M_{ij}} \cdot \left(\prod_{i=1}^{w_1} r_{ij} \right)^n \bmod n^2 \\
&= g^{\sum_{i=1}^{w_1} (D_{ij} + s_{ij}) \bmod n} \cdot \left(\prod_{i=1}^{w_1} r_{ij} \right)^n \bmod n^2
\end{aligned}
\tag{3-8}
$$

式（3-8）中，w_1 表示 SM 子区域内智能电表的数量。

步骤 3：FN_j 使用共享密钥 pk_j 生成聚合签名：

$$
\sigma_j = h\left(C_j \| id_j \| T_p\right)^{pk_j} \tag{3-9}
$$

步骤 4：FN_j 生成聚合报告 $\left\{C_j, id_j, T_p, \sigma_j\right\}$ 发送给控制中心。

3.3.6 聚合数据解密

控制中心接收到来自雾节点 FN_j 发送的聚合报告后，将进行以下操作：

步骤 1：控制中心检查聚合报告的时间戳 T_p 和身份 id_j，并验证聚合签名：

$$
\sigma_j = \sigma_j' = h\left(C_j \| id_j \| T_p\right)^{pk_j} \tag{3-10}
$$

如时间戳、身份及聚合签名三者都正确则继续下一步，如错误则拒绝接收该聚合报告，并向分配器发送雾节点投诉消息 $\left\{id_j, T_p\right\}$。在雾节点分配时，分配器将大幅降低受到反馈的恶意雾节点优先级，既给系统足够时间检查该雾节点，又避免当出现大量数据负载时，雾节点资源不足而造成的长时间延迟。

步骤 2：CC 生成保护隐私的聚合报告：

$$
\begin{aligned}
C &= \prod_{j=1}^{w_2} C_j \bmod n^2 \\
&= \prod_{j=1}^{w_2} \left(\prod_{i=1}^{w_1} C_{ij} \bmod n^2 \right) \\
&= \prod_{j=1}^{w_2} \left(\prod_{i=1}^{w_1} g^{M_{ij}} \cdot r_{ij}^n \bmod n^2 \right)
\end{aligned}
\tag{3-11}
$$

式（3-11）中，w_2 表示控制中心覆盖范围内雾节点数量。

并将聚合报告存储在云服务器中。

步骤 3：控制中心 CC 解密聚合密文 C_j，恢复聚合数据：

令 $M=\sum_{i=1}^{w_1}\left(D_{ij}+s_{ij}\right)\bmod n$，$R=\prod_{i=1}^{w_1}r_{ij}$，由式（3-8）得：

$$C_j=g^M\cdot R^n \bmod n^2 \tag{3-12}$$

控制中心使用私钥(λ,μ)恢复M：

$$M=L\left(C_j^{\lambda} \bmod n^2\right)\mu \bmod n \tag{3-13}$$

解密后控制中心使用s_j获得：

$$\sum_{i=1}^{w_1}D_{ij}=M-s_j \bmod n \tag{3-14}$$

步骤 4：控制中心使用解码函数恢复每个聚合数据$\sum_{i=1}^{l}d_{ik}$。CC 将二进制表示的$\sum_{i=1}^{w_1}D_{ij}$分为l个字节块，每个字节块的长度为$\left(\left[\log_2\left(w_1\right)\right]+z\right)$。由此，第一个字节块最低有效位对应于聚合结果$\sum_{i=1}^{l}m_{i1}$，依次类推。控制中心可以恢复每个类型的聚合数据：

$$\left(\sum_{i=1}^{w_1}D_{ij}\right)=\sum_{i=1}^{w_1}m_{il}\left\|\cdots\cdots\right\|\sum_{i=1}^{w_1}m_{i2}\left\|\sum_{i=1}^{w_1}m_{i1}\right.\right. \tag{3-15}$$

3.4 安全性分析

在本节中，讨论了本方案的安全性，以说明本方案如何实现数据隐私、认证、数据完整性及降低单点故障风险：

（1）数据隐私

为了避免 SM 的用电消费数据遭到泄露，我们主要考虑外部攻击和内部攻击。

首先，我们假定外部攻击者能够通过公共信道获取 SM 发送的消息，并且获取密文C_{ij}，其中密文形式$C_{ij}=g^{M_{ij}}\cdot r_{ij}^n \bmod n^2$。为了获取明文$M_{ij}$，攻击者将对密文进行解密。然而，在 IND-CPA（不区分选择明文攻击）模型下 Paillier 加密方案具有语义安全性[21]。这意味着没有解密的私钥，任何对手都无法获取明文。

其次，我们假定内部攻击者通过 CC 和 FN 共谋以获取 SM 用电消费数据。同样，为了获取明文，攻击者必须对密文C_{ij}进行解密。虽然 CC 拥有私钥，可以很轻易破解密文C_{ij}，解密获取的明文$M_{ij}=D_{ij}+s_{ij} \bmod n$，然而，内部攻击者只拥有 CC 中的附加秘密参数$s_j$，无法获取 SM 中$s_{ij}$，攻击者仍无法获取准确的明文信息。因此，尽管方案受到内部攻击，用户的个人数据仍无法被泄露。

（2）数据完整性

当数据在公共信道传输时，完整性可以确保数据的完整，防止数据被篡改。在本方案中，CC 和 FN 可以检测到被篡改的消息。对于每个由 SM 发送给 FN 的消息$\left\{C_{ij},id_{ij},T_p,\sigma_{ij}\right\}$，FN 首先检查其身份$id_{ij}$和时间戳$T_p$，然后通过验证

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/308114033045006026