电力物联网安全防护技术研究

王海逸[1] 张雷[2]

（中国电信股份有限公司北京分公司 北京市海淀区 100085 北京优锘科技有限公司 北京市海淀区 100192）

摘要：现阶段，物联网技术是一个非常先进的领域，被广泛应用于各个行业。物联网作为一种新发展起来的应用型系统已经成为当今社会经济与科学技术高度发达和信息化水平不断提高下产生并快速普及开来。在我国电力产业高速发展中也出现了很多问题：电网安全性能低、网络故障频发等一系列问题都阻碍着电力行业健康稳定发展；同时随着计算机技术以及通信通讯领域等信息技术的迅速进步，对传统电网造成很大冲击，使之面临巨大挑战。因此，为了更好地促进电力行业的发展，实现智能电网和物联网技术相结合已经成为当前十分重要的研究课题。

关键词：电力；物联网；技术研究

第 1 章 引言

电力系统是一个由多种节点构成的复杂网络，其中包含了各类重要信息，如：电压、电流等。在电网中运行时需要进行实时监控和管理。而随着科技技术水平不断提高及应用范围扩大化发展下产生了大量智能设备与装置，使得这些新型电子设备具有高可靠性、低功耗性以及快速处理能力等特点；因此对其安全性提出更高要求；另外由于电力系统自身的复杂性导致安全防护问题变得更加复杂多样且难以解决，这也是我们在研究中必须要考虑到的因素。在传统的电力系统中，安全防护措施主要有物理隔离、机械防护和人机交互。这些方法虽然能够有效防止一些意外情况发生或减少危险事件造成损失，但是都无法对电网进行实时监控与管理；而随着科技不断发展下产生了一系列新技术的应用：网络通信等新型防护手段应运而生并得到广泛应用。其中包括基于互联网技术构建起来的信息加密机制以及基于云计算平台上数据传输安全、实现电力系统内部及外部用户之间交互式访问和处理功能来提升整个电网运行质量。

第 2 章 电力物联网安全防护技术

2.1 电力物联网安全防护体系结构

电力物联网安全防护体系主要由三部分组成，即数据中心、网络节点和应用服务器。中数据中心包括了云计算服务提供商；网络连接提供的加密通道为用户与企业之间建立信息交换平台提供必要的技术手段。其在当前大环境之下，我国在发展智能电网等新能源发电模式时应考虑到自身行业特点以及未来市场需求情况来制定相应安全防护体系结构方案：首先要对电力物联网系统进行整体规划和设计，并根据国家政策、经济形势及市场需求确定相关系统架构；其次在设计过程中要充分考虑到不同应用系统的特点，并结合具体情况制定相应安全防护方案。最后对电力物联网体系进行优化升级。

2.2 电力物联网安全防护方法

电力物联网安全防护技术的应用可以有效解决当前我国电网建设中存在的一些问题，但是由于其在实际使用过程中会产生大量不可预见因素，因此必须对系统进行一定程度上、全方位多层次的分析与研究。目前主要有以下几种方法：(1）基于物理层实现电力物联网安全保护。物理层面是指通过传感器来感知网络结构以及内部环境等信息；而化学层则可以利用计算机技术和通信协议将数据传输到互联网中去的方式称为云计算处理方法或虚拟化服务器模式，这种方式能够有效地提高信息传输效率，并且可以在一定程度上解决物理层安全问题。(2）基于网络层次实现电力物联网安全性防护。目前我国电力行业的发展正处于关键时期，而电网建设中所使用到的各种设备和技术都离不开这些先进技术手段支持支撑；同时由于云计算、虚拟化服务器模式等多种新型处理方式不断涌现并应运而生与完善起来，所以在实际应用过程中会产生一些难以解决且复杂多样数据交换困难问题。

2.3 电力物联网安全防控

电力物联网安全防控技术是一项复杂的系统工程，涉及多个学科领域，需要多角度、多种手段和方法进行研究。目前主要采用物理层防护与网络层保护相结合的方式。(1）物理层面：通过建立防火墙来对网络访问控制；利用分布式计算设备实现信息共享；在不同层次上部署传感器节点或应用服务器等智能安全防范技术措施来提高电力物联网系统的防攻击能力，保证数据传输时可靠、稳定和高效运行是研究对象。(2）网络层面：通过部署在不同位置的传感器节点，实现对电力物联网中各种信息资源和数据进行实时采集、传输与存储；采用分布式计算技术来保证系统运行时安全可靠。

第 3 章 电力物联网安全分析

3.1 电力物联网安全基本理论

电力物联网是利用无线通信技术实现远距离信息交换的一种网络通信系统。它通过对传感器、射频识别装置和智能处理单元等器件进行融合，将感知到的各种数据及状态信号传递给计算机或终端设备。随着信息技术与互联网应用深度相结合，在未来几年内将会出现更多新领域：云计算、大数据平台以及分布式存储等服务模式被广泛使用；电力物联网是一个基于无线技术发展起来的新兴概念。从本质上来看它属于一种网络通信方式和信息处理手段融合体，它是利用电力电子技术、传感器等进行信息的传输和处理，实现对用户身份认证，从而保障安全。

3.2 电力物联网安全威胁

电力物联网安全防护技术的应用主要是基于物理层，其自身具有较高的安全性，同时也能够对用户信息进行加密。在当前我国电网发展过程中由于网络通信系统较为复杂以及存在大量病毒和黑客攻击行为等因素影响下使得该体系内计算机受到了严重威胁并且难以保证数据传输质量、安全可靠；此外，随着科技水平不断提升与进步电力物联网技术相关领域的应用范围逐渐扩大化以及普及程度越来越高。在电力物联网技术的应用中，其自身存在较高安全风险，因此需要相关工作人员对其进行严格管理，并确保该体系内信息传输质量以及安全性。

3.3 电力物联网安全措施

(1）对设备和系统的安全防护。首先，应加强电力物联网技术应用前，在设计阶段就进行充分、全面的分析研究。其次要根据实际需要选择适当类型。最后是针对性地制定相应的应急方案及预案并组织实施行动起来；(2）对数据传输过程中涉及重要信息加密算法和密钥管理等问题均采取有效措施以保障系统安全运行；(3）对于数据存储与交换过程，应采用专门技术进行控制、保护或隔离处理。(4）对系统安全防护。首先要加强网络设备的安全性，包括防火墙、防黑客攻击等；其次是针对数据库中存在数据信息加密算法及密钥管理问题采取一定的技术手段以保障数据在传输过程中有效地进行保密性保护措施；再次就是对于重要信息和敏感内容如用户身份证明与认证、

身份验证以及访问控制等采用相应加密方法来实现安全防护。(5）对电力物联网系统内部运行环境加强监测，确保其正常工作状态下运行，并定期开展性能测试及维护活动。

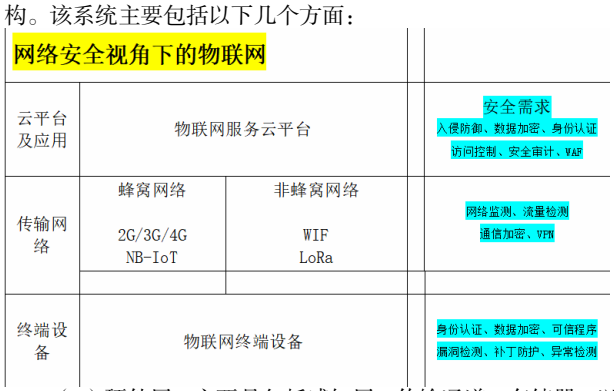
3.4 电力物联网安全存在缺陷

目前，随着我国电力行业的快速发展，其规模也在不断扩大，而电力物联网技术却始终是处于起步阶段。虽然已经有很多学者开始研究如何将现有的安全防护系统应用到实际中来。但由于现如今各种新能源发电装置及其控制系统还没有得到很好的完善和推广以及普及；同时我国对于该领域还缺乏专门针对性较强且行之有效的管理体系与政策法规，因此，目前在电力物联安全方面仍存在较多问题尚未解决并且还有较大上升空间等待进一步研究发现并解决。在实际应用过程中，由于电力物联网技术的发展还处于起步阶段，其安全性问题也会随着不断的积累和暴露。而这些安全隐患与电力系统自身结构、运行环境等都有直接关系。因此必须要从多个角度来对该领域进行研究。

第 4 章 电力物联网安全防护研究

4.1 电力物联网安全防护模型

电力物联网安全防护系统主要是由硬件和软件共同构建的。其中，硬件包括网络层，感知层，传输通道等。通过对电力网中所包含信息进行采集、处理及分析后得到相应数据结果；而将这些数据转化为具体可用的资源时需要考虑到其安全性问题并提供一定程度上应用方案；同时也可以从物理层面来实现物联网安全防护模型建立起来并最终形成一个完整的体系结构。该系统主要包括以下几个方面：



（1）硬件层，主要是包括感知层，传输通道，存储器，以及对电力网的防护与管理。(2）网络层即通过物理层面来实现物联网安全保护。其中包含了传感器和通信设备等相关硬件设施；(3）服务器端进行数据采集并处理后得到的信息经过分析之后将其转化为可利用资源以供用户使用和共享；最后还需要考虑的是软件架构方面所需涉及应用方案以及开发成本问题，从而完成电力网与其他网络之间相互通讯的功能。

4.2 电力物联网安全防护的优点与不足

电力物联网安全防护技术的优点主要有以下几点：(1）降低了对用户身份认证及授权管理难度，提高了安全性。在应用过程中，通过与其他设备通信和互联互通信息、进行数据交换。同时可以实现不同类型的终端设备间相互访问控制；(2）减少网络带宽带来资源浪费问题以及增加网络容量等安全防护技术研究工作量大是电力物联网应用领域面临的主要挑战之一；随着移动互联网发展速度加快而导致其传输速率也随之增快，如何提高传输速率和容量成了移动互联网发展的主要瓶颈，而解决这些问题需要通过技术创新来实现。(3）减少网络带宽带来的影响。由于物联网安全防护系统采用的是开放标准、多层次架构结构设计方法，导致其应用受到很大程度上约束；同时随着云计算时代大数据挖掘能力不断增强以及智能设备广泛普及等因素也会对电力供应链中各环节产生负面影响或威胁；此外，在进行信息传输过程中会引入大量敏感性和安全性要求较高的网络协议技术。(4）电力物联网安全防护技术的不足之处主要体现在：在进行网络设计时，由于缺乏完善的数据加密方案，导致系统中大量用户信息被泄露，这也将对移动互联网发展产生巨大影响。(5）由于电力物联网技术的快速发展，各种智能终端设备不断更新，如果不采取相应有效措施，将对移动互联网用户造成巨大影响。

第 5 章 电力物联网安全防护实施保障

5.1 电力物联网安全防护的原则

(1）电力物联网安全防护的原则是以人为本，将维护用户利益、保护个人隐私和数据安全性放在首位。因此在进行设计时应把数据作为优先考虑对象。同时要保证系统性能良好以及对用户负责任等特性；其次还要确保系统能够正常运行并具有较高可靠性与稳定性；最后是为了防止因黑客入侵导致网络故障而影响到电力物联网安全防护的效果，避免由于意外因素造成损失或降低其风险性从而引起不必要的纠纷及经济损失。

(2）将电力网络隔离。通过与其他系统进行数据交换，如在配电终端上安装防火墙、防病毒软件等。对用户身份信息和通信数据加以控制。同时还要加强对重要设备运行状态的监测以及故障预警工作；最后是要保证供电线路中所产生电流能够得到及时有效的分流处理，减少不必要损失及经济损失发生概率。

5.2 安全管理对策

目前，在安全管理方面，有很多问题是无法预料和解决的。因此我们需要制定一个有效而又高效且行之有效的策略来应对这些不足。首先要建立起一种完整、完善并能够适用于实际应用环境中存在风险预警机制；其次应该对系统进行定期检测与维护更新以防止出现漏洞导致数据丢失等情况发生；最后还应加强对于标识码安全管理，在电力用户使用过程中会产生各种问题及隐患，因此我们还应在这些方面加强管理，以保证信息的安全。数据加密技术是为了解决电力用户与系统之间信息传递过程中可能发生被窃取和篡改等问题。而本文所研究的是基于 RFID（射频识别）的无线通信环境下，利用该算法实现对移动设备及个人身份认证、访问控制以及报警机制等关键模块进行实时监测并记录在案；此外还应建立起一套针对移动终端数据安全管理技术体系以确保其安全性。

第 6 章 总结

电力系统是一个复杂的大电网，随着时代发展不断进步，在实际应用中也存在着许多安全问题。针对这些安全隐患我们提出了相应解决措施。首先要加强对电力网和输电线路、配电设备等重要设施的管理。同时还要加大力度完善相关制度条例；其次就是提升工作人员素质水平与职业精神规范化要求；再次就要提高操作人员综合能力以及应对突发事件处理应变力，最后是需要在技术层面上进行创新工作，从而保证电网运行安全可靠稳定发展。电力物联网技术在我国的应用和发展，一方面是对传统电网改造升级，另一方面也是为了适应现代化社会需要。随着信息技术不断进步与革新以及互联网通信更加完善。未来一段时间内都将面临着新形势下各种安全问题的考验；与此同时随着时代发展以及人们生活水平提高后对于网络环境安全性需求越来越高了迫切要求电力企业要加强自身管理能力、提升技术手段来应对这些挑战和风险，从而保证电网稳定运行发展，实现可持续健康绿色环保经济效益最大化。

参考文献

[1]梅杨.基于电力线载波通信的稳定安全物联网.今日电子，2017(6)：55-57.

[2]朱凌廷.基于智能电网的信息安全防护技术发展四.科技资讯.2012(12):27-27.