

[电网管理]

基于哈希算法的电力物资编码优化初探

文/国网浙江省电力有限公司 李 明 屠晓栋
浙江大学 袁康培
爱植保科技(杭州)有限公司 尹玉凤

电力物资编码是物资唯一的“身份证”，是建设泛在电力物联网的基础性工作，编码的科学性对物资管理的有序高效、数据统计分析等都有着极其重要的意义。结合现有电力物资编码方式，通过哈希算法的运用，突破传统的编码模式，在实现电力物资编码的统统一的同时，探讨电力物资编码与IPv6结合的可能性。

2019年国家电网公司“两会”做出全面推进“三型两网”建设，加快打造具有全球竞争力的世界一流能源互联网企业的战略部署，建设泛在电力物联网是落实“三型两网、世界一流”战略目标的核心任务。泛在电力物联网，就是围绕电力系统各环节，充分应用移动互联、人工智能等现代信息技术和先进通信技术，实现电力系统各环节万物互联、人机交互，具有状态全面感知、信息高效处理和应用便捷灵活特征的智慧服务系统。泛在电力物联网包含感知层、网络层、平台层和应用层四层结构。感知层是信息数据采集的关键部分，是实现电力系统中发电、变电、输电、配电和用电等各个环节万物互联、人机交互的基础。

电力物资的品类繁多、数量庞大，需要赋予物资唯一的身份码，而科学、合理和统一的物资编码方式，是系统安全运行、数据的协同共享、信息的高效处理重要支撑。目前，电力物资的垂直管理模式相对成熟，但管理的环节冗长，涉及多个部门，导致部门之间的横向专业协同、信息共享存在壁垒，阻碍数据价值的深入发掘。同时项目编码、供应商编码、仓储点编码和物资编码

等来源于不同业务系统，仅能在局部系统中实现部分编码的关联，信息在整个过程中的衔接程度十分有限。

因此，探索建立适应泛在电力物联网建设需求的物资编码技术尤为重要。

国家电网物资编码现状

1. 国家电网物资编码规范

国网浙江省电力公司早在2016年已经启用物资身份码RFID标签，并制定了身份码编码技术标准，规范了应用内容及安装工艺。

2018年，国家电网公司制定了《电网资产统一身份编码建设推广实施总体工作方案》，提出全面开展电网资产统一身份编码建设推广工作。2019年4月30日，国家电网印发《国家电网有限公司关于印发电网资产统一身份编码建设实施方案的通知》（国家电网设备[2019]414号），推进公司电网实物资产统一身份编码（以下简称实物“ID”）建设和应用，提升公司资产全寿命周期管理水平，夯实泛在电力物联网建设基础。

现行实物ID编码采用24位十进制数据组成，代码结构由网省公司代码段、识别码、流水号和

基金项目：国家电网公司2019年管理咨询项目《基于物联网技术的智能配送机制研究》（ZBGW19-009-020）。

校验码四部分组成。各部分代码位数如表1所示。

表1 日均回馈率与35 kV回馈效率

序号	1	2	3	4
代码名称	网省公司代码	识别码	流水号	校验码
位数	3	2	18	1

1) 网省公司代码: 3位数, 用于标识电网资产实物ID归属单位, 由国家电网公司统一制定, 如国网浙江省电力公司为“011”。

2) 识别码: 2位数, 用于区分不同业务应用生成的电网资产实物ID, 如供应商交付的增量设备资产实物为“01”。

3) 流水号: 18位数, 按照数字序列自动生成。

4) 校验码: 1位数, 用于检查电网资产物资是否启用。

2. 电力物资实物ID业务流程

国家电网现行的电力物资实物ID, 主要包含以下“14+2”的电网一次设备, 14类主网设备: 主变压器、断路器、组合电器、隔离开关、电流互感器、电压互感器、电抗器、电力电容器、耦合电容器、接地变压器、站用变压器、开关柜、避雷器和消弧线圈。2类配网设备: 配电变压器和环网柜。

电力物资实物ID业务流程如图1所示。

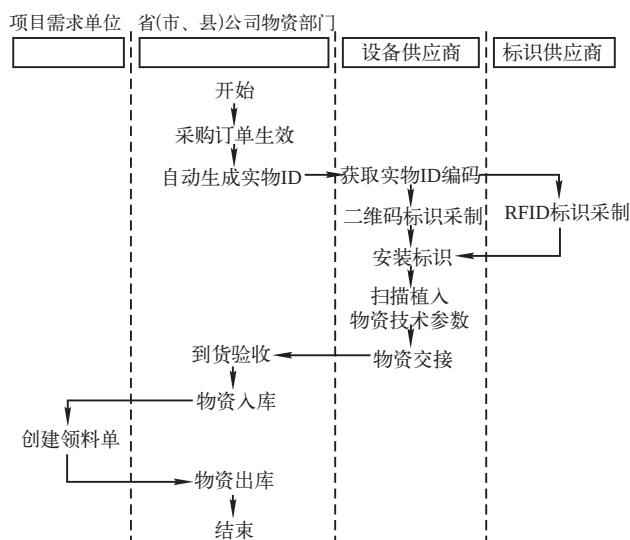


图1 现行电力物资实物ID业务流程图

3. 现行电力物资编码存在不足

(1) 物资品类有待拓展

电力物资实物ID目前仅运用于“14+2”的电力物资品类, 在建设泛在电力物联网的要求下, 有待进一步扩展应用到其他物资类别, 不仅仅是电力物资, 生产服务车辆、仪器仪表及后勤设备

设施也存在赋码需求。电力物资的多样性、不同分类方式和其他设备设施, 都对现行的物资编码方式提出了适用性挑战。

(2) 编码形式不统一

目前业务活动中, 项目编码、供应商编码、仓储码编码和物资编码等来源于不同业务系统, 编码形式不统一, 仅能在局部系统中实现部分编码的关联, 信息在整个过程中的衔接程度十分有限。

(3) 编码缺少节点信息

现行物资编码规则采用24位十进制, 每段代码名称所指代的含义, 仅考虑物资自身属性及其在国网系统内部的流转的唯一性, 没有有效地结合物资从生产、供应、仓储、配送、运维和报废的全寿命周期的关键节点信息, 为物资管理信息共享、价值挖掘提供基础支撑。

基于哈希算法的电流物资编码优化

1. 哈希算法概述

Hash, 一般翻译做散列、杂凑, 或音译为哈希, 是把任意长度的输入(又叫预映射pre-image)通过散列算法变换成固定长度的输出, 该输出就是散列值。Hash函数, 简单地说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。著名的哈希函数有MD4、MD5、SHA-1和SHA-2等。

随着互联网的飞速发展, 网络安全问题日益突出。为了确保接收方所接收到的报文数据的完整性, 人们开始采用消息认证来验证。在FSE 2008上, Shamir设计了第一个轻量级MAC算法(Message Authentication Code) SQUASH。

MAC (Hash-based Message Authentication Code), 是由H.Krawczyk, M.Bellare, R.Canetti于1996年提出的一种基于Hash函数和密钥进行消息认证的方法, 并于1997年作为RFC2104被公布, 并在IPSec和其他网络协议(如SSL)中得以广泛应用, 现在已经成为事实上的Internet安全标准。它可以与任何迭代散列函数捆绑使用。

2. 电力物资编码优化

(1) 哈希算法的选择

基于Hash算法的HMAC, 其安全强度远高于Hash算法, 本文运用基于MD5消息摘要算法基础上构造而成的HMAC-MD5算法, 探索电力物资编码的新方向。HMAC-MD5算法将密钥与消息

数据混合，使用哈希函数对混合结果进行哈希计算，将所得哈希值与该密钥混合，然后再次应用哈希函数。HMAC－MD5接受任何大小的密钥，并生成长度为128位的哈希序列。

HMAC－MD5算法的描述如下

$$HMAC(K, M) = H(K + opad \parallel H(K + ipad \parallel M))$$

式中，K是密钥；M是消息内容；H是散列函数（本文选取MD5）；opad和ipad分别是由若干个0x5c和0x36组成的字符串；+是异或运算； $\parallel$ 是连接操作。

过程步骤如下：①在密钥K后面添加0来创建一个长为B的字符串；②将上一步生成的字符串与ipad做异或运算，形成结果字符串；③将消息M的数据流附加到第2步的结果字符串的末尾；④将MD5算法作用于第3步生成的数据流；⑤将第1步生成的字符串与opad做异或运算，形成结果字符串；⑥再将第4步的结果附加到第5步的结果字符串的末尾；⑦将MD5算法作用于第6步生成的数据流，最终输出结果。

HMAC的安全性依赖于嵌入的Hash函数的同时，也依赖于密钥，密钥的安全性依赖于它的长度和随机性。因此，在保证密钥安全性的前提下，HMAC要比单一的Hash函数具有更高的安全性。

(2) 基于HMAC－MD5算法的电力物资编码
国家电网现行的编码体系有多种，现列举了电力物资实物ID编码、配送车辆、检测仪器编码、库存地点编码和仓位编码等在现行编码方式，不同编码体系，会在不同业务系统中的对数据编码的关联，数据信息的衔接等方面产生制约。

基于HMAC－MD5算法，对不同的编码体系下的现状编码进行了转化，生成统一的128位哈希序列编码，转换为16进制后为32位。同时，对同一编码的内容，采用两种不同的密钥进行了对比，产生完全不同的哈希序列。在实际运用过程中，可以采用“伪随机序列”等方法生成密钥，通过安全的密钥协商机制、密钥的更新等方式保障其安全性。如表2所示。

表2 基于HMAC－MD5算法各类编码示例

编码类别	编码内容 (M)	密钥 (K)	128位哈希序列 (转换为16进制)
实物ID编	011010000000000002868403	123456	bd1c21a2bfb6dccc9a716ae0df267003
		888888	0609fdaabc4942f26ae9ca1ba77dc493
配送车辆	浙A·G2019	123456	6832fbe0496cb7723684da892b138e27
		888888	e144d28c0710589e19c9f17060f05205
检测仪器编码	9801001	123456	804b54b1e8a36ff306c458415461df28
		888888	22d12ce09b3641c78b3fba87176ab7f0
库存地点编码	ICA3	123456	75642c9be26754b2225b29da8ff29184
		888888	92037966cb0c0e1aa6518140a5e23603
仓位编码	B01-020101	123456	3d37bb356fc8cfb20ee04a89f8537d5f
		888888	98c4a07eac2d2baa71268e6a13927b13

在建设泛在电力物联网的要求下，可以预见，包括电力物资在内的各类车辆、仪器和设备的赋码需求可能会出现爆炸式增长。传统的编码体系，将不足以应对如此庞大的物资数量，而128位的哈希序列最大地址个数为2128，据说可以为全世界的每一粒沙子编上一个地址，完全可以满足对电力物资，甚至是整个电力系统中所有要素的唯一编码。

由于哈希算法具有压缩信息的特点，采用哈希算法的编码方式，可以让编码本身携带更多的数据，实现物资全寿命周期的信息维护。同时，采用基于哈希算法的编码方式，在保障信息安全、海量数据处理等方面具有重要的意义。

基于HMAC－MD5算法的编码与IPv6融合的探讨

IPv6是英文“Internet Protocol Version 6”（互联网协议第6版）的缩写，是互联网工程任务组（IETF）设计的用于替代IPv4，成为下一代互联网的基础通信协议。

IPv6的文本表示法也与RFC5952中确定，IPv6地址通常使用冒号十六进制形式表示，即x:x:x:x:x:x:x，每个x都以16进制表示一个16位长的整数，且里面的字母用小写表示。其中包括48位的全球网络标识符、16位的本地子网标识符、64位的主机标识符，后48位的主机标识符一般是由设备的MAC地址自动生成。IPv6协议定义的地

址格式如表3所示。

表3 IPv6协议定义的地址格式

48位	16位	64位
Global ID	Subnet ID	Interface ID

随着物联网技术的兴起和发展,众多学者对IPv6在物联网感知层的应用进行了大量的研究。而运用哈希算法在IPv6的地址生成、地址安全等方面的研究,也取得了丰硕的成果。

泛在电力物联网背景下,将面临物联网设备IP地址不足的问题,IPv6将有机会成为物联网应用的基础网络技术。合理运用IPv6的移动性、快速响应、设备安全和端到端的IP链接能力,才能真正开启泛电力物联网的大门。

在对IPv6地址分配的研究中,一般针对后64位的进行设计和定义,上述基于HMAC-MD5算法的编码方式产生的编码加入了密钥,而融合了带密钥的哈希值生成的IPv6地址,具有更好的抗攻击

能力。基于HMAC-MD5算法的编码与IPv6的融合方式如图2所示。

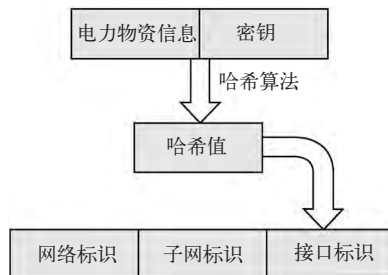


图2 基于HMAC-MD5算法的编码与IPv6的融合方式

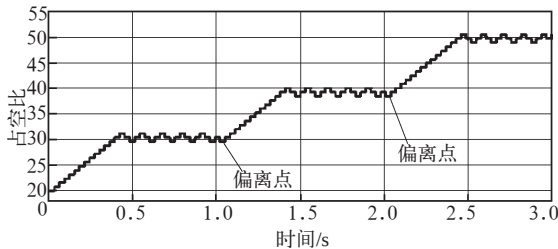
结束语

在国家电网全力推进泛在电力物联网建设的背景下,本文初步研究了一种基于HMAC-MD5算法的全新的电力物资编码方式,并探讨了与IPv6结合的可能性。EA

(收稿日期: 2019.11.07)

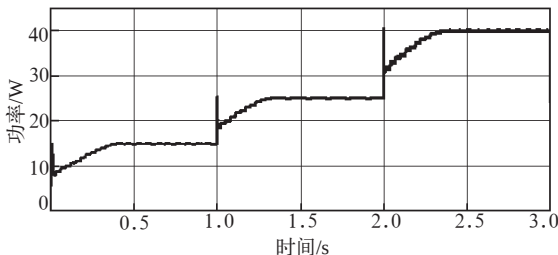
(编辑: 朱金凤)

(上接第88页)

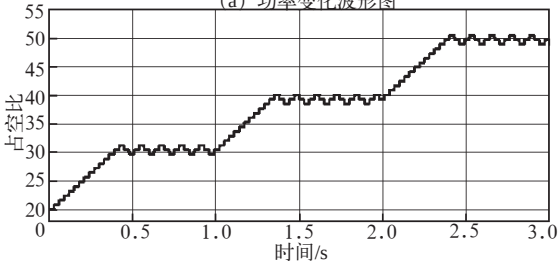


(b) 占空比变化波形图

图6 辐照度扰动下传统算法仿真结果



(a) 功率变化波形图



(b) 占空比变化波形图

图7 辐照度扰动下所提算法仿真结果

对比可以看出,当辐照度从 0.3 kW/m^2 增加到 0.5 kW/m^2 时,传统算法响应时间为 0.39 s ,所提算法响应时间为 0.30 s ,追踪速度提升 23.1% ,光伏阵列的平均输出功率分别为 25.09 W 和 25.1 W 。当辐照度从 0.5 kW/m^2 增加到 0.8 kW/m^2 时,传统算法响应时间为 0.43 s ,本文算法响应时间为 0.35 s ,追踪速度提升 18.6% 。光伏阵列的平均输出功率分别为 40.01 W 和 40.18 W 。综上所述,与传统的电导增量法相比,所提算法在不同的辐照度变化范围内都具有解决误判现象产生的能力,且在不同的辐照度变化范围内追踪速度有不同程度的提升。不仅解决了辐照度变化时所产生的误判现象,还有效地提高了系统的响应速度,减小了追踪过程中的功率损失,提高了系统的输出效率。

结束语

本文提出了一种改进型的电导增量法,采用一种全新解决问题的思考方向,且本文所提算法的控制系统结构相比于目前国内外所采用模块化方式更加简单、稳定,且能够准确地响应和追踪MPP,提高了系统的稳定性,以避免在辐照度改变时系统会产生误判现象。EA

(收稿日期: 2020.04.02)

(编辑: 朱金凤)