文章编号：2095-2163(2020)08-0140-04 中图分类号：TP3-05 文献标志码：A

泛在电力物联网的多项式密钥管理算法研究

陈虹旭[1]，李晓坤[1]，徐 龙[2]，董潍赫[2]，刘清源[1]，付文香[2]
（1.黑龙江恒讯科技有限公司 国家博士后科研工作站，哈尔滨 150090；2 黑龙江大学，哈尔滨 150090）

摘 要：随着泛在电力物联网(UPIOT)的快速发展，其传感器网络出现的安全问题也广受关注。本文针对在国家电网、安全监控等关键领域中密钥管理技术进行了研究。虽然 RSA 和椭圆曲线等公钥加密方案能够提供足够的安全性，但由于计算量大，与传感器节点的资源约束相冲突，使得它们的使用受到了限制。对于集群密钥的安全管理方面，本文将双变量多项式的概念引入密钥管理。这不仅仅确保了任意两个节点之间的成对密钥，还对生成的双变量多项式进行簇间密钥分配，对生成的双变量多项式在密钥管理中的各种特性进行测试，并在多项式的不同阶数下进行了仿真实验及结果分析。

关键词：泛在电力物联网；传感器网络；多项式密钥；密钥管理

Research on polynomial keymanagement algorithm ubiquitous in power Internet of Things

CHEN Hongxu[1], LI Xiaokun[1], XU Long[2], DONG Weihe[2], LIU Qingyuan[1], FU Wenxiang[2]
(1 Postdoctoral Program of Heilongjiang Hengxun Technology Co., Ltd., Harbin 150090, China;
2 Heilongjiang University, Harbin 150090, China)

【Abstract】 With the rapid development of the ubiquitous Power Internet of Things (UPIOT), the security problems of its sensor networks are also widely concerned. Traditional sensor networks are composed of hundreds of self-organizing sensor nodes. Key management is one of the most important security primitives in state grid, security monitoring and so on. Although public key encryption schemes such as RSA and elliptic curve can provide sufficient security, their use is limited due to the large amount of computation and the conflict with the resource constraints of sensor nodes. For the security management of cluster keys, this paper introduces the concept of bivariate polynomial into key management. This not only ensures the pair key between any two nodes, also for key distribution between the clusters of the bivariate polynomial, and finally to generate various features in the key management of bivariate polynomial test.Under different order polynomial, the simulation experiment and the simulation results are analyzed.

【Key words】 ubiquitous in the Internet of Things; sensor network; polynomial key; key management

0 引 言

泛在电力物联网的发展带动了大规模传感器网络的发展[1]。传感器网络由成百上千的微型传感器节点组成，这些节点没有支持基础设施，并且是自组织的。它们可以安装在任何地方，并且将在没有任何帮助的情况下工作。但传输数据的真实性、保密性和完整性需要由有效的机制来保证[2-4]。除了一般的无线网络的安全限制，传感器网络容易受到几种其它类型的攻击。其中主要是节点捕获攻击，使安全成为对其最重要的关注[5-6]。尽管如此，施加在传感器节点上的计算、能量和内存限制以及它们所处的攻击环境使它们更容易受到攻击[7]，并禁止使用更安全的公钥加密技术。因此，迫切需要安全协议来保护这些类型的网络免受恶意攻击[8]。为了实现安全通信，密钥预分发已经成为一种可接受的技术，允许传感器节点动态地建立对等关系[9]。

最简单的密钥预分配形式涉及到在整个网络范围内使用一个密钥，允许任何节点对有效地连接，但任何节点的折中都可能导致整个系统崩溃[10]。本文提出了一种多项式密钥管理的方案，该方案提供了足够的安全性，任何单个节点的泄露都不会泄露

基金项目：国家自然科学基金(81273649,61501132,61672181)；中央高校基本科研业务费专项资金(3072019CFT0603)；中国博士后科学基金(2019M650069)；中小企业创新基金(2017FF1GJ023)；专利优势示范企业基金(2017YBQCZ029)；黑龙江省自然科学联合引导基金(LH2019F049, LH2019A029)；黑龙江省基础科研科技创新基金(KJCX201805)；黑龙江省基础科研青年创新团队基金(RCYJTD201805)。

作者简介：陈虹旭(1986-)，男，硕士，高级工程师，CCF 会员，主要研究方向：虚拟化、云计算、人工智能等；李晓坤(1979-)，男，硕士，研究员级高级工程师，教授，CCF 高级会员，主要研究方向：虚拟化、人工智能、生物特征识别等；徐 龙(1997-)，男，硕士，主要研究方向：移动通信、信息安全、软件开发等；董潍赫(1999-)，男，本科生，主要研究方向：无线通信、智慧城市、人工智能等。

通讯作者：李晓坤 Email：li.xiaokun@163.com

收稿日期：2020-06-07

其它节点的机密。然而，随着节点数量的增加，系统无法扩展，因此需要更多的内存来存储密钥，使其更好的提供系统的稳定性与安全性。

1　相关技术

1.1　泛在电力物联网技术

泛在电力物联网技术未来要呈现的是物理互通更紧密、数据维度更多元、技术更成熟的智慧电力能源系统。泛在电力物联网将内外部元素都整合在一起，即信息和数据的“普遍存在”。物联网是泛在电力物联网的具体体现；“电力网络”是物联网技术的特定应用对象；“泛在网络”也可以通俗的理解为是物联网与互联网的结合。也就是说利用二者的技术实现在生产、服务场景中信息的传送，不受时间、环境等因素的干扰，完成信息的无缝连接通信[11]。

借助移动互联网、人工智能等现代信息技术以及先进的通信技术，泛在电力物联网可以实现不同能源系统的物理互连，信息互连和商业互连。它具有整体感知，无处不在的连通性，开放共享和集成创新的功能[12]。国家电网根据泛在电力物联网的要素及特点提出了其体系结构如图 1 所示。

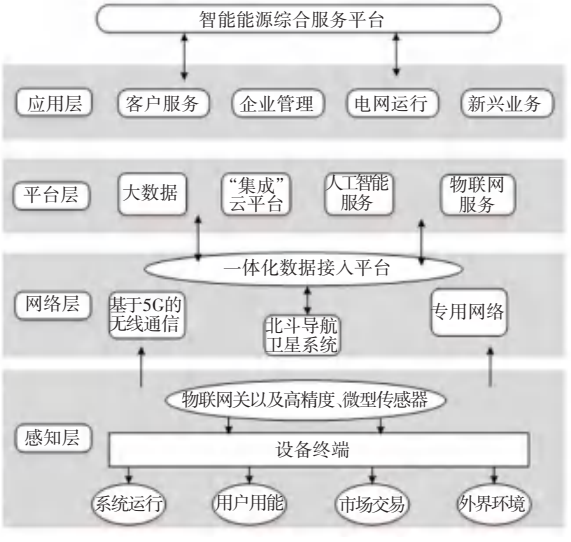

图 1　泛在电力物联网体系结构

Fig. 1　Ubiquitous power Internet of things architecture

(1)整体感知：通过使用各种传感技术(例如传感器和射频识别(RFID))，动态获取发电厂，配电网络，负载侧和储能设备的运行状态和环境信息。

(2)无所不在的连通性：利用专有网络或移动物联网技术，实现电力系统设备和用户相关信息和数据的全时空连接，即无处不在的信息传输。

(3)集成与创新：海量数据通过通信技术传输到统一平台进行共享和统一管理，实现数据的实时交互。使数据真正有效，并发挥其最大价值。

(4)开放和共享：通过各种创新要素的创造性整合，可以将不同设备和用户在不同时间和空间的信息相互联系。整个业务可以在线实现；电网可以安全稳定地运行，建立智能化的综合能源服务平台；可开发电力市场，促进电网改造。

1.2　多项密钥管理

传统的传感器密钥管理网络被划分为簇，每个簇包含一个簇头(Cluster Head，之后简称 CH)和一般传感器节点。在放置之前，每个 CH 节点将一组密钥存储在内存中，之后每个传感器节点选择 CH 节点，并从节点中随机选一个密钥，将这个密钥与 CH 节点的 ID 信息一起存储在内存当中。之后，每个传感器节点与其 CH 交换密钥信息，如果 CH 的内存中有密钥信息，则可以直接建立安全连接。否则 CH 从匹配的 CH 节点请求所需的密钥。这确保了改进的网络性能，因为层次化的网络结构有助于降低能耗。而 CH 节点之间的通信使用了组密钥，这对于传感器网络来说是非常危险的[12]。

多项式密钥管理的方案大致分为 3 个阶段：第一阶段是密钥预分配；第二阶段是集群间成对建立；第三阶段是集群内成对密钥建立。

2　框架提出

此框架将双变量多项式引入密钥管理，不仅确保了任意两个节点之间的成对密钥，还将生成的双变量多项式进行簇间密钥分配，实现了三层的异构传感器网络。该网络由具有无限资源的基站组成，与普通传感器节点相比，簇头具有额外的存储和计算功能。

多项式中的项式可以视为多元单项式，其程度为变量的指数之和。给定一个单项式 P，如式(1)所示：

$$P = x^i y^j. \tag{1}$$

单项式的度数 $\deg(P) = i + j$。由式(2)给出二元多项式：

$$f(x,y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j. \tag{2}$$

在这种情况下，多项式的阶数不能超过 t，并且多项式的系数是有限群 $GF(q)$ 的元素，也称为带有 q 元素的伽罗华域。因此，使用这种多项式的传感器节点可以与另一个传感器节点建立链接，也就是说，该组仅限于对应于两个变量的两个成员。这代表着在 n 个节点网络中，只要共享同一多项式，就够建立起 $(n-1)$ 个拥有唯一密钥的链接。由此可见，单链接的危害仅限于该特定链接，如果 $(t+1)$ 个节点遭到破坏，攻击者便能够重构所使用的多项

式,因此可能会遇到安全性问题。

2.1 密钥预分配

离线密钥分发中心(KDC)为集群间成对阶段生成对称的双变量多项式 $f(x,y)$。网络中的每个节点都有一个唯一的 ID。如 CH 节点 i 的 ID 是 ID_{CHi}。KDC 为 $f(x,y)$ 创建多项式的额度,并评估 $x = ID_{CHi}$ 在 i 处的每个份额,并得出一个存储在节点 i 中的单变多项式 $f(ID_{CHi},y)$,如式(3)所示。

$$f_{CHi}(x,y) = f(ID_{CHi},y). \tag{3}$$

同时,生成第二个双变量多项式以用于集群内阶段。

2.2 集群间密钥对建立

在此阶段,每个群集头(CH)与其它群集头建立一个成对密钥,再将其 ID_{CHi} 发送出去。此后,每个节点可以生成成对密钥,而无需彼此协作。CH_i 通过在 $y = ID_{CHi}$ 时给出的 $f(ID_{CHi},ID_{CHj})$,评估其存储的份额 $f(ID_{CHi},y)$ 与 CH_j 建立成对密钥。由于本文使用对称双变量多项式,因此获得的密钥是相同的。

2.3 集群内密钥对建立

该阶段涉及在传感器节点与其 CH 之间建立成对密钥。最初,KDC 将密钥 K_{Ni} 以及从中生成密钥 CH 的相应 ID 一起预加载到每个传感器中。通过对几个键执行按位 XOR 生成此键,如式(4)所示:

$$K_{Ni} = k_1 \oplus k_2 \oplus k_3. \tag{4}$$

k_1、k_2 和 k_3 将使用与集群间成对密钥相同的概念从选定数量的多项式份额中生成:

$$k_1 = f_{2a}(ID_{CHa},N_i), \tag{5}$$

$$k_2 = f_{2b}(ID_{CHb},N_i), \tag{6}$$

$$k_3 = f_{2c}(ID_{CHc},N_i). \tag{7}$$

f_{2i} 是第二个二元多项式的多项式份额。在此阶段,节点将用于与 K_{Ni} 关联生成密钥的 CH 的 ID 发送到其预期相应的 CH 节点。式(5)~(7)分别用于生成密钥 k_1,k_2 和 k_3。然后,预期的 CH 节点使用公式(4)生成的密钥 KNi。

通常,度数为 k 的多项式需要使用 Lagrange 的插值方法[13],来重建 $k+1$ 个或更多点,如式(8)所示。

$$P_j(x_i) = y_j \prod_{k+1} \frac{x_i - x_k}{x_j - x_k} \bmod N. \tag{8}$$

因此,该方案仅在不超过 k 个传感器受损的情况下才是安全的。但考虑到如果少于 k 个传感器受到攻击,它们将不包含足够的信息来揭示其它未受影响节点的秘密,则它可以抵抗节点捕获攻击。

可以证明,使用该方案存储任何多项式所需的存储空间 Sp 为:

$$Sp = (k+1)^{m-1}, \tag{9}$$

其中,m 是需要建立密钥组的大小。式(9)为 $GF(q)$ 的 $(k+1)$ 个系数的存储。这导致每个连接所需的存储空间更少。因此,如果网络中有 n 个 CH,则每个 CH 都可以建立与每个其它 CH 的 $(n-1)$ 个链接,这需要 $(n-1)*(k+1)$ 个存储空间。因此,存储空间线性地取决于组大小,在这种情况下,则取决于网络中 CH 节点的数量。但是,对于集群内密钥对的建立,需要恒定的存储空间,可以随着网络规模的增加而很好地扩展。

给定一个 k 度的多项式,具有 $(k+2)$ 个实数系数和一个未知变量,它需要 k 次乘法和 k 次加法才能对其求值。基于此算法寻求提高多项式次数的效率。

3 验证分析

本文进行了仿真实验,并对实验结果进行了分析。模拟参数见表 1。

表 1 实验环境

Tab. 1 Lab environment

参数	值
网络节点数	250、500、700、1 000
内存	16 GB
覆盖区域	100 * 100
初始簇头能量	10 J

实验中假设使用 3 个不同的组成键,并且这些键均匀分布,以保证每个 CH 节点均与其它任何 CH 节点均等地评估其内部簇多项式 CH 节点。

由图 2 可得,多项式次数的增加伴随着计算量的增加,同时,网络中节点数量的上升,伴随的是每一个 CH 的计算量的上升。因此,如果捕获了 $(k+1)$ 个 CH 节点,则安全性将受到损害。

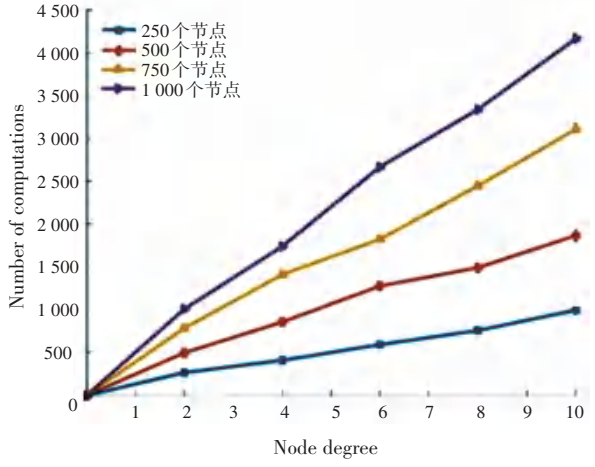

图 2 多项式次数与计算次数对比

Fig. 2 Polynomial degree vsnumber of computations (using 5 CHs)

如图 3 所示，由于将计算性能分配给了更多 CH 节点，则 CH 节点数量的提升可以提高网络的性能。

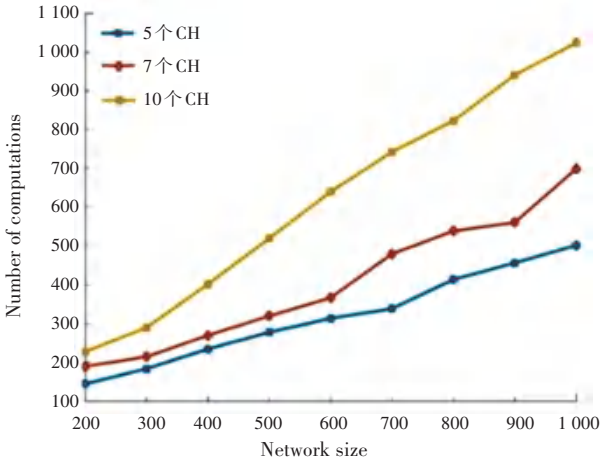

图 3　计算结果及组网规模计算

Fig. 3　Calculation result and calculation diagram of network scale

图 4 在式(9)的基础上进行仿真，对于大于两个的组，所需的存储空间呈指数增长。因此，对于成对密钥建立是可行的。因为存储线性地依赖于多项式。然而，对于普通的传感器节点，该存储仅被限制为存储两个密钥，一个密钥用于与 CH 节点的通信，另一个密钥用于与 BS 的认证通信。

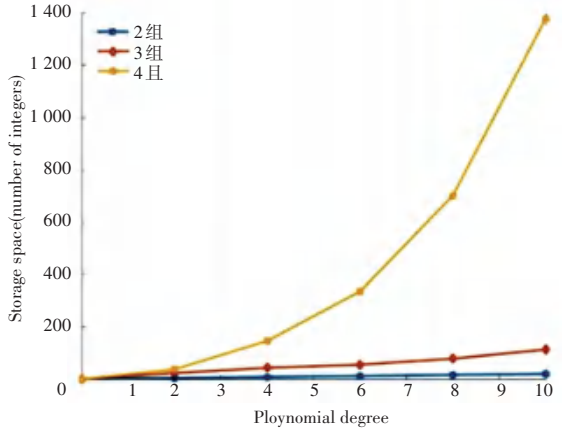

图 4　计算结果及组网规模计算

Fig. 4　Calculation result and calculation diagram of network scale

4　结束语

随着 5G 战略的部署和泛在电力物联网的建设，对于物联网传感器网络的密钥管理分发提出了新的要求[14]。本文研究中，在传统的密钥管理网络中提出了不同的密钥管理属性方案。对于传感器网络的规模及计算量进行了仿真模拟，且进行了不同规模下的数据对比。证明该协议的实用性和优越性。

泛在电力物联网依托现在 ICT 技术，运用高感应智能传感、人工智能等实现了电网希望的感知能力，高效的信息处理，方便灵活的应用程序，和电网的安全经济运行，可以提高服务质量，促进战略性新兴产业和生成强大的数据资源[15]。

参考文献

[1] 高 飞. 一种量子密钥分发和身份认证协议[J]. 北京邮电大学学报(自科版)，2004，27(3)：98-102.

[2] 刘友明，汪超，黄端，等. 高速连续变量量子密钥分发系统同步技术研究[J]. 光学学报，2015，35(1)：88-97.

[3] LO H K，MA X，CHEN K. Decoy state quantum key distribution [J]. Physical review letters，2005，94(23)：230504.

[4] LO H K，MA X，CHEN K. Decoy state quantum key distribution [J]. Physical review letters，2005，94(23)：230504.

[5] LI H W，CHEN W，HUANG J Z，et al. Security of quantum key distribution[J]. Scientia Sinica Physica，Mechanica & Astronomica，2012，42(11)：1237-1255.

[6] LO H K，CHAU H. Security of quantum key distribution[J]. IEEE Access，1998，4(1)：724-749.

[7] GOTTESMAN D，LO H K，LUTKENHAUS N，et al. Security of quantum key distribution with imperfect devices [C]// International Symposium Oninformation Theory. IEEE，2004.

[8] RENNER，RENATO. Security of quantum key distribution[J]. International Journal of Quantum Information，2008，06(1)：1-127.

[9] YUEN，HORACE P. Security of Quantum Key Distribution[J]. IEEE Access，2016，4：724-749.

[10] GOTTESMAN D，LO H K，LÜTKENHAUS，NORBERT，et al. Security of quantum key distribution with imperfect devices[J]. Quant.inf.comput，2002.

[11] MA X，QI B，ZHAO Y，et al. Practical decoy state for quantum key distribution[J]. Physical Review A，2005，72(1)：012326.

[12] INAMORI H N，LÜTKENHAUS，MAYERS D. Unconditional security of practical quantum key distribution [J]. European Physical Journal D，2007，41(3)：599-627.

[13] VAZIRANI U，VIDICK T. Fully device independent quantum key distribution[J]. physical review letters，2012，11(4)：1-2.

[14] BUTTLER W T，HUGHES R J，KWIAT P G，et al. Free-space quantum-key distribution[J]. Physical Review A，1998，57(4)：2379-2382.

[15] LO H K，CURTY M，TAMAKI K. Secure quantum key distribution[J]. Nature Photonics，2014，8(8)：595-604.