区块链系统节点私钥泄露的电力数据防篡改方法与验证机制设计

吉 斌[1,2],昌 力[1,2],朱丽叶[1,2],曹 斌[1,2]
(1. 南瑞集团有限公司(国网电力科学研究院有限公司),江苏 南京 211106;
2. 国电南瑞科技股份有限公司,江苏 南京 211106)

摘要:基于区块链技术的电力应用系统中,私钥泄露节点的签名电力数据存在被恶意篡改或伪造的风险,且当前缺乏有效的防护措施,为此,提出数据加密方法和数据交互验证机制。结合区块链基础加密技术原理,提出随机数与电力数据的组合方法,利用非对称加密算法和Hash算法进行多重加密,构造数据发出节点私钥泄露后的数据防篡改加密方法;为了防止恶意节点利用数据发出节点的私钥对电力数据进行伪造和替换,设计电力数据交互验证机制,利用数据发出节点私钥进行加密并利用接收节点公、私钥进行解密验证;抽象加、解密和数据交互验证机制的数据模型。算例分析验证了所提数据加密方法和数据交互验证机制的有效性。

关键词:区块链;私钥泄露;加密方法;数据交互验证;防篡改;防伪造
中图分类号:TM 73 **文献标志码**:A DOI:10.16081/j.epae.202107018

0 引言

随着电力市场参与主体不断向负荷侧延伸,电力用户、负荷聚合商、售电公司、产消主体相继加入需求响应、辅助服务等市场范畴[1-2]。区块链技术作为数字新基建的基础技术而备受关注,其可为电力市场主体提供可信的业务数据安全交互与溯源支撑,但基于区块链技术的业务数据安全严重依赖密码学。当利用区块链技术支撑负荷侧市场主体间的电力交易时,系统节点私钥泄露将导致节点数据资产对外呈现“不设防”状态[3],针对负荷侧交易的申报、发布、认证、出清以及结算过程的数据均存在被恶意篡改或替换的风险。

目前,针对区块链的密钥安全研究主要集中在防止私钥泄露,从已经发生私钥丢失的案例来看,因区块链系统节点的主观疏忽或管理不当而导致的资产丢失事件时有发生[4-5]。基于区块链技术的分布式电力交易应用、加密技术的私钥保护已有一定的研究。文献[3]基于区块链技术对社交网络隐私数据加盖时间戳并引入加密算法对隐私数据进行保护,这为电力数据的组合加密算法提供了参考和思路。文献[6]利用密钥分割技术对区块链密钥进行分割并分段保存,这是一种事前私钥防丢失的技术。文献[7]以数据安全防护为目标设计一种基于区块链技术的搜索加密数据共享方案,能够保证数据密文和关键字的安全。文献[8]基于区块链技术开展分布式电力交易方案的设计,通过密码学原理实现电力交易数据的安全防护。文献[9]对区块链技术在电力领域的应用进行回顾和分析。文献[10]结合区块链技术防篡改、可追溯的特征,展望其在能源互联网中的应用前景,提出利用区块链技术进行调控运行的流程和方式,对区块链技术在电力调度中的应用进行研究和探讨。文献[11-12]对区块链技术在能源互联网数据安全保护中的应用进行研究,利用区块链技术支撑能源交易数据的可追溯,为电力末端数据的安全防护提供思路。文献[13]分析区块链技术在应用中可能存在的安全威胁,提出区块链的平行安全概念,并总结未来区块链数据安全将面临的问题。上述研究均侧重区块链技术的密码学基础对分布式数据安全交互的重要作用,同时区块链数据安全防护的研究主要集中在数据签名私钥的保护方面,而针对区块链系统节点私钥泄露后电力数据主动安全防护方面的研究不足。

为避免应用区块链技术的负荷侧市场主体节点私钥泄露后出现交易发出数据被篡改或伪造的风险,本文结合分布式数据广播通信方式与系统数据认证机制,从数据加密方法、数据验证机制2个方面开展研究。首先,提出电力指令数据加密和解密方法;其次,为防止恶意节点截断区块链通信网络,利用其他节点私钥伪造电力数据,设计业务数据加密交互认证机制;然后,通过分析数据交互的流程,对数据加密和交互认证流程中存在篡改或伪造隐患的环节进行分析;最后,抽象防篡改的概率模型并通过案例进行验证,案例分析表明,所提加密算法和交互验证机制能够在网络安全的情况下防止恶意节点利用已泄露的节点私钥篡改和伪造电力数据。

收稿日期:2020-08-20;**修回日期**:2021-05-21
基金项目:国家电网公司科技项目(5400-202011441A-0-0-00)
Project supported by the Science and Technology Project of State Grid Corporation of China(5400-202011441A-0-0-00)

1 区块链数据安全防护

区块链技术作为分布式数据库，通过加密技术和共识认证机制保障数据的一致性、防篡改和安全性。从以太坊和比特币的区块链应用来看，椭圆非对称加密算法、Hash-256算法（简称Hash算法）等成熟加密技术为区块链数据多重加密提供了基础加密技术支撑。

1.1 区块链加密算法

加密算法包括对称和非对称2种，区块链技术采用非对称加密算法，主要是椭圆非对称加密算法。椭圆非对称加密算法按照椭圆曲线上离散对数要求给定素数p（大于3）、椭圆曲线E、椭圆曲线外无穷远点Q（对应纵轴坐标无穷大），在已知p、Q的情况下通过式（1）求出小于p的正整数k。根据相关文献可知，在已知k、p时计算Q比较容易，而由Q和p计算k比较困难，因此将区块链椭圆非对称加密的公钥Q作为公钥，k作为私钥[12]。区块链节点可以利用私钥生成公钥，但不能利用公钥生成私钥。在区块链加密应用中，分别保留和公开1个密钥，利用公开的密钥加密业务数据，利用保留的密钥解密进行查看。

$$kp=Q \tag{1}$$

为防止区块链的区块数据被篡改，引入Hash算法对业务数据进行单向数据Hash加密，生成固定长度的字符串，通过与时间戳结合，构建不可篡改的区块链数据。但区块链技术的加密算法需要结合具体业务需求进行算法重构，否则应用场景的数据依然存在安全隐患。

1.2 区块链数据加密安全隐患

1.2.1 传统区块链数据安全保护分析

随着区块链技术在电力系统中的应用和试点部署，负荷侧的市场主体从互联网接入电网安全网络，按照电网运营机构对电力调度和敏感数据的管理要求，区块链平台一般部署在安全内网，这导致链上数据不能在负荷侧的外网本地存储，只能通过数据安全访问通道在外网获得许可后访问内网的链上数据。这种方式由于未发挥区块链技术分布式存储、认证和交互的功能，难以构建透明、互动、共享的交易环境，同时安全网络与互联网间的逻辑隔离无法实现负荷侧市场主体执行数据上链的认证，因此开展区块链技术在互联网部署的配套保障方案研究是推动负荷侧互信电力交易环境构建的重要基础。

基于区块链技术的电力交易应用平台中，区块链技术不仅提供透明、可追溯的数据存储功能，还提供数据安全保护支撑。其中，数据加密技术保障主要体现在：区块链采用非对称和Hash加密的形式对调控运行的业务数据进行保护和验证；通过区块链应用平台分配参与用户的系统权限，防止敏感数据的扩散；按照区块链分布式数据广播机制，构建数据交互业务通道，隔离通道以外的恶意节点对业务数据的破坏。因此区块链技术可以提供安全的电力数据交互保障，但区块链技术的安全防护功能需要在确保节点私钥未泄露的前提下才能实现。如果节点私钥泄露，则恶意节点可以利用非法获取的节点私钥在区块链应用平台上以合法身份对发出的业务数据进行篡改和伪造。

1.2.2 区块链私钥保护分析

利用区块链加密技术可实现业务数据的安全、防篡改和可追溯等功能，参考目前的计算机算力，从区块链的系统节点地址和公钥逆向推导私钥的途径尚不可行[14]。但从区块链数据加密策略来看，系统节点的私钥是该节点身份的唯一标识，通过绑定节点ID地址来对ID地址上的资产进行管理操作，因此传统区块链技术数据安全防护的关键是私钥保护。

对区块链系统节点的私钥保护主要采用指纹、声纹、面部识别等技术对私钥进行二次加密，也有委托第三方可信机构进行私钥托管或者使用在线热钱包的方式进行互联网的私钥管理[15-16]。但因私钥管理不善或被窃取而导致节点账户资产损失的事件时有发生，且目前针对已泄露私钥的节点或者该节点所在区块链系统的数据安全缺乏主动防护的措施，因此，对于数据安全等级要求苛刻的电力系统，开展节点私钥泄露后的主动防护措施研究具有现实意义。

1.2.3 负荷侧电力数据安全隐患分析

在区块链应用平台上，如果调度中心节点或市场主体节点的私钥被窃取，则在区块链平台权限内丢失私钥节点的数据安全防护将会失效，更严重的是基于区块链技术的电力交易平台上的数据在节点之间进行传输时存在被截断、篡改、伪造等风险。

基于区块链技术在互联网部署电力应用平台，电力调控中心和市场主体间的数据交互网络架构拓扑如图1所示。调度中心将负荷侧调控需求数据穿

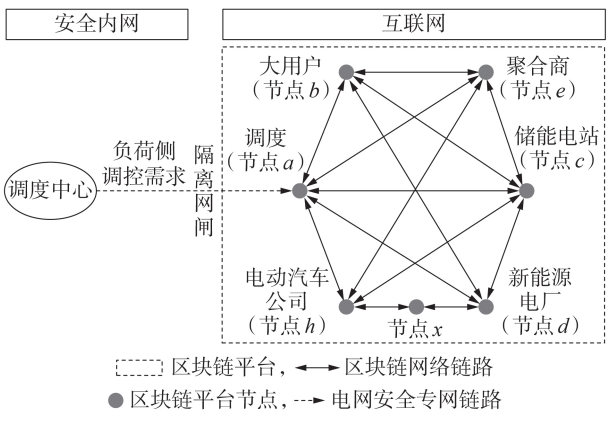

图1 互联网区块链数据交互拓扑图

Fig.1 Topological diagram of data interaction for Internet blockchain

过隔离网闸同步到外网的区块链平台调度节点并触发数据上链智能合约，上链调控数据经分布式广播网络同步更新区块链数据库数据并推送交易发布的信息，参与负荷侧电力交易的市场主体通过区块链平台申报交易数据给本时段优选出的算力最强节点进行自动交易匹配和出清，将交易出清数据进行分布式广播和确认，并将经过确认的出清数据更新区块链数据库进行分布式存储。

在互联网区块链交易平台上开展交易数据的交互主要面临的威胁包括：相比于传统电网安全网络，互联网的可控性和安全性均较差，遭受来自互联网的攻击威胁增多，且可防护的手段较少；负荷侧的市场主体（大用户、聚合商）网络安全意识和网络安全防护能力参差不齐，区块链身份密码的保护意识缺乏。

区块链技术能构建透明互信的交易环境，有利于提高负荷侧用户参与交易的积极性，但是传统区块链技术的加密算法存在系统节点私钥泄露后的数据安全防护风险，因此面向负荷侧的电力交易数据交互过程需要通过二次加密、交互验证的方式构建主动数据安全加密防护，利用其他节点私钥进行安全验证，确保市场主体交易数据的主动防御和预警。

2　加、解密方法与验证机制设计

为防止区块链系统节点私钥泄露后电力数据遭恶意篡改和伪造，在高安全等级需求的应用场景下运用区块链技术开展多重加密和验证技术研究[17-19]。本文引入随机数、随机数+业务数据、业务数据，利用非对称的公、私钥和Hash算法进行组合数据加密算法和数据交互验证设计，实现系统节点发出数据的防篡改和防伪造。

2.1　发送数据加密方法设计

传统区块链数据加密是以节点私钥未泄露为前提，因此传统电力交易业务数据的加密流程包括利用接收节点的公钥直接对电力数据进行非对称加密和Hash单向加密2个部分。传统发送数据加密流程见附录A图A1，加密方式如式（2）所示。

$$\begin{cases} \text{电力数据} \xrightarrow{\text{Hash}} N'_{\text{Num}} \\ \text{电力数据} \xrightarrow{P_{\text{key}}(B)} N'_{\text{Num1}} \end{cases} \tag{2}$$

式中：Hash表示利用Hash算法进行加密；$P_{\text{key}}(B)$表示利用接收节点B的公钥加密；N'_{Num}、N'_{Num1}分别为电力数据加密后的密文字符串和密文数据。

在传统区块链技术的数据加密算法中，如果数据发出节点的私钥泄露，则恶意节点可以利用获得的私钥对电力数据进行篡改并按照既定的Hash算法进行数据加密，从而实现电力数据的伪造，接收电力数据的节点根据接收到的指令内容操作自身发用电行为，这将对电力系统造成极大风险。为增强电力业务数据的安全性，本文引入随机数N_{Nonce}，通过本地生成N_{Nonce}，将电力数据与N_{Nonce}组成数组，采用非对称加密与Hash算法对电力数据进行格式化处理，同时利用接收节点的公钥对N_{Nonce}进行加密，生成密文N'_{Nonce}。同时，将N_{Nonce}与电力数据进行组合，利用Hash加密算法得到N_{Nonce}+电力数据的字符串摘要N'_{Num}。电力数据需要经过发出节点私钥签名，生成密文N_{Num1}，再利用接收节点公钥对N_{Num1}进行查询权限加密，生成仅可被接收节点解密查看的电力数据N'_{Num1}。最后，发出节点同时将N'_{Nonce}、N'_{Num}、N'_{Num1}打包，通过区块链的分布式广播机制进行发送。发送数据的加密流程图如图2所示，加密模型如式（3）所示。

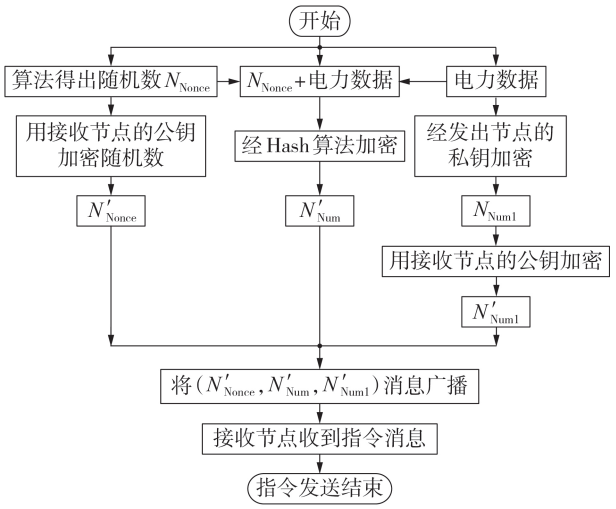

图2　发送数据加密流程图

Fig.2　Flowchart of sending data encryption

$$\begin{cases} N_{\text{Nonce}} \xrightarrow{P_{\text{key}}(B)} N'_{\text{Nonce}} \\ N_{\text{Nonce}} + \text{电力数据} \xrightarrow{\text{Hash}} N'_{\text{Num}} \\ \text{电力数据} \xrightarrow{S_{\text{key}}(A)} N_{\text{Num1}} \xrightarrow{P_{\text{key}}(B)} N'_{\text{Num1}} \end{cases} \tag{3}$$

式中：$S_{\text{key}}(A)$表示利用数据发出节点A的私钥进行加密。

2.2　接收数据解密方法设计

传统接收数据解密过程如附录A图A2和式（4）所示。如果数据发出节点的私钥已泄露，则伪造的电力数据被接收节点解密查看后将不会出现任何异常。同时根据工作量证明PoW（Proof of Work）的共识机制，一般超过51%的节点认证通过的电力数据会被执行，因此，接收节点按照伪造的电力数据执行是合法行为。

$$N'_{\text{Num1}} \xrightarrow{S_{\text{key}}(B)} \text{电力数据} \xrightarrow{\text{Hash}} N'_{\text{Num2}} \tag{4}$$

式中：$S_{\text{key}}(B)$表示利用接收节点B的私钥进行解密；N'_{Num2}为接收节点解密随机数和电力数据的组合

Hash字符串。

电力数据接收节点通过webservice或rest等方式接收电力数据密文$N'_{\text{Nonce}}+N'_{\text{Num}}+N'_{\text{Num1}}$的数据包。首先,将其分解为$N'_{\text{Nonce}}$、$N'_{\text{Num}}$、$N'_{\text{Num1}}$的独立数据段;其次,利用自身私钥对$N'_{\text{Nonce}}$和$N'_{\text{Num1}}$进行解密,返回明文$N_{\text{Nonce}}$和密文$N_{\text{Num1}}$,并利用发出节点的公钥对$N_{\text{Num1}}$进行二次解密获得电力数据的明文内容;然后,将解密获得的N_{Nonce}和电力数据进行组合,并通过Hash算法进行加密,生成字符串摘要N'_{Num2};最后,对比N'_{Num2}与接收到的N'_{Num}是否一致,如果一致,则判定电力数据在传输过程中没有被篡改过,否则向私钥对应的用户ID发送电力数据被篡改的告警信息。接收节点的密文解密流程如图3所示,解密模型如式(5)所示。

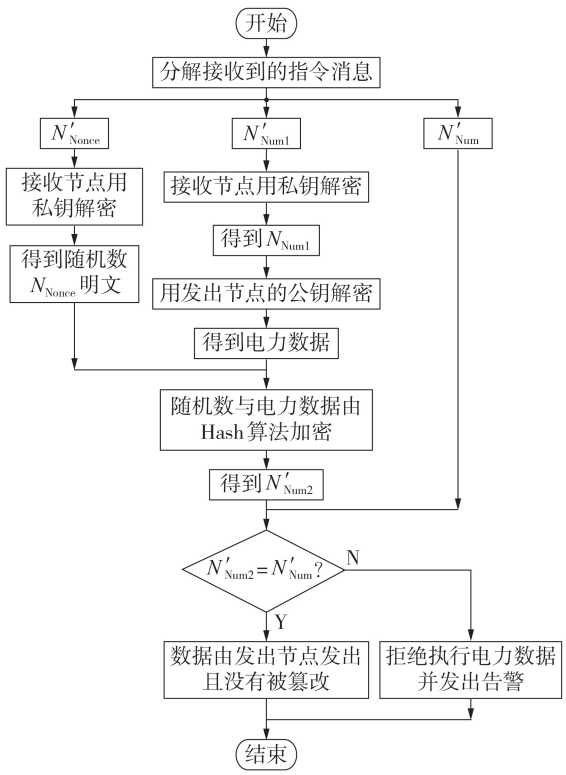

图3 接收数据解密流程图

Fig.3 Flowchart of receiving data decryption

$$\begin{cases} N'_{\text{Nonce}} \xrightarrow{S_{\text{key}}(B)} N_{\text{Nonce}} \\ N'_{\text{Num1}} \xrightarrow{S_{\text{key}}(B)} N_{\text{Num1}} \xrightarrow{P_{\text{key}}(A)} \text{电力数据} \\ N_{\text{Nonce}}+\text{电力数据} \xrightarrow{\text{Hash}} N'_{\text{Num2}} \end{cases} \tag{5}$$

式中:$P_{\text{key}}(A)$表示利用发出节点A的公钥解密。

2.3 数据交互验证机制

基于区块链系统的节点间信息共享采用分布式广播机制,比特币和以太坊分别用Gossip、Kademlia协议进行节点间的数据交互,保障区块链电力应用系统的节点分布式数据库的数据同步[20]。传统的区块链数据验证机制是通过非对称公、私钥和Hash加密方式来验证确定数据的发出节点,但是并不会主动检测交互的业务数据是否为节点私钥泄露后由恶意节点伪造或篡改发出的,因此如果区块链系统节点私钥泄露后的数据被篡改将无法被识别和防护。为防止恶意节点利用指令发送节点私钥伪造电力数据和随机数,通过系统电力数据加密和发送机制伪造指令数据,误导接收节点错误响应指令要求,需要在防止数据被篡改的加密机制基础上,结合区块链的分布式数据广播机制开展电力数据交互认证流程的数据防伪造验证机制设计。

防止电力数据被伪造的认证流程如图4所示。电力密文数据验证流程分为3步,包括密文发送、签名摘要返回、公钥确认数据回执。在基于区块链技术的电力应用平台上,发出节点A在本地按照式(3)对随机数、电力数据进行加密,生成$N'_{\text{Nonce}}+N'_{\text{Num}}+N'_{\text{Num1}}$并执行密文上链,通过分布式网络广播更新系统所有节点的本地数据库。接收节点B利用私钥对更新数据进行解密,如果解密成功,则将随机数与电力数据经Hash加密算法加密后用私钥签名广播返回给节点A,节点A接收返回的摘要密文(N_{Nonce}与电力数据),利用节点B的公钥进行解密,对比判断N_{Nonce}与电力数据是否正确,并返回确认摘要,节点B根据确认摘要执行电力数据。

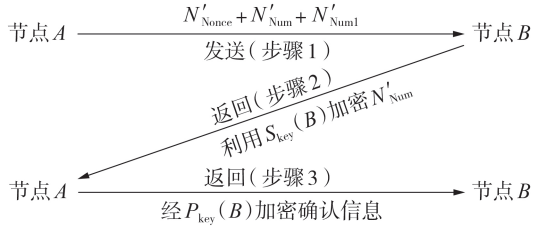

图4 电力数据交互验证流程图

Fig.4 Flowchart of power data interactive verification

为了应对紧急情况,当数据交互过程超时数据发出节点未收到反馈信息或数据接收节点信息验证出现差错时,信息验证节点均将通过安全网络发送告警信息给对应主体,确认对应节点状态和密钥安全。

3 电力数据防伪分析

3.1 电力数据交互风险分析

对于负荷侧部署区块链交易平台开展电力交易,如果系统中存在若干节点私钥泄露,则该交易数据的发布、申报、认证均存在安全风险,一般主导电力需求发布节点的私钥泄露给系统带来的影响最大。针对复杂的互联网环境,在区块链电力应用的负荷侧电力需求发布环节中存在的风险主要分为3种情况:情况1,恶意节点窃取数据发出节点的私钥,但不知道接收节点的信息,即无法获得接收节点

公钥；情况 2，恶意节点窃取数据发出节点的私钥，且知道接收节点的信息，即获得了接收节点公钥；情况 3，恶意节点窃取数据发出节点的私钥，获得了接收节点公钥，且具有短暂区块链网络通信控制能力，包括截断替换、泛洪、阻断等网络攻击能力。

1）情况 1。在加密阶段，拥有电力数据发出节点私钥的恶意节点可以对数据进行篡改，具体见附录 A 图 A3 的阴影部分。但由于缺乏接收节点信息，无法利用接收节点的公钥对 N_{Num1} 进行加密且不能修改随机数，即无法生成 N_{Nonce} 与电力数据的 Hash 字符串。本文设计的加密方式可以防止在电力数据发出节点私钥泄露的情况下电力数据内容被篡改。同理，恶意节点仅有数据发出节点的私钥，无法进一步利用接收节点的公钥对伪造的电力数据进行加密且无法获得随机数，从而在未知接收节点公钥的情况下，伪造的电力数据无法通过接收节点的本地解密验证过程，这将导致验证反馈失败。综上，恶意节点无法伪造完整的 N'_{Nonce}、N'_{Num}、N'_{Num1}，即恶意节点篡改和伪造电力数据失败。

2）情况 2。在情况 1 的基础上，由于恶意节点已知接收节点的信息，可以使用接收节点的公钥进行签名成功篡改 N'_{Num1} 的内容，见附录 A 图 A4 的步骤 3。但是由于恶意节点不知道接收节点的私钥，无法获得随机数明文，因此图 A4 中步骤 1 和步骤 2 的内容篡改失败。

获得了接收节点信息的恶意节点，可以通过伪造随机数和电力数据来伪造密文，并替代原数据发出节点的电力数据，见附录 A 图 A5。接收节点接收到伪造数据的密文数据包后，根据图 3 的解密验证步骤，可以按照系统既定的数据解密方式完成本地电力数据的验证，即可以本地验证通过 $N'_{\mathrm{Num2}}=N'_{\mathrm{Num}}$。因此，单纯的加密方法无法防范区块链电力应用系统中节点私钥泄露的数据被伪造的隐患。

针对情况 2 的数据防伪造需求，利用本文的数据交互验证机制进行数据防伪分析。结合图 1 中节点间的数据交互方式，情况 2 下恶意节点伪造确认信息的示意图见附录 A 图 A6。由于节点 A 发出的数据被恶意节点截断并伪造，因此接收节点 B 接收到的密文可能为伪造信息，如图 A6 中虚线箭头的步骤 1 所示。但恶意节点没有接收节点的私钥，无法对节点 B 的返回信息进行伪造传递给节点 A，因此步骤 2 为安全步骤。由于分布式广播机制会将确认信息返回给恶意节点，因此恶意节点利用节点 A 的私钥对伪造的信息进行签名，并发出验证通过的信息返回给节点 B。节点 A 收到节点 B 的返回信息后发现伪造信息与自身发出的信息不一致，发出告警信息分别广播至系统所有节点，通过分布式广播机制将验证结果传递到节点 B。节点 B 会收到 2 种完全相反的验证确认信息，分别来自恶意节点和节点 A、C、D、H，从而篡改的恶意信息无法通过节点 B 的本地验证，节点 B 不会执行恶意节点的伪造信息，恶意节点破坏电力系统运行的行为失败。节点 A 通过约定的危机数据交互模型进行数据交互，确保数据的安全送达并结合电力数据泄露现象开展私钥安全检测。

3）情况 3。此时恶意节点在保证自身安全（指窃取私钥的行为和短时控制某个节点通信的恶意行为不被发现）的情况下，结合图 1 中节点间的数据交互方式，可以得到情况 3 下电力数据交互过程中可能受到篡改和伪造的数据传输链路如图 5 中虚线所示，图中，灰色底纹表示恶意节点短时控制了节点 B。

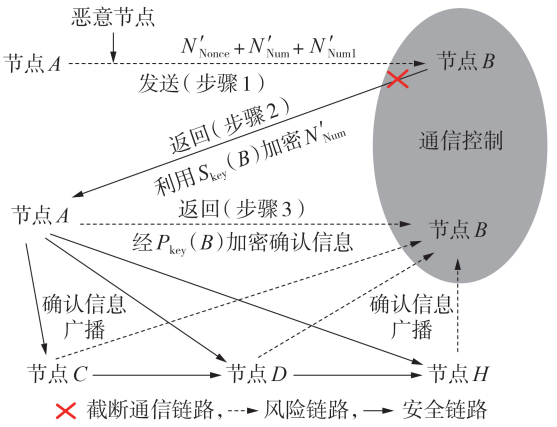

图 5　恶意节点具备通信控制时受影响的数据链路示意图

Fig.5　Schematic diagram of data links affected by malicious nodes with communication control

图 5 中：在步骤 1，恶意节点截断节点 A 发出的电力数据信息，利用系统数据加密规则伪造恶意电力数据和随机数，将生成的伪造密文替换原电力数据并传送给节点 B；在步骤 2，恶意节点截断节点 B 发送给节点 A 的确认信息并利用节点 A 的私钥伪造返回确认信息，完成信息验证的闭环。

恶意节点篡改数据的行为能否成功分为 2 种情形：情形 1，恶意节点伪造节点 A 的电力数据发送给节点 B；情形 2，恶意节点凭空制造电力数据发送给节点 B。针对情形 1，恶意节点在控制节点 B 数据验证交互通信的基础上，可以完成电力数据的验证，但由于恶意节点没有节点 B 的私钥，无法在规定的时间内返回利用 $S_{\mathrm{key}}(B)$ 加密的 N'_{Num}，这会引起节点 A 发出超时无返回信息的告警，阻止恶意节点的电力数据被节点 B 执行，保证电力系统的安全稳定运行。针对情形 2，恶意节点伪造电力数据并阻断节点 B 与节点 A、C、D、H 的数据交互验证，同时私钥丢失的节点 A 也不会发出数据验证返回超时的告警。因此，恶意节点制造的电力数据会被接收节点接收并执行，从而破坏电力系统稳定运行。

3.2 风险概率模型

基于3.1节的分析，恶意节点获取数据发出节点的私钥后，将给区块链应用系统的业务数据安全带来潜在的风险，包括电力数据的篡改和伪造。恶意节点只有同时完成电力数据加、解密和数据交互验证，才能在保证自身安全的前提下破坏基于区块链的电力系统运行。因此，需要从恶意节点获取数据发出节点私钥后的数据加、解密和数据交互验证2个部分分析数据模型。

$$M = N\rho(i^2 + iN) \tag{6}$$

式中：M为加密数据被篡改的风险概率；N为随机数被泄露的概率；ρ为恶意节点获取接收节点信息的概率；i为私钥被泄露的概率。

$$Y = fmq \tag{7}$$

$$Y = (ML)(i\rho J_s)\frac{gL}{n-2} = \frac{Mi\rho gL^2 J_s}{n-2} \tag{8}$$

式中：Y为验证阶段的风险概率；f为数据交互发送的风险概率；m为接收节点返回认证N'_{Num}的私钥签名被泄露的风险；q为验证确认信息被篡改的风险；L为网络控制能力；J_s为电力数据接收节点私钥被泄露的概率；g为通过系统共识机制认证的概率，当网络控制力超过51%的节点时其值为1，否则为0；n为区块链系统的节点数。

随机数的安全性由接收节点私钥被泄露的概率决定，即：

$$N = J_s \tag{9}$$

则基于区块链技术的电力数据发出节点私钥被泄露后数据被篡改或伪造的风险F可表示为：

$$F = MY \tag{10}$$

4 算例分析

在互联网中建设基于区块链技术的源网荷储调控平台，接入电动汽车公司、负荷聚合商、调度中心、大用户、售电公司等共50个市场主体节点。以图1的区块链网络架构为基础，区块链应用平台的各节点间以分布式广播机制进行数据交互。本文以调度中心节点私钥被泄露、恶意节点试图破坏正常电力调控运行为背景，开展加密算法和机制设计验证。结合风险概率模型与3.1节中数据交互的3种情况进行分析。

情况1下，结合图1和图3的数据发出节点、接收节点及恶意节点间的数据广播交易机制，由于恶意节点不知道接收节点的信息，无法查看截获的密文数据包(N'_{Nonce}, N'_{Num}, N'_{Num1})，则电力数据的篡改将会失败，即利用本文加密算法的节点私钥泄露导致数据被篡改的概率为0。同时，恶意节点可伪造电力数据并利用数据发出节点的私钥加密生成密文N_{Num1}，但由于恶意节点不知道接收节点信息，随机选择一个系统节点的公钥进行加密，则在加密阶段成功伪造N'_{Num1}并生成对应伪造密文N''_{Num1}的概率为1/48。在数据交互验证阶段，恶意节点将伪造的密文(N'_{Nonce}, N'_{Num}, N''_{Num1})发送给接收节点进行本地解密验证，由于将对N''_{Num1}解密得到的电力数据与N_{Nonce}结合并利用Hash算法加密后生成的字符串与N'_{Num}不一致，因此恶意节点在情况1下伪造电力数据的概率为0。

情况2下，恶意节点可以利用接收节点的公钥对N_{Num1}进行加密生成N'_{Num1}，并生成对应的伪造密文N''_{Num1}，但由于缺乏接收节点的私钥，不能获得N_{Nonce}，从而无法成功篡改电力数据，即电力数据被篡改的概率为0。但恶意节点通过接收节点公钥顺利伪造N''_{Num1}概率为100%，即恶意节点在加密阶段伪造N'_{Num1}成功。在数据交互验证阶段，恶意节点将伪造的密文(N'_{Nonce}, N'_{Num}, N''_{Num1})发送给接收节点进行本地解密验证。与情况1相同，由于无法获得和伪造N_{Nonce}，因此不能通过接收节点的本地验证，即恶意节点在情况2下伪造和篡改电力数据成功的概率为0。

情况3下，由于恶意节点没有接收节点的私钥，无法获得N_{Nonce}，因此篡改的电力数据无法通过接收节点的本地解密验证，即恶意节点篡改数据成功的概率为0。在该情况的情形1下，由于恶意节点能够控制通信网络阻断接收节点的验证返回过程，因此恶意节点可以重新伪造一个调控指令密文替换调控节点发出的密文，接收节点接收到伪造数据后，恶意节点通过控制接收节点的通信并利用“堡垒机”代替其他节点返回确认的伪造电力数据接收节点本地验证。电力数据发出节点在超时未收到利用接收节点私钥加密的返回信息后，向系统发出超时告警信息或通过备用通信系统与接收节点进行信息交互，因此设置返回确认的时间短于电力指令执行时间可以确保恶意节点伪造的电力数据信息不被执行，即恶意节点伪造电力数据成功的概率为0，则$Y=0$。在该情况的情形2下，由于恶意节点拥有控制接收节点网络通信的能力，当恶意节点利用某节点的私钥伪造没有发出的电力数据时，数据发出节点不会有数据验证返回超时的告警，即恶意节点通过控制接收节点的通信完成数据交互验证，诱导接收节点执行伪造电力数据，则$Y=100\%$。

综上，在系统节点私钥泄露率低于51%时，采用传统方法与本文方法的50个节点的数据防篡改防护率和防伪造防护率分别见表1和表2。

表1中，由于本文设计的组合加密方法引入N_{Nonce}，并利用接收节点的公钥和私钥加密，可以确保电力交易业务数据的安全。

表2中，在恶意节点具备数据伪造能力的情况(情况2、3)下，当且仅当恶意节点能够控制接收节点网络通信时才可以伪造数据并使接收节点执行，因此本文设计的数据加密和验证机制对防止数据被伪造具有较好的效果。

表 1　私钥泄露情况下数据防篡改防护率

Table 1　Data anti-tampering protection rate under condition of private key leakage

情况	防篡改防护率 / %			
	加密阶段		交互验证阶段	
	传统方法	本文方法	传统方法	本文方法
1	0	100	0	100
2	0	100	0	100
3	0	100	0	100

表 2　私钥泄露情况下数据防伪造防护率

Table 2　Data anti-counterfeiting protection rate under condition of private key leakage

情况	防伪造防护率 / %			
	加密阶段		交互验证阶段	
	传统方法	本文方法	传统方法	本文方法
1	0	97.96	0	100
2	0	0	0	100
3（情形 1）	0	0	0	100
3（情形 2）	0	0	0	0

综合表 1 和表 2 可以得出表 3 的综合对比结果。恶意节点需要同时突破本文设计的加密算法和交互验证机制才可以控制接收节点进行违规操作或误动，因此针对 3 种情况本文的数据安全防护相较于传统区块链的加密和验证机制有很大的提升。情况 3（情形 2）相当于获得了数据发出节点的私钥且控制了接收节点的网络，这种情况对恶意节点的要求极高，恶意节点无需伪造和篡改指令数据，而只需直接控制节点行为。

表 3　私钥泄露情况下传统方法与本文方法防护效果对比

Table 3　Comparison of protection effect between traditional method and proposed method

情况	防篡改		防伪造	
	传统方法	本文方法	传统方法	本文方法
1	×	√	×	√
2	×	√	×	√
3（情形 1）	×	√	×	√
3（情形 2）	×	×	×	×

注：“×”表示不支持，“√”表示支持。

综合表 3 的分析结果可知，本文设计加密环节对于数据防篡改和防伪造均具有较好的效果，但当区块链系统网络被恶意节点控制之后，本文所设计的解密和数据交互验证机制的防护效果与区块链传统数据签名方式相同，均会失效。同时，本文的数据计算结果是在共识机制有效的情况下得到的，需要保证私钥泄露的节点数小于总节点数的 51%。

5　结论

本文通过引入随机数与电力数据的组合，将非对称加密和 Hash 算法相结合，构建由数据发出节点和接收节点多重数据签名的方式确保数据发出节点私钥泄露的密文不可篡改。同时，引入数据交互验证机制，保证数据发出节点私钥泄露情况下的电力数据防伪造。算例结果表明，本文的电力数据加密方式能够有效防止数据被篡改和伪造，仅当区块链网络被恶意节点控制时电力数据存在被伪造的可能。

本文加密方式是在原有区块链数据加密技术的基础上构造的，基础支撑技术成熟，能够适用于电力交易应用的数据加密操作。但相较于传统区块链数据加密和共识验证机制，本文设计的二次加密和交互验证机制可能会在一定程度上降低区块链技术的数据交互效率。未来需要在保证数据交互安全的前提下进行数据加密和交互验证机制的优化，确保安全高效的分布式数据交互。

附录见本刊网络版（http://www.epae.cn）。

参考文献：

[1] 徐嘉辉，马立新. 区块链技术在分布式能源交易中的应用[J]. 电力自动化设备，2020，40(8)：17-22，30.
XU Jiahui，MA Lixin. Application of blockchain technology in distributed energy transaction[J]. Electric Power Automation Equipment，2020，40(8)：17-22，30.

[2] 陈冠廷，张利，刘宁宁，等. 基于区块链的面向居民用户需求响应交易机制[J]. 电力自动化设备，2020，40(8)：9-17.
CHEN Guanting，ZHANG Li，LIU Ningning，et al. Blockchain-based transaction mechanism for residential users demand response[J]. Electric Power Automation Equipment，2020，40(8)：9-17.

[3] 徐嘉辉，马立新. 区块链技术在分布式能源交易中的应用[J]. 电力自动化设备，2020，40(8)：17-22，30.
XU Jiahui，MA Lixin. Application of blockchain technology in distributed energy transaction[J]. Electric Power Automation Equipment，2020，40(8)：17-22，30.

[4] 秦金磊，孙文强，朱有产，等. 微电网中基于区块链的电能交易方法[J]. 电力自动化设备，2020，40(11)：130-138.
QIN Jinlei，SUN Wenqiang，ZHU Youchan，et al. Energy transaction method of microgrid based on blockchain[J]. Electric Power Automation Equipment，2020，40(11)：130-138.

[5] 朱鹏，胡剑，吕宋皓，等. 基于区块链的社交网络隐私数据保护方法研究[J]. 情报科学，2021，39(3)：94-100.
ZHU Peng，HU Jian，LÜ Songhao，et al. Blockchain-based privacy data protection in social networks[J]. Information Science，2021，39(3)：94-100.

[6] 马臣云. 基于密钥分割实现区块链私钥保护的方法及系统：CN106548345A[P]. 2017-03-29.

[7] 牛淑芬，刘文科，陈俐霞，等. 基于联盟链的可搜索加密电子病历数据共享方案[J]. 通信学报，2020，41(8)：204-214.
NIU Shufen，LIU Wenke，CHEN Lixia，et al. Electronic medical record data sharing scheme based on searchable encryption via consortium blockchain[J]. Journal on Communications，2020，41(8)：204-214.

[8] 王蓓蓓，李雅超，赵盛楠，等. 基于区块链的分布式能源交易关键技术[J]. 电力系统自动化，2019，43(14)：53-64.
WANG Beibei，LI Yachao，ZHAO Shengnan，et al. Key technologies of distributed energy trading based on blockchain[J]. Automation of Electric Power Systems，2019，43(14)：53-64.

[9] 谢开，张显，张圣楠，等. 区块链技术在电力交易中的应用与展

望[J]. 电力系统自动化,2020,44(19):19-28.
XIE Kai,ZHANG Xian,ZHANG Shengnan,et al. Application and prospect of blockchain technology in electricity trading [J]. Automation of Electric Power Systems,2020,44(19):19-28.
[10] 王胜寒,郭创新,冯斌,等. 区块链技术在电力系统中的应用:前景与思路[J]. 电力系统自动化,2020,44(11):10-24.
WANG Shenghan,GUO Chuangxin,FENG Bin,et al. Application of blockchain technology in power systems:prospects and ideas[J]. Automation of Electric Power Systems,2020,44(11):10-24.
[11] GUAN Z T,LU X,YANG W T,et al. Achieving efficient and privacy-preserving energy trading based on blockchain and ABE in smart grid[J]. Journal of Parallel and Distributed Computing,2021,147:34-45.
[12] 梅文明,李美成,孙炜,等. 一种面向分布式新能源网络的终端安全接入技术[J]. 电网技术,2020,44(3):953-961.
MEI Wenming,LI Meicheng,SUN Wei,et al. Terminal security access technology for distributed new energy networks[J]. Power System Technology,2020,44(3):953-961.
[13] 韩璇,袁勇,王飞跃. 区块链安全问题:研究现状与展望[J]. 自动化学报,2019,45(1):206-225.
HAN Xuan,YUAN Yong,WANG Feiyue. Security problems on blockchain:the state of the art and future trends[J]. Acta Automatica Sinica,2019,45(1):206-225.
[14] 翟峰,杨挺,曹永峰,等. 基于区块链与*K*-means算法的智能电表密钥管理方法[J]. 电力自动化设备,2020,40(8):38-46.
ZHAI Feng,YANG Ting,CAO Yongfeng,et al. Key management method of smart meter based on blockchain and *K*-means algorithm[J]. Electric Power Automation Equipment,2020,40(8):38-46.
[15] FRÖHLICH A,CIACH M. Dead tree branches in urban forests and private gardens are key habitat components for woodpeckers in a city matrix[J]. Landscape and Urban Planning,2020,202:103869.
[16] 秦艳琳,吴晓平,胡卫. 多重PKG环境中高效的身份基认证密钥协商协议[J]. 计算机科学,2020,47(11):68-72.
QIN Yanlin,WU Xiaoping,HU Wei. Efficient identity-based authenticated key agreement protocol with multiple private key generators[J]. Computer Science,2020,47(11):68-72.
[17] JUNG J,LEE D,LEE H,et al. Security enhanced anonymous user authenticated key agreement scheme using smart card[J]. Journal of Electronic Science and Technology,2018,16(1):45-49.
[18] KUMAR A,OM H. An improved and secure multiserver authentication scheme based on biometrics and smartcard[J]. Digital Communications and Networks,2018,4(1):27-38.
[19] 詹丽,姚国祥,强衡畅. 改进的基于smartcard的云用户双向认证方案[J]. 计算机工程与设计,2014,35(2):440-444.
ZHAN Li,YAO Guoxiang,QIANG Hengchang. Improved mutual authentication scheme based on smartcard for cloud computing [J]. Computer Engineering and Design,2014,35(2):440-444.
[20] 陈思捷,王浩然,严正,等. 区块链价值思辨:应用方向与边界[J]. 中国电机工程学报,2020,40(7):2123-2132,2392.
CHEN Sijie,WANG Haoran,YAN Zheng,et al. Rethinking the value of blockchain:direction and boundary of blockchain applications[J]. Proceedings of the CSEE,2020,40(7):2123-2132,2392.

作者简介:

吉 斌

吉 斌(1992—),男,安徽马鞍山人,工程师,硕士,主要研究方向为区块链技术、电力市场、电力调度(**E-mail**:1498206259@qq.com);

昌 力(1982—),男,安徽巢湖人,高级工程师,硕士,主要研究方向为电力系统调度自动化及电力市场(**E-mail**:changli80@163.com);

朱丽叶(1995—),女,安徽安庆人,工程师,硕士,主要研究方向为电力自动化调度、区块链技术应用开发(**E-mail**:zhuliye@sgepri.sgcc.com.cn)。

(编辑 王锦秀)

Anti-tampering method and verification mechanism design of power data for private key leakage of node in blockchain system

JI Bin[1,2],CHANG Li[1,2],ZHU Liye[1,2],CAO Bin[1,2]

(1. NARI Group Corporation(State Grid Electric Power Research Institute Co.,Ltd.),Nanjing 211106,China;
2. NARI Technology Co.,Ltd.,Nanjing 211106,China)

Abstract: In the power application system based on blockchain technology,there exists a risk of malicious tampering or forgery of signature power data of node whose private key is leaked,and there is no effective protection measures at present,for which,a data encryption method and a data interactive verification mechanism are proposed. Combined with the principle of blockchain basic encryption technology,a combination method of random number and power data is proposed,and the asymmetric encryption algorithm and Hash algorithm are used for multiple encryption,and a data anti-tampering encryption method after private key leakage of data sending node is constructed. In order to prevent malicious nodes from using the private key of data sending node to forge and replace the power data,an interactive verification mechanism of power data is designed,the private key of data sending node is used for encryption,and the public and private keys of receiving node are used for decryption and verification. The data model of encryption,decryption and data interactive verification mechanism is abstracted. Example analysis verifies the effectiveness of the proposed data encryption method and data interactive verification mechanism.

Key words: blockchain; private key leakage; encryption method; data interactive verification; anti-tampering; anti-forgery

附录 A：

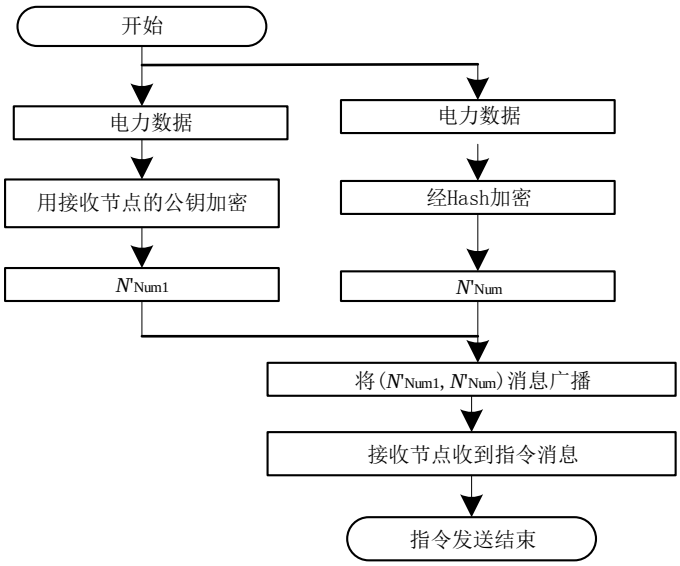

图 A1 传统发送数据加密流程图

Fig.A1 Flowchart of traditional sending data encryption

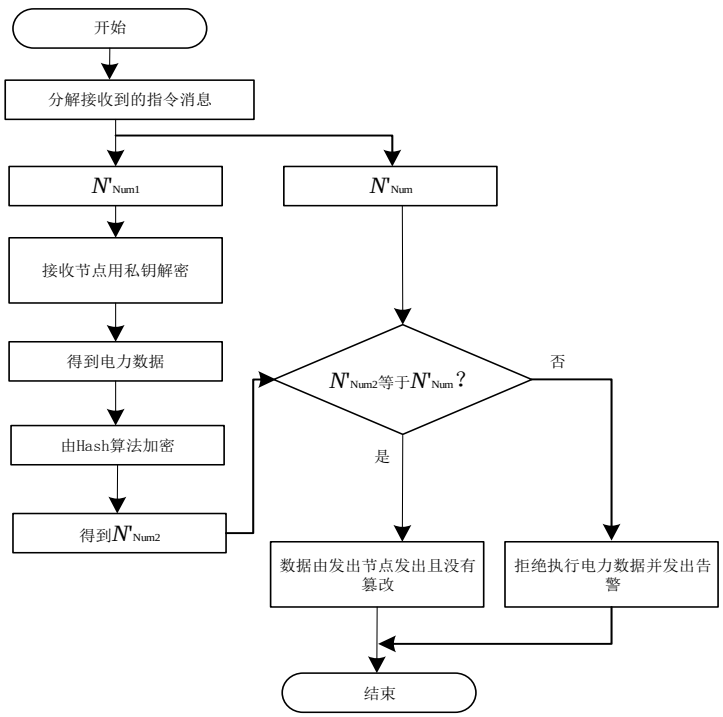

图 A2 传统接收数据解密流程图

Fig.A2 Flowchart of traditional received data decryption

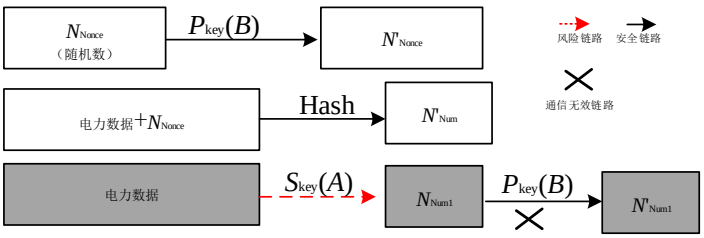

图 A3 恶意节点仅获得私钥的可篡改操作

Fig.A3 Tamperable operation of malicious node when it only obtains private key

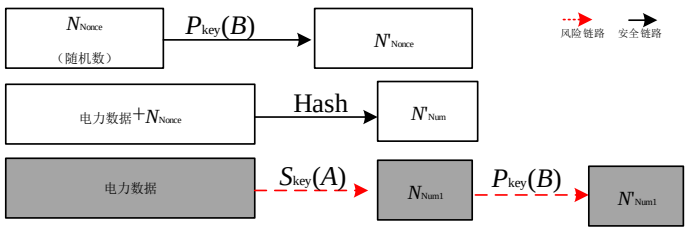

图 A4 恶意节点获得私钥和接收节点信息的可篡改操作

Fig.A4 Tamperable operation of malicious node when it obtains private key and information of receiving node

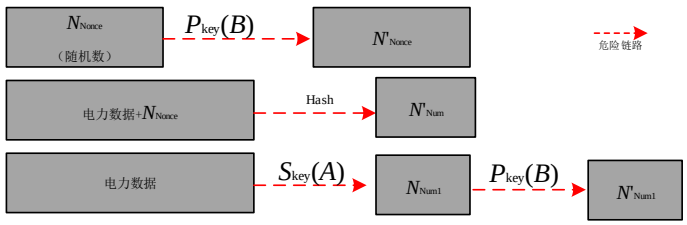

图 A5 恶意节点获得私钥和接收节点信息的伪造数据操作

Fig.A5 Forging data operation of malicious node when it obtains private key and information of receiving node

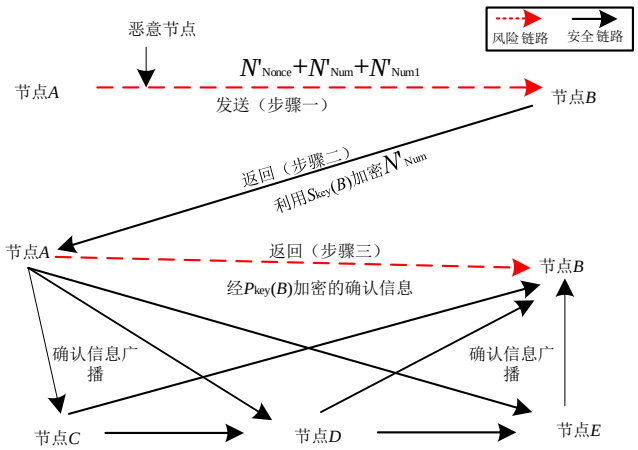

图 A6 恶意节点伪造确认信息的示意图

Fig.A6 Schematic diagram of malicious node forging confirmation information