计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(2):89−96 [doi: 10.15888/j.cnki.csa.007795]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链的物联网大坝监测系统架构①

胡忠启[1], 赵　锋[1], 李雪强[1], 阎　峻[2], 江　帆[2]

[1](华东桐柏抽水蓄能发电有限责任公司, 杭州 310003)
[2](国网新源控股有限公司, 北京 100761)
通讯作者: 胡忠启, E-mail: 1043079139@qq.com

摘　要: 针对大坝监控数据存在的安全性与可靠性隐患问题, 本文提出了一种基于区块链 (BC) 的由传感器云和无人机云组成的系统架构, 以用于监控大坝和确保数据的安全性与可靠性. 其中传感器云提供各种感测数据, 无人机 (UAV) 云则收集这些数据并将其传送到大坝监控中心 (DMC), 区块链技术用于保证数据的完整性、真实性、安全性和可追溯性. 分析表明, 所提出的系统具有很好的伸缩性, 并可以有效保证大坝监测数据来源的可靠性, 数据传输的安全性以及预防潜在的数据攻击. 最后, 本文通过评估数据传递延迟率来评估工作绩效, 仿真结果表明, 所设计系统的延迟率与生成事件概率、重访时间成正相关, 与警报间隔时间成负相关, 且具有更高的支付成功率.

关键词: 区块链; 传感云; 无人机云; 大坝监测; 数据传递延迟率

引用格式: 胡忠启,赵锋,李雪强,阎峻,江帆.基于区块链的物联网大坝监测系统架构.计算机系统应用,2021,30(2):89–96. http://www.c-s-a.org.cn/1003-3254/7795.html

Architecture of IoT Dam Monitoring System Based on Blockchain

HU Zhong-Qi[1], ZHAO Feng[1], LI Xue-Qiang[1], YAN Jun[2], JIANG Fan[2]

[1](East China Tongbai Pumped Storage Power Co. Ltd., Hangzhou 310003, China)
[2](State Grid Xinyuan Company Ltd., Beijing 100761, China)

Abstract: With regard to the hidden security and reliability problems of dam monitoring data, this study proposes a system architecture composed of sensor cloud and the Unmanned Aerial Vehicle (UAV) cloud based on BlockChain (BC) technology for monitoring dams to ensure the security and reliability of data. The sensor cloud provides various sensing data, while the UAV cloud collects these data and transmits them to the Dam Monitoring Center (DMC), and the BC technology is applied to ensuring integrity, authenticity, security and traceability of data. The analysis shows that the proposed system has good scalability, which can effectively guarantee the reliable sources of monitoring data and the security of data transmission and prevent potential data attacks. Finally, this study assesses the work performance by evaluating the delay rate of data transfer. The simulation results reveal that the delay rate of the designed system is positively correlated with the probability of generating events and revisit time, but negatively correlated with the alarm interval time, and it presents a higher payment success rate.

Key words: Blockchain; sensor cloud; drone cloud; dam monitoring; data transfer delay rate

为了保水并帮助减轻洪水, 通常, 需要在暴雨之前、之中和之后测量水深以确保水坝的安全性, 因此, 不断监测水库中的水位和天气状况对降低洪水灾害的危险至关重要[1]. 但由于大坝周围环境的干扰, 大坝监控设备布置稀疏等原因, 导致大坝监测数据不可靠和不安全[2], 因此制定一个可靠安全的大坝监控方案以确保数据的安全性和可靠性是十分有必要的.

近年来, 云计算和物联网[3,4] 的发展催生了一套新

① 收稿时间: 2020-06-09; 修改时间: 2020-07-14, 2020-07-29; 采用时间: 2020-08-10; csa 在线出版时间: 2021-01-27

的智能服务和应用程序, 在这种情况下, 云和物联网在大坝监控中的结合使用将提供应对水挑战的新方法. 文献 [5] 研究了水力发电厂结构大坝安全监控系统, 该系统使用标准协议 XMPP 在安装在听诊仪器上的不同传感器之间提供通信服务. 文献 [6] 描述了在特定的大坝安全管理系统中应用物联网的可能性, 定义了一个新的数据采集模块, 用于与监控网络中的传感器通信. 文献 [7] 为了减少了人工干预大坝结构的施工和运营成本, 提出了智能水坝结构化系统, 将物联网、智能监控、云计算和控制技术智能地集成在一起, 以在整个生命周期内实施实时, 在线进行个人管理与分析, 并对其性能进行控制. 文献 [8] 提出了一种新颖的集成信息系统, 它结合了物联网 (IoT)、云计算、地理信息学以及电子科学用于环境监测和评估. 文献 [9] 基于物联网和 5G 无线网络, 利用传感器数据构建尾矿坝多关键信息系统, 包括潜水线, 水库水位, 尾矿坝内部和外部变形等稳定性指标, 应用云平台基于实时监测数据预测潜水线的未来状态. 文献 [10] 分析了当前我国水库大坝安全管理存在的问题, 并以 F 大坝为例, 探讨了基于物联网技术与云技术的大坝安全管理系统的具体建构. 但以上这些工作没有提供全球大坝监测解决方案, 而且, 它们非常昂贵, 并且不提供可伸缩性和安全性.

本文提出了一种基于区块链 (BC)[11,12] 技术并由传感器云和无人机云组成的系统架构, 包括: (1) 一组传感器小云, 用于测量各种数据, 例如天气状况, 水质和水位以及大坝的结构状态; (2) 由无人机提供商控制的一组无人机小云, 负责数据传输. BC 技术可以解决与数据伪造和重播有关的潜在安全威胁, 保证数据完整性和数据不可伪造性. 其中, 传感器云的使用可以带来了许多益处, 包括解决方案的普遍性, 可伸缩性和可重用性. 而且, 小云可以服务于各种应用, 例如, 集成了一组用于测量气候条件的传感器的气象站可以同时用于设计应用程序和其他解决方案, 例如农业监测. 而使用 UAV 云进行数据传输, 可以有效解决面积大而基础设施较少、部署的传感器形成遥远且孤立的小云地区的数据传输问题.

1 系统架构

1.1 系统架构描述

本文设计的体系结构的目标是使 DMC 能够确保数据完整性, 数据支付的可追溯性以及行为人的报酬. 图 1 为系统架构图, 图 2 为系统流程图.

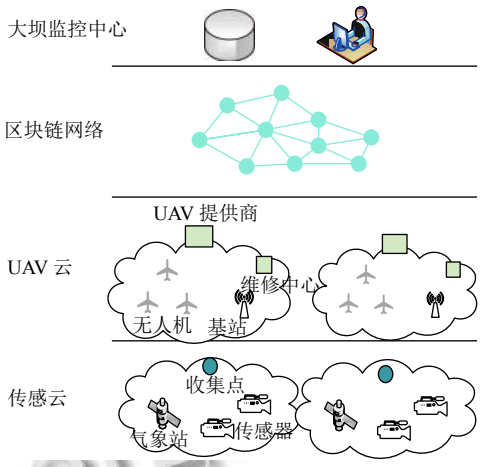

图 1 系统架构

传感器云[13]: 由散布在该区域并提供各种数据的一组传感器云组成. 每个小云与控制和配置传感器的 WSN(气象站) 代理进行交互. 每个小云均包含一组传感器和一个固定的收集点 (CP), 具体包括: (1) 一个或多个气象站, 这些气象站安装在农场的露天环境中; (2) 一套水位和水质传感器, 用于测量物理和化学水参数; (3) 一组用于监测大坝结构状态的传感器. 其中, 固定 CP 具有更多的计算和通信资源. 每个 CP 执行: (1) 从小云收集和聚合传感器数据; (2) 审计: 它验证是否从无人机提供商那里收到了发票中所有元组的付款.

无人机云: 由一组无人机小云组成, 并与无人机代理进行交互. 无人机云可以通过添加更多无人机提供商来提供可伸缩性, 并且可以为许多应用程序提供服务. 每个小云均由提供商控制, 并由一组基站 (BS), 一组维护中心和一组无人机 (例如四旋翼飞机) 组成. 无人机从 CP 收集数据并将其传输给提供商. 无人机作用有: (1) 接收和存储请求: 它从 DMC 接收请求, 然后将其存储以供以后验证; (2) 选择将要处理请求的无人机提供商; (3) 发票的产生: 它创建一个发票, 其中包含与给定请求有关的锚定到 BC 的元组列表, 然后将其发送给 DMC 以接收付款; (4) 审计: 它验证是否收到发送给 DMC 的元组列表的付款; (5) 无人机供应商付款: 从 DMC 收到付款并核实无人机供应商的发票后, 代理将继续向提供商付款. 无人机提供商: (1) 选择将请求服务的候选无人机; (2) 无人机路径规划: 它发出命令以调整无人机的飞行运动; (3) 数据传递: 它将无人机收集的数据 (相关的大坝监测服务) 传递给 DMC 和 BC; (4) 审计: 它验证是否从无人机代理那里收到了发

票中所包含的元组的付款; (5) 付款: 在收到代理的付款并核实从 CP 收到的发票后, 它开始向 CP 支付.

大坝监控中心 (DMC) 负责: (1) 请求发送和数据接收: 它将数据收集请求发送到 UAV 代理, 并从 UAV 提供商接收收集的感测数据; (2) 审计: 它验证是否收到了从无人机代理收到的发票中包含的所有元组; (3) 向无人机代理付款: 在验证收到的发票, 验证数据并执行审计功能之后, DMC 继续向无人机代理付款.

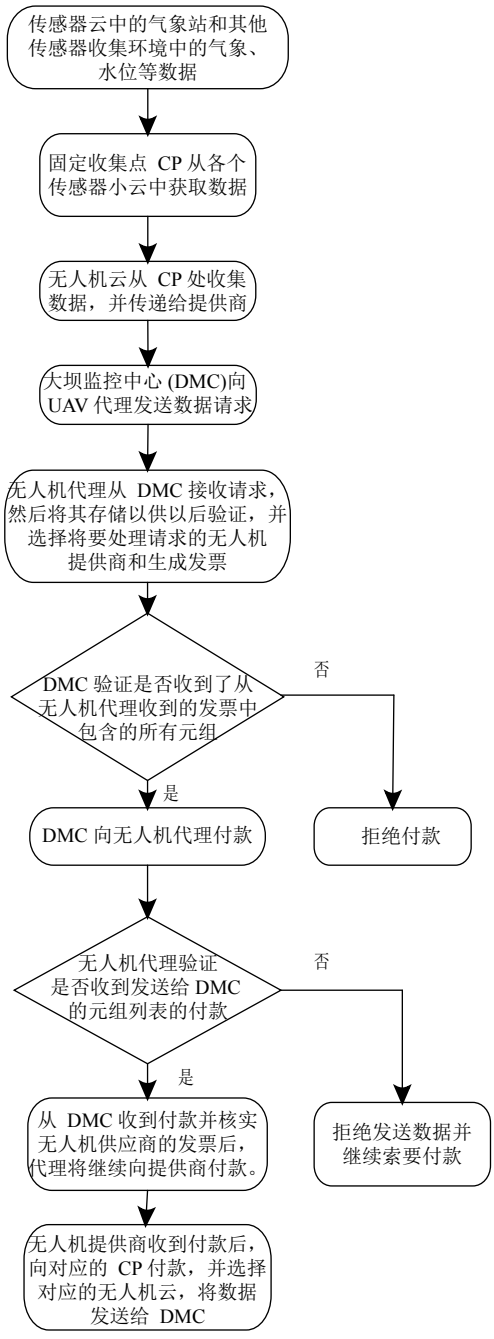

图 2 系统流程图

1.2 系统要求

为了有效地在地面传感器和 DMC 之间传输数据, 设计的方案必须得到数据保护并面向云, 并且必须确保参与者的支付, 具体需要满足以下要求:

可扩展性: 在大型且基础设施较差的区域 (例如水坝站点), 通过采用云概念, 可以通过增加设备数量或添加更多资源来确保扩展能力. 传感器云可以增加同一云中传感器的数量, 可以添加更多 CP 或更多资源. 此外, 通过增加更多的 UAV 提供商、UAV 和更多的资源也可提升扩展性, 且这种增加不会影响请求处理和数据传递.

身份验证: 为了确保数据真实可靠且防止数据被篡改, DMC 需要对数据来源进行身份验证, 这可以通过按原点对数据对象进行签名登记来完成. 此外, 为了确保请求来源是可信的, CP 需要验证请求来源, 这可以通过 DMC, UAV 代理和 UAV 提供商签署请求来完成.

完整性: 为了保护请求、数据和声音的完整性, 可以对数据进行签名、哈希处理, 然后将处理后的数据上传到 BC. 数据完整性由块挖掘过程中使用的共识机制 (即永久证明) 保证, 通过定期向 BC 网络请求 BC 收据, DMC 可以随时验证数据完整性. 请求的完整性和不可伪造性可以通过将数字附加到已签名的请求中来提供, 区块链网络区通过检查发票中是否包含请求编号, 验证元组列表以及验证是否已支付此请求来提供发票的完整性和不可伪造性.

跟踪数据支付: 本文所设计的系统中, 无人机代理负责从 DMC 接收请求, 而无人机提供商则负责从 CP 收集数据并将其传递到 DMC. 若要保证系统的有效性, 则要将无人机云完成的数据支付任务可靠地追溯到其来源, 并应该跟踪每个操作. UAV 代理应验证与给定请求相关的数据是否已正确发送到 DMC. UAV 提供商应跟踪 UAV 收集的数据是否来自真实的 CP. CP 应验证: (1) 收集的数据是否已支付给无人机提供商; (2) 这些数据是否已经很好地固定在了基站; (3) 这些数据是否被发送到 DMC.

付款: 为保证支付的可靠性, 付款仅在数据和发票验证之后执行. 例如, DMC 可以在验证真实性, 数据完整性, 总请求持续时间和发票付款后, 继续向 UAV 代理付款. 付款金额取决于元组中包含的度量数量. 为了支付这些实体, 应使用支付系统, 该系统应利用存储在 BC 中的数据. 因此, 支付系统应依赖于 BC 技术, 例如比特币网络.

2 区块链技术

2.1 使用区块链保护系统

本文将 BC 技术用作响应系统要求的潜在解决方案, BC 可被视为分布式和公共分类帐, 本文使用混合 BC 网络[14], 即使用公共比特币 BC 来支付操作, 使用私有 BC 来存储数据并确保其完整性和可追溯性[15].

大坝和无人机提供商的结合起到共识节点的作用, 要加入 BC 网络, 实体应具有从证书颁发机构获得的证书, 且实体之间的所有交互都存储在 BC 中. 对于数据事务, 将从 CP 收集的每个数据都视为一个对象, 并由 UAV 提供商将其散列和锚定到 BC 网络中. 数据锚定带来许多好处: (1) 通过哈希函数和共识机制提供了数据完整性和防篡改功能; (2) 数据以分布式方式永久存储, 以确保稳定性, 可用性和弹性. (3) BC 使生成任何上载数据的收据成为可能.

UAV 提供商执行以下操作: (1) 将散列数据发布到 BC 网络: 将接收到的元组进行哈希处理, 然后将处理后的数据发布到 BC. BC 将为每个哈希元组提供一个标识, 并将这些标识发送给 UAV 提供商. 上传每个数据元组将有助于以后验证数据完整性, 并提供使 UAV 提供商的任务可追溯的指纹. (2) 储存 BC 网络给定的元组身份: 从 BC 网络接收到元组的身份后, UAV 提供商会将其存储在 DMC、UAV 代理和 CP 可以访问的安全平台中. 平台为每个请求号存储元组的数量, 它们的相应 CP 以及从 BC 网络接收到的元组的标识.

CP 通过确保 UAV 收集的每个元组是否已支付给其提供商和 BC 来跟踪 UAV 提供商的支付任务. 每个 CP 将访问 UAV 提供商的平台, 以验证元组号是否已更改, 以及是否具有 BC 给出的身份.

UAV 代理通过访问由 UAV 提供商创建的平台来跟踪 UAV 提供商的支付任务, 以提取与给定请求相关的元组, 然后验证每个元组是否具有来自 BC 网络的相应标识.

为了提供数据完整性保护和验证, DMC 在从 UAV 提供商的平台接收到元组的身份后, 要求为每个元组提供 BC 收据. 通过将数据库中计算的哈希值与生成的 BC 收据中的目标哈希值进行比较, 可以验证每个元组.

2.2 区块链上的数据操作

为了体现应用区块链的大坝数据传输的安全性和可靠性, 下面将详细介绍数据如何在 BC 上生成、传输和验证.

(1) 请求生成和传递

DMC 请求可以定期生成, 也可以在事件发生时生成, 请求时间可以根据实际水质进行调整. DMC 向 UAV (无人机) 代理发送一个请求, 包括一个随机请求号、请求的最大持续时间、安全时间戳和请求位置:

$$Req_{\mathrm{DMC}} = (num_{req}, \max - duration_{req}, time_{\mathrm{DMC}}, location_{req}) \tag{1}$$

这个请求用 DMC 的私钥签名并发送给 UAV 代理:

$$Req_{\mathrm{DMC_{signed}}} = (Req_{\mathrm{DMC}}, sig_{req_{\mathrm{DMC}}}),$$

其中, $sig_{req_{\mathrm{DMC}}} = S_{SK_{\mathrm{DMC}}}(Req_{\mathrm{DMC}})$, S 是签名算法 (非对称加密), SK_{DMC} 是 DMC 的私钥. 无人机代理通过验证请求中包含的数字签名来验证 DMC 的真实性, 它验证$time_{\mathrm{DMC}}$是否包含在请求中, 并将其与其时钟时间进行比较. 然后, 无人机代理选择一个候选的 UAV 提供商并命令它处理这个请求:

$$Req_{\mathrm{Br}} = (Req_{\mathrm{DMC_{Signed}}}, Cert_{\mathrm{Br}}, Time_{\mathrm{Br}}) \tag{2}$$

其中, $Cert_{\mathrm{Br}}$是它的证书, $Time_{\mathrm{Br}}$是它的安全时间戳. 发送给 UAV 提供商的请求是:

$$Req_{\mathrm{Br_{Signed}}} = (Req_{\mathrm{Br}}, sig_{req_{\mathrm{Br}}}) \tag{3}$$

其中, $sig_{req_{\mathrm{Br}}} = S_{\mathrm{SK_{Br}}}(Req_{\mathrm{Br}})$, SK_{Br}是无人机代理的私钥. 提供商验证无人机代理的真实性, 它从网络中选择一架无人机, 命令它飞越请求的位置. 然后, 提供商验证$Time_{\mathrm{Br}}$并将其与其时钟时间进行比较, 并通过添加它的时钟时间和证书构建了下面的请求:

$$Req_{\mathrm{Pr}} = (Req_{\mathrm{Br_{Signed}}}, Cert_{\mathrm{Pr}}, Time_{\mathrm{Pr}}) \tag{4}$$

最后, 提供商将请求发送到无人机:

$$Req_{\mathrm{Pr_{Signed}}} = (Req_{\mathrm{Pr}}, sig_{req_{\mathrm{Pr}}}) \tag{5}$$

其中, $sig_{req_{\mathrm{Pr}}} = S_{\mathrm{SK_{Pr}}}(Req_{\mathrm{Pr}})$是提供商的私钥, UAV (无人机) 验证接收请求的真实性.

(2) 数据报告

收到请求后, 每个 CP 都会注册请求的最后时间戳, 在验证了 UAV 提供商的真实性之后, 它将汇总的数据发送到 UAV, 然后, UAV 使用 DMC 的公钥加密其数据. 事实上, UAV 是在登记阶段发送给 CPs 的, 这个数据条目可以构造为一个元组, 其中包含元组编号、加密数据 (使用公钥加密)、度量值的数目、请求编号、请求的最大持续时间、证书和安全时间戳:

$$Tuple_{\mathrm{CP}i}=(num_{\mathrm{tuple}},Data_{\mathrm{CP}i_{\mathrm{encrypted}}},num_{\mathrm{measures}},num_{\mathrm{req}},cert_{\mathrm{CP}i},cert_{\mathrm{Br}},cert_{\mathrm{Pr}},Time_{\mathrm{CP}i},Time_{\mathrm{DMC}},Time_{\mathrm{Br}},Time_{\mathrm{Pr}},Location_{\mathrm{CP}i},\max-Duration_{\mathrm{req}}) \quad (6)$$

然后用 CP 的私钥签署每个元组:

$$Tuple_{\mathrm{CP}i_{\mathrm{signed}}}=\{Tuple_{\mathrm{CP}i},sig_{\mathrm{TupleCP}i}\} \quad (7)$$

其中, $Tuple_{\mathrm{CP}i_{\mathrm{signed}}}=\{Tuple_{\mathrm{CP}i},sig_{\mathrm{TupleCP}i}\}$. UAV 从 CP 接收所有元组, 然后将它们转发给 UAV 提供商, UAV 提供商将构造一个连接元组块$Block=<Tuple_{\mathrm{CP1}_{\mathrm{signed}}},\cdots,Tuple_{\mathrm{CP}n_{\mathrm{signed}}},Tuple_{\mathrm{quad}_{\mathrm{signed}}}>$然后将其发送到 DMC, 其中$Tuple_{\mathrm{quad}_{\mathrm{signed}}}$与无人机收集的数据相关. 在每个接收到元组之后, DMC 向 UAV 提供商发送确认 (ACK).

(3) 将数据发布到 BC 网络

在向 DMC 发送数据之后, UAV 提供商散列元组, 构造一个由连接的散列元组组成的块

$$Block_{hash}=<hash(Tuple_{\mathrm{CP1}_{\mathrm{sig}}}),\cdots,hash(Tuple_{\mathrm{CP}n_{\mathrm{sig}}}),hash(Tuple_{\mathrm{quad}_{\mathrm{sig}}})> \quad (8)$$

ACK 也是散列的, 无人机提供商将元组和 ACK 都上传到 BC 中, 因此散列元组和 ACK 都将存储在数据存储中, 这可以通过层级来实现, 因为它提供了一个向 BC 上传和发布数据的平台. 执行中, 每个元组都将被散列, 然后与其他元组一起存储在 BC 网络中的一个事务中, 并最终转换为默克尔树节点, 根节点将锚定在遵循 Chainpoint 3.0 协议的 BC 事务中, 该协议为每个元组提供时间戳证明. 每个被散列化的元组都有一个标识, 用于检索 BC 收据 (即验证交易的证据), UAV 提供商检索哈希元组的身份, 然后, 提供商将哈希元组存储在一个可由 DMC 访问的安全平台上, 以便进行完整性验证, 平台为每个请求存储: 序列号、元组数、它们的 CP 以及散列元组的标识, 并由无人机代理和 CPs 对无人机供应商的支付任务进行验证.

(4) 由 DMC 进行数据验证

在每个接收到的元组块之后, DMC 验证安全时间戳, 它计算请求支付的持续时间和数据报告的持续时间, 然后计算总的请求持续时间, 即延迟时间之和, 并将其与最大持续时间进行比较. 如果总请求持续时间超过最大持续时间, 则 DMC 不验证接收到的数据, 反之, DMC 验证接收到的数据并访问无人机供应商的安全平台, 以提取元组的身份. 为了验证每个元组, DMC 向 BC 发送一个请求并等待 BC 收据, 每个元组将通过比较计算得到的散列和生成的 BC 收据中的目标哈希值来验证. 此外, DMC 必须验证 BC 收据的格式和内容, 并且必须确认一个元组的摩尔根存储在 BC 中.

(5) 发票的生成和验证

发票生成: 3 个参与者负责生成发票: ① 无人机代理: 对于每个请求, 它检索所有相应的元组, 生成发票, 并将其发送给 DMC, 以便日后支付; ② 无人机供应商: 它准备发票, 并将其发送给无人机代理, 以便日后支付; ③ CP: 每个 CP 生成发票, 并将其发送给无人机供应商, 以便日后支付. 每张发票包含号码、元组列表、寄件人的比特币地址以及准确的 BTC 值, 支付的数量取决于度量值的数量和一个块中包含的元组的数量, 因此, 可以将支付的数量计算为固定价格之和, 以及块中包含的所有元组的度量值数乘以每个单位数据的价格.

发票核对: 3 个行为体 (即 DMC、UAV 代理和 UAV 提供商) 负责发票核对. 在收到发票后, DMC 验证发票中的元组列表和数据库中为给定请求存储的元组列表, UAV 代理通过比较包含在发票中的元组和从 BC 检索到的元组来验证每个发票, 以及 UAV 提供商通过比较包含在发票中的元组和存储在其平台中的元组来验证每个发票.

(6) 付款

发票确认后, 付款人将开始付款. 比特币是一种加密货币系统, 吸引了大量感兴趣的用户, 为了在收款人和付款人之间进行比特币转账, 双方都必须有钱包. 本文使用 BIP3 支付协议, 它代表了商家和客户之间的通信协议.

在验证请求持续时间, 每个收到的元组和每个收到的 BC 收据确认之后, DMC 继续支付 UAV 代理的款项. UAV 代理在收到 DMC 的付款后就向无人机提供商支付任务的费用. 无人机供应商在收到无人机代理的付款后, 向 CPs 支付传感任务的费用. 支付是通过比特币交易实现的, 每个支付人在执行付款并从收款人收到应收款项后, 在 BC 网络中登记给定请求的最后一次付款时间, 以避免为同一请求号码支付两次付款.

(7) 攻击检测

本文设计的系统侦测到的可能攻击包括:

① 数据和请求伪造: 无人机供应商可能通过注入非法数据和准备未经授权的付款来伪造数据, 这可通过 BC 网络检测到. 执行中, UAV 提供商可以伪造数据, 而不是发送 UAV 收集的数据, 但由于本文设计通

过证书和数字签名的验证对数据进行了身份验证, 因此不会发生这种攻击. 此外, 由 UAV 代理实现的请求伪造可以被 CP 检测到, 因为每个请求必须包含 DMC 的请求号和安全时间戳, 因此数据的真实性可以得到很好的保证.

② 数据和请求回放: CP 可能会尝试向候选无人机发送旧数据. 本设计中, DMC 可以通过每个元组中包含的时间戳和请求号来验证数据, 同时由于元组存储在 BC 网络中, 因此, DMC 可以检测到这些旧数据已经存在于 BC 网络中. 此外, 由于 CP 注册了每个请求的最后时间戳, 因此可以检测到请求回放.

③ 伪造发票: 这种攻击可通过接收不是真实来源产生的发票来实现. 这可由发票接收者检测到, 3 个发票接收者 (DMC、UAV 代理和 UAV 提供商) 接受到发票信息后, 通过比较核对来排除伪造的发票. 此外, 发票和请求号码存储在接收方的数据库中, 以便于进行发票验证. 另外, 即使 DMC 没有接收数据, CPs 也可以生成发票, UAV 提供商在从 DMC 为每个接收到的元组接收 ACK 时检测到这种攻击, 因此, CP 只有在接收到 ACK 之后才支付.

④ 双重付款: 可以通过收到相同的发票, 从而为相同的请求号码支付两次. 这可由支付者检测到, 因为每个发票包含发票和请求号码. 此外, 对于每个请求, 付款人在 BC 网络中登记最后一次付款时间, 因此, 付款人可以随时核实发票上的要求编号是否已经付款.

⑤ 拒绝支付: 例如, 即使在收到发票后, DMC 也可以拒绝支付给无人机代理. 这可通过在接收到每个元组之后, DMC 向 UAV 提供商发送一个 ACK 检测到, 发送的 ACK 与元组一起上传到 BC 网络中, 因此, DMC 不能拒绝付款.

3 仿真结果与分析

3.1 系统工作性能分析

在这一部分, 本文旨在分析所提出的工作的性能. 本文考虑了边长长度为 L=1.5 km 的正方形监测区, 并将整个区域划分为边长长度为 l=0.5 km 的正方形分区网格, 在每个传感器采集数据的子区域中心都有一个 CP.

假设所有的无人机都遵循同样的轨迹. 在接收到无人机供应商的请求后, 候选无人机会检查一组 CP, 然后将收集到的数据转发给无人机供应商. 假定无人机对指挥中心的重访时间为常数, 模拟中使用的参数总结在表 1 中.

表 1 参数设置

参数	数值	参数	数值
事件发生的概率	0.5	L_{pay}	500 B
提醒的时间间隔	20 s	L_H	10 kB
回访时间	240 s	接收率	250 kb/s
T_{CCI}	5 s	传输率	250 kb/s
S_{Cr}	20 m/s	为DMC提供公关与信托	150 s

为了所提出的模型, 本文计算数据传递延迟比率, 并在对应于数据交互生成时间的每个时隙上, 利用均匀随机分布来设置事件发生概率 (警报生成), 警报的大小定义为:

$$Size_{\text{alerts}} = \sum_{i=1}^{(L/l)^2} L_H + Nb_{\text{alerts}}(i) \times L_{\text{pay}} \tag{9}$$

其中, L_{pay}是传感器数据包有效载荷的长度, L_H是 CP 的聚合包的头的长度; Nb_{alerts}是警报的数量.

支付延迟等于:

$$D_{\text{delivery}} = T_{\text{Cr}} + T_{\text{Cl\&Des}} + T_W + T_{\text{Pr\&trBS}\to\text{DMC}} + T_{\text{col}} + T_{\text{tr to BS}}, \tag{10}$$

其中, $T_{\text{Cr}} = (L^2 - l^2)/(l \times S_{\text{Cr}})$是行驶的总距离, 除以巡航速度 ($S_{\text{Cr}}$), $T_{\text{Cl\&Des}} = 2 \times \left(\frac{L}{l}\right)^2 \times T_{\text{CCI}}$是爬升和下降的总数乘以爬升和下降所花费的时间 ($T_{\text{CCI}}$), $T_{\text{Pr\&trBS}\to\text{DMC}}$是处理收集的数据所需的时间和从 BS 到 DMC 的传输时间的总和, 它等于 BC 网络的处理时间, 并假设为是常数, T_W是从传感器产生数据到无人机到达的等待时间, $T_{\text{Col}} = Size_{\text{alerts}}/Rate_{\text{reception}}$是 UAV 从所有 CP 收集聚合包所需的时间, $T_{\text{tr to BS}} = Size_{\text{alerts}}/Rate_{\text{transmisson}}$是 UAV 从 CP 向 BS 传输数据所需的时间.

支付延迟率定义为:

$$Ratio_{D_{\text{delivery}}} = D_{\text{delivery}}/T_{\text{flight}} \tag{11}$$

其中, $T_{\text{flight}} = T_{\text{Cr}} + T_{\text{Cl\&Des}}$为无人机巡航、爬升、下降所花费的时间.

本文所提出系统的工作性能仿真结果如图 3, 本文针对事件发生概率从 0.1 到 0.8 的变化模拟了支付延迟比率, 从图中可看出延迟比随着生成事件概率的增加而增加. 因为, 当增加事件概率时, 生成警报的机会就会增加, 因此数据大小也会增加. 因此, 收集时间和传输到 BS 的时间都增加了. 同时还可观察到, 由于警

报数量的大量增加, 延迟比首先迅速增加 (在概率值 0.1 和 0.2 之间), 然后由于警报数量的缓慢增加而缓慢增加.

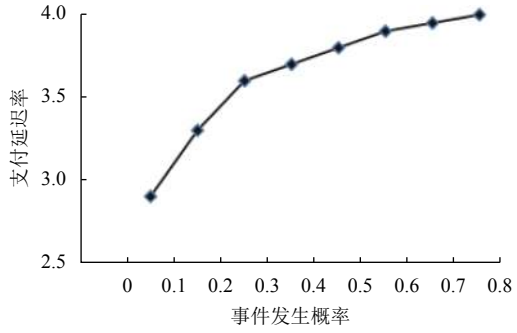

图 3 支付延迟率与事件发生的概率之比

图 4 针对从 120 s 到 360 s 的重新访问时间评估了数据传递延迟比. 从图中可以观察到, 随着重访时间的增加, 支付延迟率会随之增加. 因为增加的重访时间越多, 数据大小的增加就越大, 因此收集时间和到 BS 的传输时间都会增加. 而且, 传感器的等待时间也会随着重访时间的增加而增加.

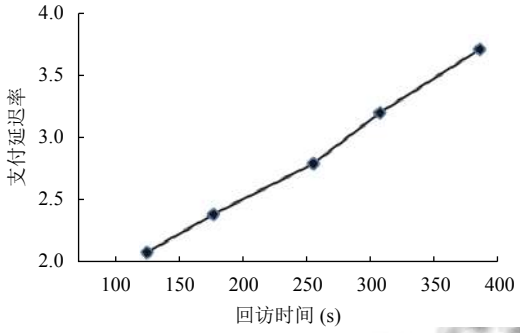

图 4 支付延迟率与回访时间之比

图 5 中模拟了警报生成的时间相对于支付延迟率的变化, 从 20 s 到 60 s 不等. 从图中可以观察到, 延迟比率随着警报间隔时间的增加而减小. 因为增加警报生成的时间越多, 生成的数据就越少, 传递延迟也就越少. 同时还可观察到, 由于警报数量的大量减少, 支付延迟比率首先迅速降低 (在 20 s 和 30 s 之间), 然后由于警报数量的缓慢减少而缓慢下降.

3.2 系统优势比较

下面为了体现本文设计系统的优势, 将本文中的基于区块链的物联网大坝监测系统与普通的未应用区块链的大坝监测系统进行比较.

为了体现系统的安全性和可靠性, 本文从支付成果率着手分析比较. 定义支付成功率为:

$$\text{支付成功率}=\frac{\text{CP收到的支付次数}}{\text{CP发出的数据次数}} \tag{12}$$

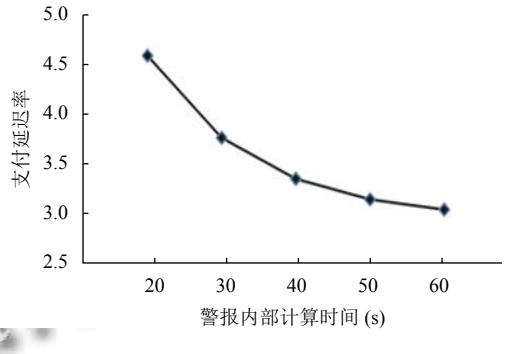

图 5 支付延迟率与警报内部计算时间之比

若 CP 收到的支付次数等于 CP 发出的支付次数, 则意味着 CP 每发出一次数据, 都得到了相应的付款, 数据在传递过程中处于安全状态. 若 CP 收到的支付次数大于 CP 发出的支付次数, 则意味着在数据传输过程中存在着虚假支付、数据被盗取的问题. 图 6 为支付次数为 1000 次 (包括虚假支付次数) 时的支付成功率比较图.

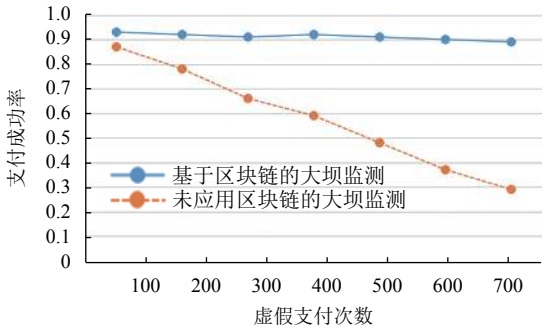

图 6 支付成功率图

从图 6 可以看出, 在支付次数为 1000 次时, 随着虚假支付次数的增多, 普通的未应用区块链的大坝监测系统的支付成功率不断降低, 因为其没有确保数据安全的审计与验证. 而本系统的支付成功率一直维持在 0.9 左右, 因为虽然虚假支付次数增加了, 但是因为经过多层的审计与验证, 可以排除虚假支付, 从而提高支付成功率.

4 结束语

本文提出了一种基于区块链的由传感器云和无人

机云组成的系统架构, 以用于监控大坝和确保数据的安全性与可靠性. 其中, 一组传感器小云可提供各种数据, 例如天气状况, 水质和水位以及大坝的结构状态, UAV 云可从传感器收集数据以及将数据传递到 DMC, 而 BC 技术确保了分布式的长期安全性, 该技术提供了身份验证, 数据存储和完整性以及 UAV 云数据支付的可追溯性, 有效的保证了大坝监测数据来源的可靠性, 数据传输的安全性以及预防潜在的数据攻击. 最后本文通过评估数据传递延迟率来评估工作绩效, 仿真结果表明, 所设计系统的延迟率所设计系统的延迟率与生成事件概率、重访时间成正相关, 与警报间隔时间成负相关, 且具有更高的支付成功率.

参考文献

1 周建平, 周兴波, 杜效鹄, 等. 梯级水库群大坝风险防控设计研究. 水力发电学报, 2018, 37(1): 1–10. [doi: 10.11660/slfdxb.20180101]

2 江科. 大坝安全监测数据分析方法研究. 科技资讯, 2012, (35): 53–54. [doi: 10.3969/j.issn.1672-3791.2012.35.044]

3 Narang S, Nalwa T, Choudhury T, *et al*. An efficient method for security measurement in internet of things. Proceedings of 2018 International Conference on Communication, Computing and Internet of Things. Chennai, India. 2018. 319–323.

4 Riahi A, Challal Y, Natalizio E, *et al*. A systemic approach for IoT security. Proceedings of 2013 IEEE International Conference on Distributed Computing in Sensor Systems. Cambridge, UK. 2013. 351–355.

5 Zhang JL, Wang YX. An intelligent college network design based on cloud IOT technology. Proceedings of 2016 International Conference on Intelligent Transportation, Big Data & Smart City. Changsha, China. 2016. 304–308.

6 Rastko M, Nikola M, Vladimir M, *et al*. Using Internet of Things in monitoring and management of dams in Serbia. Facta Universitatis-Series: Electronics and Energetics, 2016, 29(3): 419–435. [doi: 10.2298/FUEE1603419M]

7 Li QB, Lin P. Demonstration on intelligent dam. Journal of Hydroelectric Engineering, 2014, 33(1): 139–146.

8 Fang SF, Xu LD, Zhu YQ, *et al*. An Integrated system for regional environmental monitoring and management based on internet of things. IEEE Transactions on Industrial Informatics, 2014, 10(2): 1596–1605. [doi: 10.1109/TII.2014.2302638]

9 Sun EJ, Zhang XK, Li ZX. The Internet of Things (IOT) and Cloud Computing (CC) based tailings dam monitoring and pre-alarm system in mines. Safety Science, 2012, 50(4): 811–815. [doi: 10.1016/j.ssci.2011.08.028]

10 张小洋. 对基于物联网技术与云技术的大坝安全管理分析. 建材与装饰, 2018, (39): 295–296. [doi: 10.3969/j.issn.1673-0038.2018.39.210]

11 Iansiti M, Lakhani KR. The Truth about Blockchain. Harvard Business Review, 2017, 95(1): 118–127.

12 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494.

13 曾建电, 王田, 贾维嘉, 等. 传感云研究综述. 计算机研究与发展, 2017, 54(5): 925–939. [doi: 10.7544/issn1000-1239.2017.20160492]

14 海沫, 朱建明. 区块链网络最优传播路径和激励相结合的传播机制. 计算机研究与发展, 2019, 56(6): 1205–1218. [doi: 10.7544/issn1000-1239.2019.20180419]

15 巫岱玥, 余祥, 王超, 等. 基于区块链的信息系统数据保护技术研究. 指挥与控制学报, 2018, 4(3): 183–188. [doi: 10.3969/j.issn.2096-0204.2018.03.0183]