基于智能合约的无人机集群安全性研究

杨忠举,朱卫星,何红悦,王梅娟

(中国人民解放军陆军工程大学 指挥控制工程学院,江苏 南京 210007)

摘 要: 智能合约是区块链的重要组成部分,具有去中心化、可追溯、自动化执行以及不可篡改等特点,在理论和技术层面能够有效适应无人机集群安全性方面的需求。以智能合约在无人机集群中飞行数据管理、自主协同、安全维护以及安全认证4个方面的应用为例,重点分析智能合约在应用过程中潜在的整数溢出、时间戳、重入、交易顺序依赖及交易授权5种安全漏洞。在此研究基础上,针对潜在的智能合约安全漏洞提出一种基于注意力机制的混合神经网络漏洞检测模型。实验表明,与当前流行的智能合约漏洞检测技术相比,该漏洞检测模型检测效果更好,具有较高的准确率和精确率。该研究结果对于提高无人机集群建设安全系数具有一定的实际意义,也为无人化建设与发展提供了参考。

关键词: 智能合约;无人机集群;注意力机制;混合神经网络;漏洞检测

DOI: 10. 11907/rjdk. 222405 **开放科学(资源服务)标识码(OSID):**

中图分类号: TP183 **文献标识码:** A **文章编号:** 1672-7800(2023)008-0164-08

Research on the Security of Drone Swarms Based on Smart Contract

YANG Zhongju, ZHU Weixing, HE Hongyue, WANG Meijuan

(*School of Command and Control Engineering, PLA Army Engineering University, Nanjing* 210007, *China*)

Abstract: Smart contracts are an important component of blockchain, characterized by decentralization, traceability, automated execution, and non tampering. They can effectively meet the security requirements of drone clusters at both the theoretical and technical levels. Taking the application of smart contracts in flight data management, autonomous collaboration, security maintenance, and security authentication in unmanned aerial vehicle clusters as an example, this paper focuses on analyzing the potential security vulnerabilities of smart contracts in the application process, including integer overflow, timestamp, reentry, transaction sequence dependency, and transaction authorization. Based on this research, a hybrid neural network vulnerability detection model based on attention mechanism is proposed for potential security vulnerabilities in smart contracts. Experiments have shown that compared to the current popular smart contract vulnerability detection technology, the proposed vulnerability detection model ACBSC has better detection performance, and has better accuracy and precision in detecting vulnerabilities. The research results have certain practical significance for improving the safety factor of drone cluster construction, and also provide reference for unmanned construction and development.

Key Words: smart contract; drone swarm; attention mechanism; hybrid neural network; vulnerability detection

0 引言

无人机技术能有效代替人类进行重复低效、高成本低产出以及危险系数高的工作,受到学术界和工业界的高度关注。然而,在带来诸多便利和经济效益的同时,无人机技术也存在潜在安全问题。目前,无人机技术大多依靠互联网的接入和覆盖实现,若恶意攻击者利用系统漏洞对无人机设备进行远程操控,进而对其实施攻击,轻则将会破坏其原有的正常功能,重则会产生巨大经济损失甚至人员伤亡。此外,无人机技术多采用中心化控制的方式,无人机设备生产商或其他可以作为第三方的对象会面临信任

收稿日期: 2022-11-25

基金项目: 国家重点研发计划项目(2018YFB1403400);陆军工程大学基础前沿科技创新项目(KYZYJQZL2203)

作者简介: 杨忠举(1999-),男,中国人民解放军陆军工程大学指挥控制工程学院硕士研究生,研究方向为需求工程与智能软件测试;朱卫星(1978-),男,博士,陆军工程大学指挥控制工程学院副教授,研究方向为军事需求、软件工程、作战实验与大数据;何红悦(1985-),男,博士,陆军工程大学指挥控制工程学院副教授,研究方向为军事需求、软件工程;王梅娟(1984-),女,博士,陆军工程大学指挥控制工程学院副教授,研究方向为信息安全隐私保护。本文通讯作者:朱卫星、何红悦。

问题。因此，防止恶意攻击者入侵、保护数据安全是无人机研究领域亟待解决的问题。

结合智能合约的区块链技术使用椭圆曲线加密算法（Elliptic Curve Cryptography，ECC）等非对称加密技术保障数据在传输与存储过程中的安全性，使得区块链上所有无人机节点在平等和信息透明的基础上达成共识，能够解决信任问题。智能合约将预先设置的条件及条件满足时触发的事件以合约的形式部署到区块链，从而摆脱第三方的参与，起到无人信托的作用。可见，区块链与智能合约相结合可以为无人机的安全性提供保障。研究表明，无人机以集群方式完成任务的效能远高于单架无人机累计效能的总和[1]。基于以上分析，本文研究内容主要分为3个部分：第一部分从飞行数据管理、自主协同、安全维护和安全认证4个方面探讨智能合约在无人机集群中的应用。智能合约为无人机集群技术实现提供解决方案，但合约一旦部署到区块链上便不可修改，含有漏洞的合约影响集群原有功能的实现，甚至产生严重的安全威胁。因此，第二部分重点研究应用过程中潜在的整数溢出、时间戳依赖、重入、交易顺序依赖以及交易授权漏洞，分析其成因和危害。第三部分研究整数溢出、时间戳依赖、重入3种安全漏洞的检测方法，基于词嵌入技术生成神经网络的输入，利用引入注意力机制的双路混合神经网络进行特征提取，通过Softmax输出漏洞检测结果。

1　相关工作

目前关于智能合约应用于无人机的研究较少，但其他领域的相似研究可为智能合约在无人机领域的应用提供参考。例如，Liu等[2]提出一个将无人机系统（Unmanned Aircraft Systems，UAS）融入国家空域的安全框架，为空中和地面智能车辆网络防御提供了解决方案。该框架支持区块链，并基于智能合约实现了飞行计划的身份验证，以及在UAS与ATM基础设施之间的密钥交换；Al-madani等[3]基于智能合约设计去中心化电子投票系统，去中心化的特性保障了投票过程的高度公正性和可靠性，解决了投票过程的信任问题；Wang等[4]提出一种基于区块链和智能合约的工业互联网（Industrial Internet of Things，IIoT）架构，用于支持不可变和可验证服务，同时提出一种分层的区块链存储结构ChainSplitter用于解决存储空间受限问题；其还提出了一种基于区块链和智能合约的InterTrust架构，能够支持不同区块链系统之间的互操作性，其功能依靠阈值签名方案和可信性硬件两部分实现[5]；Wöhrer等[6]为不同去中心化应用程序提供了架构蓝图，描述了概念组件以及它们之间可能的关系。

目前，深度学习技术在智能合约漏洞检测领域受到广泛关注，并取得了一定成果。由于准确率是衡量深度学习中神经网络模型好坏以及漏洞检测模型是否有效的重要指标，目前许多学者专注于提高漏洞检测模型准确率的研究。例如，Hwang等[7]提出的CodeNet可在保证语义和上下文的同时检测智能合约是否存在漏洞，其将智能合约源代码经过预处理转化为图像作为检测模型输入，是否存在漏洞作为输出，该漏洞检测方法与现有漏洞检测工具相比有更好的检测性能；Wu等[8]提出基于关键数据流图和预训练技术的Peculiar模型，与现有方法中使用的传统数据流图相比，关键数据流图不那么复杂，也不会带来不必要的深层次结构，使得模型更容易关注关键特征，该模型在检测重入漏洞方面可以达到91.80%的准确率和92.40%的召回率；Ren等[9]创建了一个安全有效的智能合约开发环境SCStudio，主要包含代码推荐模块和代码验证模块，集成了Oyente v0.2.7、Mythril-classical v0.22.1、Securify v1.0.0、SmartCheck v2.0.0、Pied-Piper v1.0.0 5种检测工具。该开发环境被用作微众银行（WeBank）的官方开发工具以及FISCO-BCOS社区推荐的开发工具；Zhang等[10]提出一种基于集成学习的合约漏洞预测方法，该方法基于7种不同的神经网络，利用合约漏洞数据进行合约级别的漏洞检测。结果表明，集成学习不仅可以在模型误差相同的情况下减小训练数据集大小，而且可以有效提高漏洞预测的准确性和鲁棒性。

以上研究大多是其他领域基于智能合约的漏洞检测方法，未涉及智能合约在无人机集群中的应用。在参考以上研究的基础上，本文首先研究智能合约在无人机集群的应用；然后分析潜在的智能合约漏洞，并研究其检测方法。本文研究包含智能合约应用、漏洞分析以及漏洞检测工作，是一项系统性研究，弥补了基于智能合约的无人机集群安全性研究的空白，拓展了智能合约的应用领域。

2　智能合约在无人机集群中的典型应用

区块链与智能合约密切相关，区块链是智能合约的依托平台，智能合约拓展了区块链的应用场景。智能合约去中心化、不可篡改、可溯性等优势能有效适应无人机集群的安全性需求，以下从飞行数据管理、自主协同、安全维护以及安全认证4个方面展开讨论。

2.1　飞行数据管理

飞行数据的安全性管理对于无人机集群至关重要，关系到集群所需执行任务的成败[11]。若飞行数据无法被准确掌握，将会影响新任务发布。通过构建分布式区块链网络，每一架无人机都被视为网络中的一个节点，网络中任意节点的动态均可被监测。分布式网络中的节点互相联通，能够实现信息共享。飞行数据管理除需掌握数据信息外，还要保障飞行数据存储的安全性。智能合约能够连接星际文件系统（Inter Planetary File System，IPFS），做到数据存储的去中心化，保障了存储安全性。无人机节点在链上成功写入数据之前需要通过共识机制验证，共识通过，数

据可被成功写入链上;共识不通过,数据则写入失败。共识机制保障了无人机集群之间数据传输的安全性。同时,建立加密机制对数据信息进行非对称加密,可保障交易安全。

2.2 自主协同

无人机以集群形式执行任务的效能往往高于单架无人机执行任务效能的总和,而这种高效性离不开集群内部无人机节点的自主协同[12]。无人机节点共处于区块链网络中,各节点之间互联互通,集群内部信息能够实时共享。区块链的去中心化特性使得各节点相互协同,如果无人机集群内部有节点出现故障而失效,分布式网络便会自动重构,而其余节点继续执行原有任务。同样的,分布式网络加入节点后也能进行重构,继续执行原有任务。现实生活中的无人机出现故障或是由于自身存在缺陷,或是被恶意攻击者劫持利用。若为后者,无人机集群会存在一定的安全风险,因为被劫持利用的无人机会向其余正常无人机传播干扰信息,影响集群决策,无法做到“共识”。然而,智能合约的可追溯特性能保证出现故障的无人机节点及其动态能够被查询到,进而准确定位故障节点并进行相关处理,从而保障集群自主协同的安全性。

2.3 安全维护

安全维护主要是针对无人机集群硬件以及软件程序升级的维护,为无人机集群执行任务时的正常运转提供保障[13]。无人机集群的维护过程可以视作一条维护链的功能,主要包括维护申请、维护受理以及维护反馈。将维护过程以智能合约的形式写入维护链中,合约的触发条件为无人机集群的硬件损坏或软件版本级别过低,合约的响应即依次进行维护申请、维护受理以及维护反馈流程。自动化维护过程需要将规则以智能合约的形式写入维护链中,在此过程中可能会涉及信任问题,例如维护受理的信任问题,若有恶意攻击者操纵无人机节点提出维护申请,将会浪费人力和物力资源对其进行检修。为解决信任问题,可以结合区块链技术加入加密机制,利用非对称加密技术产生公钥和私钥,将维护申请视为公钥处理,技术人员使用相应私钥完成数字签名,可受理或驳回维护申请。有了智能合约的参与,无人机集群的整个安全维护过程对内部人员变得公开透明,能够实时查询安全维护状态,提升了安全维护的工作效率。

2.4 安全认证

向无人机集群内加入无人机节点之前需要进行身份认证,身份认证通过的节点才被允许加入到集群内部[14]。身份认证的目的是防止恶意攻击者使用已控制的节点破坏集群正在执行的任务。基于区块链的智能合约通过数字签名和加密机制为无人机集群内部的身份验证提供了解决方案。依据典型的访问控制模型开发智能合约,例如在基于角色的访问控制中,不同角色有不同的细粒度访问权限,能有效管理用户访问权限,提高了身份认证的安全系数。此外,基于区块链的智能合约能为指定用户节点提供公平、公正、公开且不易被干扰的决策环境。构建区块链网络,指定用户节点参与进来,将决策内容以及相关背景信息以智能合约的形式存储到区块链网络中并使用加密技术对其加密,此时恶意节点需要破坏区块链网络中超过51%的节点才可以阻碍决策过程。恶意节点对决策过程发动攻击的高成本是保障决策过程顺利进行的重要原因。

3 智能合约潜在漏洞分析

智能合约在无人机集群应用中会存在潜在漏洞,轻则导致无人机集群功能失灵,任务执行失败;重则危害人员财产和生命安全。下文重点分析整数溢出、时间戳依赖、重入、交易顺序依赖以及交易授权漏洞5种智能合约潜在安全漏洞,其中整数溢出漏洞包含整数上溢和整数下溢。

3.1 整数溢出漏洞

整数溢出漏洞对应智能合约漏洞库中的SWC-101以及表示“不正确的计算”的CWE-682,该漏洞包含整数上溢和整数下溢两种情况,整数上溢指存储大于最大支持值,整数下溢指存储小于最小支持值[15]。整数溢出漏洞产生的原因为智能合约开发前未提前对计算结果进行逻辑验证。该漏洞会产生极其严重的后果,如代币无限增发,指恶意攻击者能够利用整数溢出漏洞发起交易,通过少量代币向指定地址发送大量代币。代币在区块链中代表着数字资产,可作为奖励用于激励矿工对无人机集群任务链进行维护和升级。数字资产的损失势必影响矿工的执行效率,进而影响无人机集群各个任务链的安全运转。

3.2 时间戳依赖漏洞

时间戳依赖漏洞对应智能合约漏洞库中的SWC-116以及表示“包含来自不受信任的控制领域功能”的CWE-829,该漏洞通常发生在利用时间戳作为执行重大事件的一个关键要素的场景[16]。该漏洞产生的原因为在时间戳作为执行重大事件的一个关键要素时,矿工能在短时间内(小于900 s)操纵对自己有利的时间戳。无人机以集群方式执行任务时,若集群中存在某无人机节点因被恶意攻击者控制而失效,可以利用时间戳技术通过溯源方式定位到失效节点,避免其干扰其他节点而影响任务执行。若时间戳依赖漏洞被恶意攻击者利用,将会影响时间戳技术在无人机集群中溯源特性的有效应用,导致无法准确定位失效节点,甚至将正常节点误判为失效节点,最终影响集群任务的正常进行。

3.3 重入漏洞

重入漏洞对应智能合约漏洞库中的SWC-107以及表示“工作流程执行不当”的CWE-841,该漏洞的本质是循环调用代码缺陷,是智能合约漏洞类型中发生较为频繁以及威胁程度较高的一种[17]。智能合约在执行期间通过函

数调用或转移以太币实现对其他合约的调用。然而，这些外部调用存在被恶意攻击者利用的风险，导致合约被强制执行其余代码，这个过程可以被看作为重入。该漏洞通常发生在使用转账函数的情况下，会导致被攻击合约账户中的代币被窃取或拒绝服务。若重入漏洞被恶意攻击者利用，将导致无人机集群存在关键功能失灵以及代币损失的巨大风险。

3.4　交易顺序依赖漏洞

交易顺序依赖漏洞对应智能合约漏洞库中的SWC-114以及表示“并发执行中使用共享资源时未正确同步”的CWE-362。区块链网络以区块为单位处理交易，交易传播以及矿工对其认同需要一定时间。恶意攻击者利用这段时间监控被攻击合约的交易，以更高的gas发送自己的交易，使其与被攻击合约交易处于同一区块内[18]。矿工检查区块内的交易，优先处理gas较高的攻击者合约交易，导致恶意攻击者因窃取被攻击合约交易内容受益，被攻击合约受到损失。若有恶意攻击者利用交易顺序依赖漏洞，原有智能合约所实现的功能会因合约执行顺序异常而失灵，同时恶意攻击者发布的交易对无人机集群的应用也会存在安全威胁，如恶意攻击者在获得交易优先处理权限时会发布带有攻击性的合约。

3.5　交易授权漏洞

交易授权漏洞对应智能合约漏洞库中的SWC-115以及表示“包含过时功能的使用”的CWE-477，该漏洞指智能合约中使用tx.origin全局变量实现用户验证时容易遭受钓鱼攻击[19]。智能合约能够解决无人机集群中的身份验证问题，若使用tx.origin全局变量开发用于身份验证的合约，如使用tx.origin全局变量进行授权操作时，会导致合约被恶意攻击者发动钓鱼攻击，引诱用户在有漏洞的合约上执行一些需要授权的操作，若授权操作设计代币转移，则会存在代币损失风险，进而影响矿工对无人机集群任务链的维护和升级。

4　智能合约漏洞检测模型

设计合理且安全的智能合约能够实现无人机集群的关键功能，拓展其应用场景。由于智能合约被部署到区块链上后无法修改，其漏洞检测变得尤为重要。现有智能合约漏洞检测技术各有优劣，但检测精度均有待提高。本文主要针对整数溢出、时间戳依赖以及重入漏洞提出结合注意力机制的混合神经网络模型，用于智能合约漏洞检测。卷积神经网络（Convolutional Neural Network，CNN）拥有强大的特征提取能力，但容易忽视上下文信息从而导致一些特征信息丢失，使合约漏洞检测误报率升高。双向门控循环单元（Bi-Gated Recurrent Unit，BiGRU）是用于解决时序问题的神经网络模型，能够解决上下文信息学习丢失问题。BiGRU与CNN结合组成的混合神经网络应用于智能合约漏洞检测领域有较好效果[20]，但这两种模型存在一个共同问题，即忽视了词对句子语义的重要程度。因此，本文提出的智能合约漏洞检测模型除了使用CNN和BiGRU外，还结合注意力机制展开研究，从大量信息中获取对漏洞检测目标起到关键作用的少量信息，进而增强特征提取能力，提高漏洞检测准确率。

如图1所示，智能合约漏洞检测模型主要包含4个部分，分别为智能合约数据集、词嵌入层、特征提取层以及分类层，其中智能合约数据集由Zhang等[20]提出；词嵌入层包含Word2Vec模型和FastText模型；特征提取层包含CNN、BiGRU、注意力机制机制以及融合层；分类层利用Softmax输出漏洞检测结果。

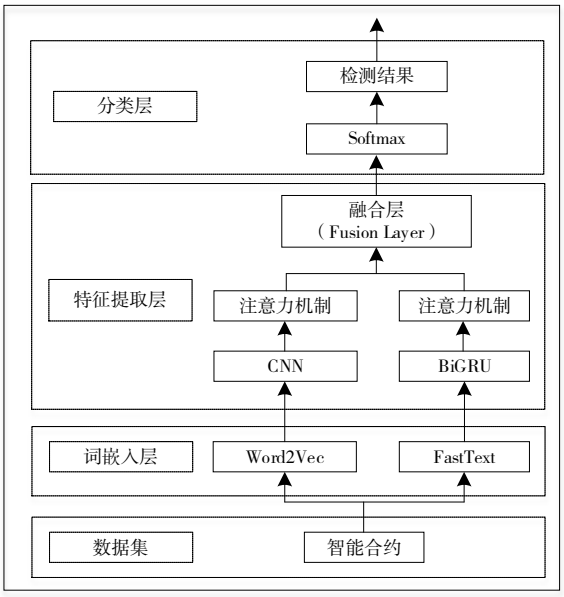


Fig. 1　Smart contract vulnerability detection model

图1　智能合约漏洞检测模型

智能合约漏洞检测模型的训练算法步骤为：

输入：#智能合约solidity源代码

1.#对智能合约solidity源代码进行CBOW预训练

2.#对智能合约solidity源代码进行FastText预训练

3.#对预训练好的词向量Word2Vec（ds）通过CNN进行特征提取

4.#对预训练好的词向量FastText（ds）通过BiGRU进行特征提取

5.#对通过注意力机制的特征FCNN和FBIGRU进行融合

6.#对融合后得到的特征Resultdetection进行Softmax处理

输出：#智能合约漏洞检测结果

以下重点介绍模型的两个关键层级，分别为词嵌入层以及特征提取层。

4.1　词嵌入层

词嵌入层利用Word2Vec模型和FastText模型将智能合约数据集转化为神经网络的输入形式，即词向量形式。

4.1.1　Word2Vec模型

本文模型采用Word2Vec模型中的连续词袋（Conti-

nous Bag of Words，CBOW）模型对词进行预训练。CBOW模型通过上下文信息预测当前值，其模型架构如图2所示，其中window=3，$w(t)$为输入层的中心词，$w(t-3)$、$w(t-2)$、$w(t-1)$、$w(t+1)$、$w(t+2)$、$w(t+3)$为$w(t)$的上下文。以下简述CBOW网络模型的各个层级：

（1）输入层。该层以上下文单词的one hot编码作为输入，假设单词向量空间的维度为V，上下文单词窗口的大小为C，输入大小为$C \times V$。

（2）隐藏层。假设隐藏层最终输出维度大小为N的词向量，输入层与隐藏层之间的权重矩阵为$W \in \mathbb{R}^{V \times N}$，$V \times N$表示$W$的大小。将向量组$\{W^{d1}, W^{s2}, \ldots, W^{sC}\} \in \mathbb{R}^{1 \times V}$中的每个向量分别同$W \in \mathbb{R}^{V \times N}$相乘，得到向量组$\{W^{d1}, W^{d2}, \ldots, W^{dC}\} \in \mathbb{R}^{1 \times N}$，再对向量组$\{W^{d1}, W^{d2}, \ldots, W^{dC}\} \in \mathbb{R}^{1 \times N}$取平均，得到向量$W^{d} \in \mathbb{R}^{1 \times N}$。

（3）输出层。初始化输出权重矩阵$W^{o} \in \mathbb{R}^{N \times V}$，将隐藏层的向量$W^{d} \in \mathbb{R}^{1 \times N}$与$W^{o} \in \mathbb{R}^{N \times V}$相乘，采用Softmax处理，输出向量$W^{r} \in \mathbb{R}^{1 \times V}$，该向量的每一维代表词库中的一个词，预测目标对应概率最大的index代表的单词。

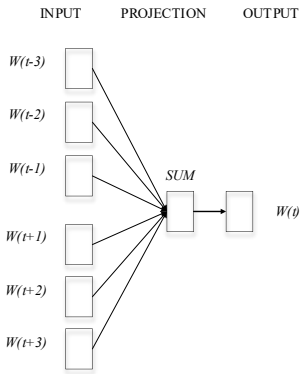


Fig. 2 CBOW model architecture

图2 CBOW模型架构

4.1.2 FastText模型

FastText模型训练速度较快，广泛用于构建并训练词向量以及文本分类。如图3所示，FastText模型架构较为简单，由输入层、隐藏层和输出层组成，其中$(x_1, x_2, \ldots, x_{N-1}, x_N)$表示智能合约文档嵌入的向量特征以及n-gram特征。FastText模型将智能合约文档的词与n-gram向量求和后平均处理得到智能合约文档向量，然后使用Softmax对其进行分类。

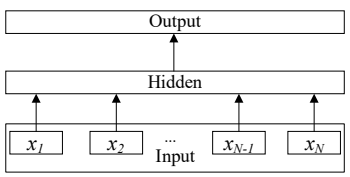


Fig. 3 FastText model architecture

图3 FastText模型架构

4.2 特征提取层

特征提取层由带有注意力机制的双路分支神经网络以及融合层组成，融合层将混合神经网络中两个分支网络的特征提取结果进行融合，进而通过Softmax输出漏洞检测结果。本文选用的分支神经网络为特征提取能力较强的CNN以及能够联系上下文信息进行特征学习的BiGRU。

4.2.1 CNN模型

CNN模型结构如图4所示，主要包括以下结构：

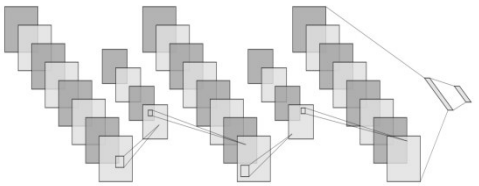


Fig. 4 CNN model structure

图4 CNN模型结构

（1）输入层。智能合约数据集中的每个词经过Word2Vec后被映射为相应的词向量x_i，词向量x_i组成矩阵$S = (x_1, x_2, \ldots x_i, \ldots, x_n)$，其中$x_i \in \mathbb{R}^k$，表示矩阵$S$中第$k$个词向量，$k$表示词向量的维度，$S \in \mathbb{R}^{n \times k}$，$n$表示矩阵$S$中词向量的个数，本实验中词向量的维度$k = 300$。

（2）卷积层。卷积核与矩阵S进行卷积操作实现矩阵S的特征提取，特征为c^f、c_i^f表示经过卷积操作后的特征。计算公式为：

$$c_i^f = f(w \cdot x_{i:i+r-1} + b) \tag{1}$$

式中：w表示卷积核，b表示偏置量，f表示$Relu$激活函数，$x_{i:i+r-1}$表示从i到$i+r-1$行的词向量。经过卷积操作的词向量集合C^f表示为：

$$C^f = \{c_1^f, c_2^f, \ldots, c_i^f, \ldots c_{n-r+1}^f\} \tag{2}$$

式中：n为卷积核个数。

（3）池化层。为获取最大特征M_{ti}，并对卷积层提取信息进一步降维，本实验选择最大池化方法。表示为：

$$M_{ti} = \max\{C^f\} \tag{3}$$

（4）输出层。该层的主要作用为连接池化层中所有的M_{ti}。

4.2.2 BiGRU

GRU由更新门和重置门组成，模型结构如图5所示。

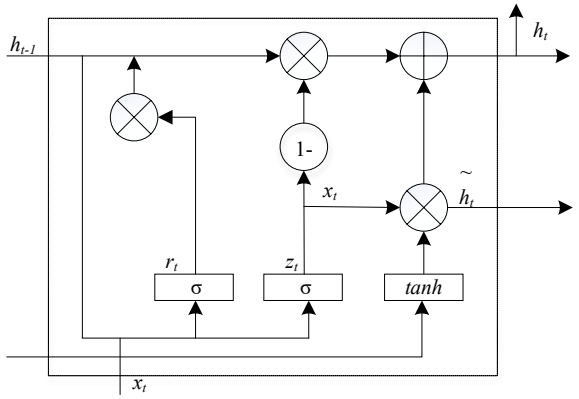


Fig. 5 GRU model structure

图5 GRU模型结构

更新门值的大小与前一时刻隐藏层输出状态h_{t-1}对当前时刻状态x_t的影响程度成正相关。重置门值的大小表示前一时刻隐藏层的输出状态h_{t-1}与当前时刻状态x_t的结合程度，其值越大，表示忽略的信息越少。σ表示*sigmoid*，与*tanh*均为激活函数，x_t表示当前时刻的输入。h_t表示当前时刻隐藏层的输出，h_{t-1}表示前一时刻隐藏层的输出，$\tilde{h}_t$表示候选隐藏层状态。计算公式为：

$$\tilde{h}_t = \tanh(W_h[r_t h_{t-1}, x_{t-1}]) \tag{4}$$

$$h_t = (1 - z_t)h_{t-1} + z_t\tilde{h}_t \tag{5}$$

式中：z_t表示更新门，r_t表示重置门。计算公式为：

$$z_t = \sigma(W_z[h_{t-1}, x_t]) \tag{6}$$

$$r_t = \sigma(W_r[h_{t-1}, x_t]) \tag{7}$$

GRU模型虽然充分考虑到当前状态与前一时刻状态的关联信息，却无法获取当前状态与下一时刻状态的关联信息，因此本文采用双向GRU模型BiGRU，包含两个单向且方向相反的GRU，其输出状态由两个GRU输出状态共同决定。BiGRU当前隐藏层状态h_t'由当前输入x_t、前向隐藏层状态的输出$\overrightarrow{h}_{t-1}$和反向隐藏层状态的输出$\overleftarrow{h}_{t-1}$3部分共同决定，w_t、v_t分别表示$\overrightarrow{h}_{t-1}$和$\overleftarrow{h}_{t-1}$的权重，b_t表示当前t时刻的偏置量。BiGRU的输出计算过程为：

$$\overrightarrow{h}_t = GRU(x_t, \overrightarrow{h}_{t-1}) \tag{8}$$

$$\overleftarrow{h}_t = GRU(x_t, \overleftarrow{h}_{t-1}) \tag{9}$$

$$h_t' = w_t\overrightarrow{h}_t + v_t\overleftarrow{h}_t + b_t \tag{10}$$

引入注意力机制能使神经网络模型在训练过程中关注对训练有用的关键信息，同时忽视不重要信息，可提高模型训练效率。图6为带有注意力机制Attention的BiGRU结构，混合神经网络的另一分支CNN+attention与此结构类似，其中$(x_1, x_2, x_3, x_4, \ldots, x_n)$为输入序列，$(h_1, h_2, h_3, h_4, \ldots, h_n)$为基于BiGRU隐藏层状态下的输出值，$(\overrightarrow{h}_1, \overrightarrow{h}_2, \overrightarrow{h}_3, \overrightarrow{h}_4, \ldots, \overrightarrow{h}_n)$为基于前向BiGRU提取得到的隐藏层输出值，$(\overleftarrow{h}_1, \overleftarrow{h}_2, \overleftarrow{h}_3, \overleftarrow{h}_4, \ldots, \overleftarrow{h}_n)$为基于反向BiGRU提取得到的隐藏层输出值。$(h_1, h_2, h_3, h_4, \ldots, h_n)$由$(\overrightarrow{h}_1, \overrightarrow{h}_2, \overrightarrow{h}_3, \overrightarrow{h}_4, \ldots, \overrightarrow{h}_n)$与$(\overleftarrow{h}_1, \overleftarrow{h}_2, \overleftarrow{h}_3, \overleftarrow{h}_4, \ldots, \overleftarrow{h}_n)$共同决定。

注意力机制相关参数计算过程为：

$$e_{ti} = a(s_{t-1}, h_i) \tag{11}$$

$$w_{ti} = \frac{\exp(e_{ti})}{\sum_{k=1}^{n}\exp(e_{tk})} \tag{12}$$

$$c_t = \sum_{i=1}^{n} w_{ti}h_i \tag{13}$$

$$p(y_t|y_1, y_2, ..., y_{t-1}, x) = BiGRU(c_t) \tag{14}$$

式中：a表示注释h_i根据状态s_{t-1}对下一个隐藏层状态s_t的重要性，w_{ti}表示h_i的注意力权重，e_{ti}表示求解w_{ti}过程中的中间变量，c_t表示步长为t的上下文向量，

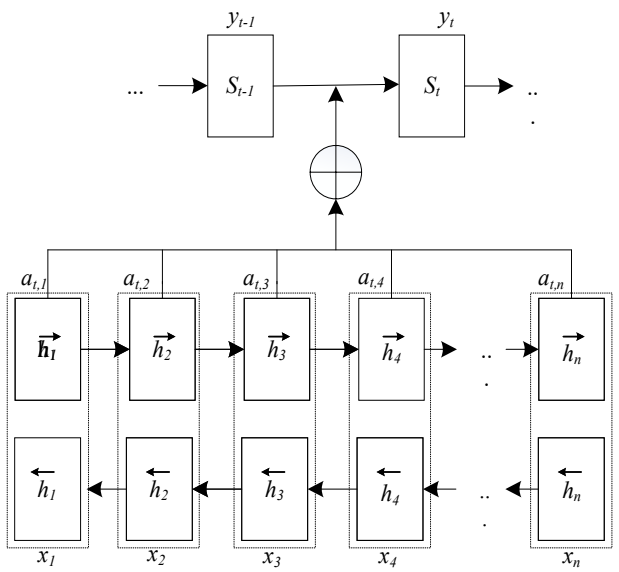


Fig. 6　BiGRU + attention structure

图6　BiGRU+attention结构

$p(y_t|y_1, y_2, ..., y_{t-1}, x)$表示BiGRU在当前步长$t$中输出最有可能的符号$y_t$。如此一来，源句信息能够分布在整个序列中，非编码器将信息编码成固定长度的向量，便于解码器在每个时间步长中有选择性地对其检索。因此，注意力机制能使神经网络专注于输入相关信息，而非无关部分。

5　实验方法与结果分析

5.1　实验数据

本文选取的智能合约数据集包含SmartBugs Dataset-Wild数据集[21]，Qian等[22]发布的智能合约数据集以及相同数量的不包含漏洞的智能合约数据集[20]。

5.2　实验环境

实验环境配置如表1所示。模型训练过程中使用的优化器为*Adam*，该优化器能够自适应参数学习率；使用*Dropout*函数用于防止过拟合现象以及提高模型泛化能力。

Table 1　Experimental environment configuration

表1　实验环境配置

软件名称	软件类型	软件版本
Windows11	操作系统	Windows11 Home
Tensorflow-gpu	Python 科学计算库	2.4.0
Keras	Python 科学计算库	2.3.1
Python	编程语言	3.8
CPU	处理器	-
GPU	处理器	-

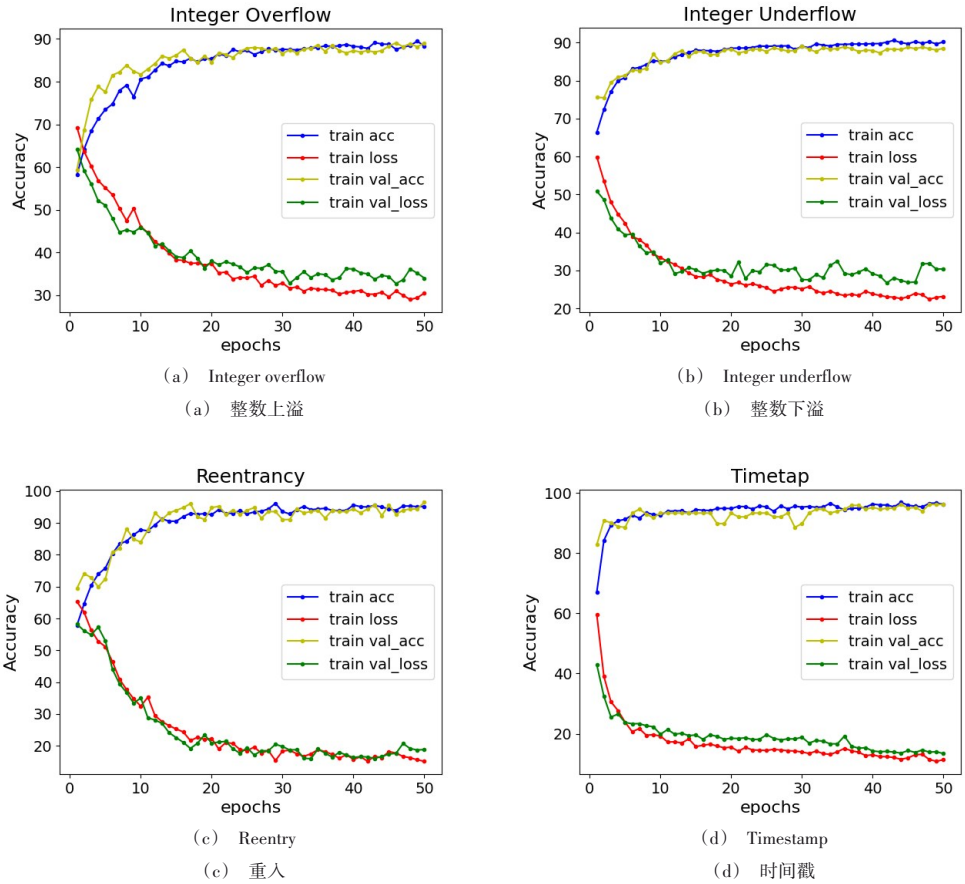
5.3　实验评估

选取准确率(Accuracy)、精确率(Precision)、召回率(Recall)作为智能合约漏洞检测效果的评估指标。为验证本文模型的有效性，选取CBGRU[20]、BLSTM-ATT[22]、DeeSCVHunter[23]、Peculiar[24]、DR-GCN[25]、DA-GCN[26]模型与本文模型进行比较。

5.4 实验结果分析

5.4.1 漏洞检测模型训练过程

图7(彩图扫OSID码可见)为本文模型针对整数上溢、整数下溢、重入以及时间戳依赖4种智能合约漏洞的检测结果,可以看出验证集和训练集中的曲线具有相同趋势且彼此接近,表明在训练过程中模型中不存在过拟合现象。本文模型对整数上溢、整数下溢、重入以及时间戳依赖漏洞的检测准确率分别为89.07%、88.55%、96.49%和96.18%,检测效果较好。



(a) Integer overflow
(a) 整数上溢
(b) Integer underflow
(b) 整数下溢
(c) Reentry
(c) 重入
(d) Timestamp
(d) 时间戳

Fig. 7 Detection results of the proposed model for four types of smart contract vulnerabilities

图7 本文模型对4种智能合约漏洞的检测结果

5.4.2 不同模型漏洞检测结果比较

针对智能合约中的重入漏洞,将本文模型分别与CBGRU[20]、BLSTM-ATT[22]、DeeSCVHunter[23]、Peculiar[24]、DR-GCN[25]模型进行比较,结果见表2。可以看出,本文模型准确率和精确率均为最高,召回率仅次于Peculiar模型。

针对时间戳依赖漏洞,将本文模型分别与CBGRU[20]、DeeSCVHunter[23]、DA-GCN[26]模型进行比较,结果见表3。

Table 2 Comparison of reentry vulnerability detection results of each model

表2 各模型重入漏洞检测结果比较 (%)

模型	准确率	精确率	召回率
本文模型	96.49	97.60	87.80
CBGRU	93.30	96.30	85.95
DeeSCVHunter	93.02	90.70	83.46
Peculiar	92.37	91.80	92.40
BLSTM-ATT	88.47	88.50	88.48
DR-GCN	81.47	72.36	80.89

Table 3 Comparison of timestamp dependent vulnerability detection results of each model

表3 各模型时间戳依赖漏洞检测结果比较 (%)

模型	准确率	精确率	召回率
本文模型	96.18	90.20	97.90
CBGRU	93.02	89.47	97.45
DeeSCVHunter	80.50	85.53	74.86
DA-GCN	87.54	87.15	82.25

可以看出,本文模型的准确率、精确率和召回率均优于其他检测模型。这是由于本文模型具有注意力机制,能够访问整个输入序列,利用更多上下文信息,并关注特定相关位置。其还可通过提取智能合约关键字,关注触发智能合约漏洞的关键信息,如容易触发重入漏洞的关键字payable、transfer、call.value等,减少无效信息关注,因此提高了智能合约漏洞检测效果。

6 结语

本文基于智能合约去中心化、可追溯、自动化执行以及不可篡改的特性探讨了其在无人机集群飞行数据管理、自主协同、安全维护以及安全认证4个方面的应用，并针对整数溢出、时间戳依赖、重入漏洞提出一种结合混合神经网络、词嵌入以及注意力机制的智能合约漏洞检测方法，是智能合约在无人机集群安全性领域应用的一次探索，为无人化建设与发展提供了一定参考。在今后的研究中，一方面将基于智能合约重点研究无人机集群内部访问控制实现技术，从而解决数据管理和存储的安全性问题；另一方面将继续关注智能合约在无人机集群应用中的潜在漏洞，并研究相关防范方法保障智能合约安全性。

参考文献：

[1] FAN B，LI Y，ZHANG R，et al. Review on the technological development and application of UAV systems[J]. Chinese Journal of Electronics，2020，29(2)：199-207.

[2] LIU Y，WANG J，CHEN Y，et al. Blockchain enabled secure authentication for unmanned aircraft systems[C]//2021 IEEE Globecom Workshops，2021：1-6.

[3] AL-MADANI A M，GAIKWAD A T，MAHALE V，et al. Decentralized e-voting system based on smart contract by using blockchain technology[C]//2020 International Conference on Smart Innovations in Design，Environment，Management，Planning and Computing，2020：176-180.

[4] WANG G，SHI Z，NIXON M，et al. Chainsplitter：towards blockchain-based industrial iot architecture for supporting hierarchical storage[C]//2019 IEEE International Conference on Blockchain，2019：166-175.

[5] WANG G，NIXON M. Intertrust：towards an efficient blockchain interoperability architecture with trusted services[C]//2021 IEEE International Conference on Blockchain，2021：150-159.

[6] WÖHRER M，ZDUN U，RINDERLE-MA S. Architecture design of blockchain-based applications[C]//2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services，2021：173-180.

[7] HWANG S J，CHOI S H，SHIN J，et al. CodeNet：code-targeted convolutional neural network architecture for smart contract vulnerability detection[J]. IEEE Access，2022，10：32595-32607.

[8] WU H，ZHANG Z，WANG S，et al. Peculiar：smart contract vulnerability detection based on crucial data flow graph and pre-training techniques[C]//2021 IEEE 32nd International Symposium on Software Reliability Engineering，2021：378-389.

[9] REN M，MA F，YIN Z，et al. SCStudio：a secure and efficient integrated development environment for smart contracts[C]//Proceedings of the 30th ACM SIGSOFT International Symposium on Software Testing and Analysis，2021：666-669.

[10] ZHANG L，WANG J，WANG W，et al. A novel smart contract vulnerability detection method based on information graph and ensemble learning[J]. Sensors，2022，22(9)：3581.

[11] CHEN W W，CHI K. UAV cluster data chain technology research[J]. Journal of Command and Control，2020，6(1)：43-49.
陈卫卫，迟凯. 无人机集群数据链技术研究[J]. 指挥与控制学报，2020，6(1)：43-49.

[12] NIU Y F，XIAO X J，KE G Y. Analysis of UAV swarm combat concept and key technologies[J]. Defense Science and Technology，2013，34(5)：37-43.
牛轶峰，肖湘江，柯冠岩. 无人机集群作战概念及关键技术分析[J]. 国防科技，2013，34(5)：37-43.

[13] QIN W L，QIAN H L，LIU G B. Research on the application of UAV swarm control of blockchain[J]. Scientific and Technological Innovation and Application，2020(21)：181-182.
秦望龙，钱海力，刘冠邦. 区块链的无人机集群控制应用研究[J]. 科技创新与应用，2020(21)：181-182.

[14] WANG Y，YANG J，SI S J. Research on UAV cluster networking certification technology[J]. Communication，2020(5)：10-14.
王云，杨娟，司书剑. 无人机集群组网认证技术研究[J]. 数据通信，2020(5)：10-14.

[15] QIU X X，MA Z F，XU M K. Analysis and countermeasures of Ethereum smart contract security vulnerabilities[J]. Information Security and Confidentiality of Communications，2019(2)：44-53.
邱欣欣，马兆丰，徐明昆. 以太坊智能合约安全漏洞分析及对策[J]. 信息安全与通信保密，2019(2)：44-53.

[16] WANG R L，WU H G，HE Y Q. A review of formal verification methods for smart contracts[J]. Cyberspace Security，2021，12(Z2)：73-79.
王润六，吴怀广，何亚琼. 智能合约的形式化验证方法综述[J]. 网络空间安全，2021，12(Z2)：73-79.

[17] NI Y D，ZHANG C，YIN T T. A review of research on smart contract security vulnerabilities[J]. Journal of Information Security，2020，5(3)：78-99.
倪远东，张超，殷婷婷. 智能合约安全漏洞研究综述[J]. 信息安全学报，2020，5(3)：78-99.

[18] YANG Z J，ZHU W X，SHI Y Q，et al. A review of smart contract vulnerabilities and detection technologies[J]. Network Security Technology and Application，2022(11)：6-9.
杨忠举，朱卫星，史涯晴，等. 智能合约漏洞及检测技术研究综述[J]. 网络安全技术与应用，2022(11)：6-9.

[19] HUANG K F，ZHANG S L，JIN S. Blockchain smart contract security research[J]. Information Security Research，2019，5(3)：192-206.
黄凯峰，张胜利，金石. 区块链智能合约安全研究[J]. 信息安全研究，2019，5(3)：192-206.

[20] ZHANG L，CHEN W，WANG W，et al. CBGRU：a detection method of smart contract vulnerability based on a hybrid model[J]. Sensors，2022，22(9)：3577.

[21] DURIEUX T，FERREIRA J F，ABREU R，et al. Empirical review of automated analysis tools on 47，587 Ethereum smart contracts[C]//Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering，2020：530-541.

[22] QIAN P，LIU Z，HE Q，et al. Towards automated reentrancy detection for smart contracts based on sequential models[J]. IEEE Access，2020，8：19685-19695.

[23] YU X，ZHAO H，HOU B，et al. DeeSCVHunter：a deep learning-based framework for smart contract vulnerability detection[C]//2021 International Joint Conference on Neural Networks，2021：1-8.

[24] WU H，ZHANG Z，WANG S，et al. Peculiar：smart contract vulnerability detection based on crucial data flow graph and pre-training techniques[C]//2021 IEEE 32nd International Symposium on Software Reliability Engineering，2021：378-389.

[25] ZHUANG Y，LIU Z，QIAN P，et al. Smart contract vulnerability detection using graph neural network[C]//Twenty-Ninth International Joint Conference on Artificial Intelligence and Seventeenth Pacific Rim International Conference on Artificial Intelligence，2020：3283-3290.

[26] FAN Y，SHANG S，DING X. Smart contract vulnerability detection based on dual attention graph convolutional network[C]//International Conference on Collaborative Computing：Networking，Applications and Worksharing，2021：335-351.

（责任编辑：尹晨茹）