航空科学技术
Aeronautical Science & Technology
Apr. 25 2022 Vol. 33 No.04 28-38

面向无人机自组网的路由消息完整性保护方法

郭晶晶[1]，高华敏[1]，刘志全[2]，王立波[2]，张兴隆[3]
1.西安电子科技大学，陕西 西安 710071
2.暨南大学，广东 广州 510632
3.航空工业自控所 飞行器控制一体化技术国防科技重点实验室，陕西 西安 710065

摘 要：安全性是无人机自组网路由协议面临的重要挑战之一。针对现有工作对分级路由协议中拓扑构建消息安全性防护的不足，本文针对分级无人机自组网的路由协议提出了一种拓扑构建消息的安全保护方案，该方案可以保证分级无人机自组网在拓扑建立过程中节点间交互消息的完整性，从而避免完整性遭到破坏的信息被用于网络拓扑构建以及创建路由的过程中，提高路由协议的健壮性与可靠性。针对拓扑消息中的静态信息提出了基于联盟区块链的完整性验证方法，减少了整个方案的计算与传输开销。通过对所提方案进行安全性分析，证明了该方案能够有效抵御拓扑消息传输过程中的假冒攻击和消息篡改攻击。最后，通过仿真试验分析了该方案在不同无人机自组网路由协议中的性能。试验结果表明，该方案的时间开销小于100ms，内存开销小于路由总开销的35%。

关键词：无人机自组网；分级路由协议；完整性保护；网络安全

中图分类号：TP393 **文献标识码：**A DOI：10.19452/j.issn1007-5453.2022.04.005

无人机自组织网络（UAV Ad-hoc Networks, UANETs）是移动自组织网络（Mobile Ad-hoc Network, MANET）在无人机领域的典型应用之一。因具有自组织、移动性、拓扑动态性和抗毁性强等特点，无人机自组织网络目前在军用和民用领域都具有广泛的应用[1]，如地质勘测、抢险救灾、区域侦察[2]和无人集群协同作战[3]等。无人机自组织网络的拓扑结构主要分为平面网络结构与分级网络结构，分级网络结构更适合于规模中等及以上的无人机自组织网络。在分级网络结构中，网络节点被分为若干个簇，每个簇拥有一个簇头节点和若干个簇成员节点，其中簇头节点负责管理簇内的其他节点并与其他簇的簇头节点通信，簇成员节点需要与其他节点通信时，首先将消息发送给其簇头，再由簇头将消息转发至目的节点。

因为开放的无线通信环境，灵活多变的协作模式，无人机自组网在构建拓扑与建立路由过程中容易遭受内、外部攻击。在网络拓扑构建过程中，无人机自组网主要面临的安全威胁包括篡改攻击、假冒攻击等，若拓扑构建消息的完整性遭到破坏，将导致错误的数据被用于网络拓扑构建，形成无效或低效拓扑结构。现有的无人机自组网安全性保护的相关工作主要集中于网络拓扑建立后节点间传输消息时的身份合法性验证、消息机密性保护、消息完整性保护、恶意节点检测[4]等领域，缺乏针对网络拓扑建立过程中的消息安全性保护机制，现有少量针对拓扑消息的安全防护方案均适用于平面网络结构的无人机自组网[5-9]，无法直接应用于分级网络结构。

针对这一问题，本文提出了一种无人机自组织网络分级路由协议中的路由消息安全性保护方案。在该方案可以保证分级网络结构的无人机自组网在拓扑建立过程中节点间交互消息的完整性，从而避免完整性遭到破坏的信息被用于网络拓扑构建以及创建路由的过程中，提高路由协议的健壮性与可靠性。

本文工作的创新之处主要包括以下三点：（1）针对无人

收稿日期：2021-12-16；退修日期：2022-01-14；录用日期：2022-02-08
基金项目：国家自然科学基金（62032025，62102167）；航空科学基金（20185881015）
引用格式：Guo Jingjing, Gao Huamin, Liu Zhiquan, et al. Integrity protection method of routing message for UAV ad-hoc networks[J]. Aeronautical Science & Technology, 2022, 33(04): 28-38. 郭晶晶，高华敏，刘志全，等. 面向无人机自组网的路由消息完整性保护方法[J]. 航空科学技术，2022，33(04)：28-38.

机自组织网络分级路由协议提出了拓扑构建消息的完整性保护方案，该方案可以避免完整性遭到破坏的信息被用于网络拓扑构建以及创建路由的过程中，提高路由协议的健壮性与可靠性。(2)为了减少所提方案对整个网络性能的影响，针对拓扑消息中的静态信息提出了基于联盟区块链的完整性保护方案，减少了整个方案的计算与传输开销。(3)针对所提方案进行了安全性分析，结果表明所提方案可以有效抵御完整性破坏攻击(假冒攻击和消息篡改攻击)，通过仿真试验验证了所提方案不会对原有路由协议造成严重的额外资源开销。

1 研究现状

随着无人机自组网的应用越来越广泛，国内外学者已经提出了大量的无人机自组网路由协议，然而目前针对路由协议的安全保护机制的研究较少，若无法保证路由建立过程中信息的完整性，恶意信息有可能被用于建立网络拓扑以及路由路径过程中，从而导致网络拓扑不稳定、路由效率低下等问题，为网络性能带来极大的负面影响。

1.1 无人机自组网路由协议

从网络拓扑结构角度出发，无人机自组网的路由协议主要可以分为不分级路由协议和分级路由协议。其中，不分级的路由协议适用于平面网络结构，在网络中所有节点地位平等，都具有转发与路由的功能，现有的经典协议包括按需距离矢量路由(ad-hoc on-demand distance vector, AODV)[10]、最优链路状态路由协议(optimized link state routing protocol, OLSR)[11]、动态源路由协议(dynamic state routing, DSR)[12]、地理位置路由协议GPSR、基于地理位置综合选择下一跳的航空自组网安全路由算法(secure geographic information routing protocol, SGRP)[13]等。然而在复杂任务情境下，随着无人机自组网中无人机节点数量的增加，为了均衡无人机节点负载、提高网络的稳定性，分级路由协议成为了研究的热点。现有的经典分级路由协议主要包括：以网络节点唯一标识符ID号为因子的Lowest-ID分簇算法[14]；考虑节点移动因素的基于移动性预测的分簇算法(mobility based metric for clustering, MOBICI)[15]；旨在优化能源消耗的分簇算法(imperialist competitive algorithm, ICA)[16]；基于权重的分簇算法(weighted clustering algorithm,WCA)[17]以节点的能量、节点度、节点间的距离和节点的移动速度作为节点竞选簇头的衡量标准，对网络进行分簇，实现网络的分级管理；基于可靠性的分簇算法(dependability-based clustering algorithm,DCA)[18]以节点能量、链路保持率、节点度和通信量为因子划分簇网络，分别以增强拓扑稳定性、节约能量、提高服务质量为目标调整分簇过程中各因子的比重，最大程度实现网络拓扑稳定、减少能量消耗或提高网络服务质量。上述分级路由协议中，路由的形成均建立在构建网络分级拓扑结构的基础上，即完成网络节点的分簇。

1.2 无人机自组网路由安全保护机制

与有线网络相比，通过无线介质通信的无人机网络更容易受到攻击，攻击者可能通过窃听网络层的控制信息发起一系列恶意行为扰乱路由机制[5]。暴露在易受攻击的无线环境下，无线自组网的网络信息安全传输必须满足数据通信的安全和路由协议的安全两个方面[6]。当前，有学者提出了一些保护无人机自组网路由协议的方案。Manel针对AODV协议提出了安全增强方法(secure ad hoc on-demand distance vector, SAODV)[6]，用来保护路由发现阶段信息与路由错误信息的安全性。Jean-Aimé等提出了SUAP[7-9,19]安全协议，该方案结合哈希链与公钥密码机制抵御数据通信过程中的虫洞攻击，从而实现对AODV协议的安全性保护。这些方案均针对非分级路由协议提出，无法直接应用于分级路由协议中。通过调研，我们发现目前针对分级路由协议的安全保护机制的研究较少，亟须设计一种高效、轻量级的分层路由协议安全保护机制，保证在构建网络拓扑结构过程中节点间传输的拓扑构建信息的完整性，避免因恶意攻击或故障导致错误信息被用于拓扑构建过程，形成低效或无效拓扑，对上层服务产生负面影响。

在数据完整性保护方面，除了利用哈希函数与数字签名技术，区块链因其可追溯、不可篡改的特点也越来越多地被用于保护信息的完整性。参考文献[20]提出了一种基于区块链的无线传感器感知数据记录系统，保护敏感数据不被篡改，提高无线传感器网络的可靠性。参考文献[21]提出了一种基于区块链的云存储数据完整性服务框架，为数据所有者和使用者提供可靠的动态数据完整性验证。

针对当前分级无人机自组网路由协议安全保护机制缺失的问题，本文提出一种无人机自组织网络分级路由协议中的路由消息安全性保护方案。该方案可以保证分级网络结构的无人机自组网在拓扑建立过程中节点间交互消息的完整性。在该方案中，利用区块链技术存储静态拓扑消息并验证和确保其完整性，同时减少所提方案的资源开销。

2 基本理论

在本文所提方案中，用到了基于椭圆曲线加密算法的

数字签名以及区块链技术来实现分级路由协议中拓扑信息的完整性保护。

2.1 椭圆曲线数字签名算法

椭圆曲线数字签名算法(elliptic curve digital signature algorithm, ECDSA)是使用椭圆曲线密码(elliptic curve cryptography,ECC)对数字签名算法DSA的模拟[22]。该算法主要包括密钥生成、签名、验证签名三个部分,细节如下所示。

(1) 密钥生成

首先,选择椭圆曲线$E(y^2 = x^3 + ax + b(\mathrm{mob}\,p))$与基点$G$,然后随机选取SK($1 \leqslant \mathrm{SK} \leqslant n-1$,$n$是基点$G$的阶)作为Alice的私钥,并利用基点$G$计算Alice的公钥PK:$(x,y) = \mathrm{SK} \times G$,其中PK、$G$为椭圆曲线$E$上的点。Alice的密钥对记为(SK,PK)。

(2) 签名

假设Alice需要发送消息M给Bob,利用函数$D = \mathrm{Sign}(\mathrm{SK}, M)$对$M$进行签名,签名的计算过程见式(1)~式(4)。

$$z = H(M) \tag{1}$$

$$(x_1, y_1) = kG \tag{2}$$

$$r = x_1 (\mathrm{mod}\, n) \tag{3}$$

$$s = k^{-1}(z + r \times \mathrm{SK})(\mathrm{mod}\, n) \tag{4}$$

式中:$H(M)$为计算得到的消息M的摘要,结果记为z;选取随机数$k \in [1, n-1]$与基点G的倍积运算得到椭圆曲线上的一个点(x_1,y_1);k^{-1}是随机数k的模的乘法逆元;式(3)和式(4)分别计算r与s值并满足条件$r, s \neq 0$,若不满足,返回式(2)选取随机数$k' \in [1, n-1]$,$k' \neq k$重新计算椭圆曲线上的点作为参数;最后生成的(r, s)作为数字签名从函数返回,结果记作$D = (r, s)$。

(3) 验证签名

Bob可以利用函数Verify(PK, D)验证Alice对消息M的签名(r, s)。验证过程见式(5)~式(7)。

$$z' = H(M) \tag{5}$$

$$(x_1,y_1) = z's^{-1} \times G + rs^{-1} \times \mathrm{PK} \tag{6}$$

$$x_1 (\mathrm{mod}\, n) == r \tag{7}$$

如果等式(7)成立,则签名验证通过,说明消息M的完整性未受到破坏。否则,验证不通过,说明消息M的完整性遭受破坏。

2.2 区块链技术

区块链概念起源于2008年发布的比特币白皮书[23],其本质上是一种由多方参与的去中心化数据库,也就是由存储各参与方交易信息的区块结合哈希链算法构成的共享账本[24-25]。从计算机技术角度看,它融合了分布式存储、对等网络、密码学原理、智能合约和共识机制等技术[26]。区块链可分为非许可链(permissionless blockchain)和许可链(permissioned blockchain)两类。任何参与方都可以随时加入非许可链网络并参与计算;在许可链网络中,每个参与方加入网络前都需要经过认证授权,许可链进一步可分为私有链(fully private blockchain)和联盟链(consortium block chain)[27],如hyperledger fabric就是联盟链的典型实现。

本文将利用联盟链的特性,设计路由过程中的静态拓扑消息的完整性验证方案,将各节点用于拓扑消息中的静态数据(如节点身份标识等)及其签名数据存储于区块链中,在完整性验证期间,通过访问存储于链上的对应信息来验证拓扑消息中的静态信息是否遭到完整性破坏,避免多次传输与计算这些信息及其签名数据,降低所提方案的计算与通信开销。

3 系统结构与安全目标

本节我们首先给出所提方案考虑的无人机网络架构,并对现有无人机自组网分层路由协议中网络拓扑构建过程中节点间的交互消息进行了分析,然后给出了无人机自组网拓扑消息的敌手模型,最后提出了本文的设计目标。

3.1 无人机网络架构

本文所考虑的无人机自组织网络由一个地面站以及若干个无人机节点组成,所有无人机节点被划分为若干个簇,每个簇由一个簇头及若干个簇内节点组成,簇头负责管理簇内节点完成簇内通信,所有的簇头与地面站构成无人机自组织网络的骨干通信网,负责完成簇间通信任务。在以上所述网络架构上提出的拓扑消息完整性保护框架如图1所示。

地面站作为可信第三方部署了密钥管理中心负责为网络中各节点生成公私钥对,认证中心(CA)采用PKI(public key infrastructure)架构负责在节点加入网络时为其签发证书并对所有证书进行管理。各无人机节点与地面站共同建立联盟区块链网络,与拓扑消息中的静态数据完整性保护相关的数据将存放在该区块链中,并可以在静态消息完整性验证时被节点或地面站访问。

在现有的无人机自组网分层路由协议中,拓扑构建(簇结构形成)过程中节点间进行交互的消息可以分为广播消息与单播消息两类。

广播消息主要包括无人机节点向外发送的用于邻居发现、效用公布、簇头声明的消息以及地面控制站向无人机节点发送的指令消息。无人机节点发送的广播消息只发送给

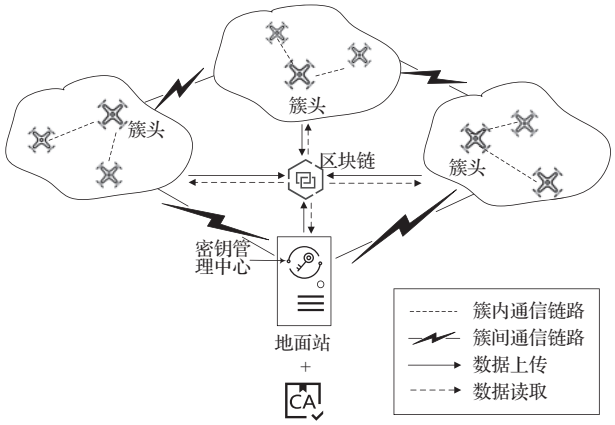

图1 无人机自组网拓扑消息安全性保护方案框架

Fig.1 Framework of topology message security protection scheme for UANET

其一跳邻居节点(单跳),而地面控制消息可能需要无人机节点的转发(多跳)从而将指令消息发送给所有节点。4种广播消息的具体介绍如下。

(1)邻居发现消息:消息内容主要包含消息类型、发送者身份、发送者基本信息(位置、速度等)、时间戳和随机数等。

(2)效用公布消息:消息内容主要包含消息类型、发送者身份及发送者的效用值(在特定范围内效用值最大的节点将被选举为簇头)、时间戳和随机数等。

(3)簇头声明消息:消息内容主要包含消息类型、发送者身份、簇头声明标识、时间戳、随机数等。

(4)地面控制消息:消息内容主要包含消息类型、发送者身份、指令、指令参数、时间戳、随机数等。

单播消息主要包含簇加入请求消息(节点请求加入某个簇),簇头节点对簇加入请求消息的响应,以及节点向地面控制站发送指令确认消息。其中,前两种消息不会被转发(单跳),而指令确认消息可能需要其他节点的转发(多跳),从而将消息从发送者送达地面控制站。下面对这三种单播消息进行具体介绍:(1)簇加入请求消息:消息内容主要包含消息类型、发送者身份、簇头节点身份、时间戳、随机数等。(2)簇加入请求响应消息:消息内容主要包含消息类型、发送者身份(簇头)、响应对象身份(发起簇加入请求的节点)、时间戳、随机数等。(3)指令确认消息:消息内容主要包含消息类型、发送者身份、指令序列号、时间戳、随机数等。

综上所述,分层次的拓扑消息中所包含的数据可以分为静态消息与动态消息,静态消息表示其内容在某节点发送的不同拓扑消息中保持不变,如发送者身份;动态消息表示其内容在同一节点发送的不同消息中可能会发生改变,如邻居发现消息中的位置、速度信息,效用公布消息中的效用值,簇加入请求消息中的簇头节点身份,以及各个消息中包含的时间戳与随机数。

我们可以将单跳消息与多跳消息形式化地表示为以下模式:

单跳消息:$m_{\mathrm{s,T}}\|m_{\mathrm{d,T}}$

多跳消息:$m_{\mathrm{s,T}}^{f0}\|m_{\mathrm{d,T}}^{f0}\|m_{\mathrm{s,T}}^{f1}\|m_{\mathrm{d,T}}^{f1}\|\cdots$

式中:$m_{\mathrm{s,T}}$与$m_{\mathrm{d,T}}$分别表示节点发送的TYPE类型的消息中的静态信息与动态信息;$m_{\mathrm{s,T}}^{f0}$与$m_{\mathrm{d,T}}^{f0}$分别表示多跳消息的发送者发出的原始消息中的静态信息与动态信息;$m_{\mathrm{s,T}}^{f1}$与$m_{\mathrm{d,T}}^{f1}$分别表示多跳消息中第一个转发者在所接收消息的基础上所增加的静态信息与动态信息。本文用到的主要记号和含义说明见表1。

表1 符号说明

Table 1 Symbol description

符号	含义
$\mathcal{U}$	无人机网络中所有节点的集合
ID_i, ID_j	任意节点$i,j\in\mathcal{U}$对应的身份标识
S	网络中的攻击者
C	拓扑消息包中的明文信息
$m_{\mathrm{s,T}}$	TYPE类型的拓扑消息中的静态字段
$m_{\mathrm{d,T}}$	TYPE类型的拓扑消息中的动态字段
PK_i	节点ID_i的公钥
SK_i	节点ID_i的私钥
Cert_i	CA为节点ID_i颁发的证书
block_i	节点ID_i的静态哈希信息在联盟区块链中的索引
$D_M=\mathrm{Sign}(\mathrm{SK}_i,M)$	签名函数。节点ID_i利用该函数及其私钥SK_i对消息M进行签名后得到D_M
$\mathrm{Verify}(\mathrm{PK}_i,D)$	签名验证函数,节点利用该函数及签名者的公钥对签名D进行验证,验证结果为通过或不通过
$H(M)$	哈希函数

3.2 敌手模型

我们假设攻击者S可以是未加入网络的陌生节点,或是网络内部的任意无人机,在网络拓扑构建过程中地面站是可信的,攻击者S无法对地面站进行攻击,但是能够进行拓扑消息的拦截、窃听、篡改及重放。

本文中,我们将网络拓扑建立过程中地面站、网络节点间发送的这些消息统称为拓扑消息。上文所述敌手行为可能会造成拓扑消息在传输中受到敌手的篡改、重放等攻击,导致错误的数据被用于网络拓扑构建,形成无效或低效拓扑结构。

3.3 安全目标

针对无人机网络面临的以上安全威胁，本文拟设计一种针对无人机自组网分层路由协议中拓扑构建过程中的拓扑消息完整性保护方案，使得拓扑消息中的信息无法在被篡改或重放后通过消息接收方的验证，确保消息接收者可以通过所提方案来确认消息是否被篡改或重放；同时，确保所提方案不给原有路由协议带来过大资源开销。

4 拓扑消息完整性保护方案

基于上一节对分层次拓扑消息的分析，我们从不同消息类型的角度出发分别为静态消息与动态消息设计完整性保护方案。针对静态消息，我们拟利用区块链的不可篡改性实现完整性保护。此外，我们拟基于公钥加密体制实现动态消息的完整性保护。

4.1 方案框架

拓扑消息完整性保护流程图如图2所示。假设在无人机自组网建立路由的过程中（包括分簇阶段与通信链路寻找阶段），无人机节点A向节点B发送消息M。为了保护消息M的完整性，节点A将根据消息M的具体特点进行不同操作。首先节点A根据消息M的类型将消息M所包含的字段划分为动、静态消息两类，根据消息M中各字段所属的类别分别计算每个字段的摘要，其中动态消息的摘要通过哈希函数计算得到，静态消息摘要可以通过访问本地存储表或读取区块链数据获得，区块链的不可篡改特性既保证了静态消息的完整性，又避免了重复计算静态消息的摘要，减少了计算与时间开销；最后，节点A对消息M及其摘要进行签名，当节点B收到消息M后，对M进行完整性验证，在验证通过后，将基于该消息中的信息进行拓扑构建。

4.2 完整性保护方案

下文将给出本文所提方案的详细内容。

4.2.1 系统初始化

当节点加入无人机自组网时，在CA处完成注册，KMC为节点生成密钥对后，CA为其颁发证书。所有网络节点构建静态信息联盟区块链网络用于存储各节点的拓扑消息中的静态信息哈希值（摘要）。节点上链信息的计算方法如算法1所示。当节点静态信息摘要记录于区块链后，区块链网络中所有客户端均可以通过将节点身份标识作为关键字对节点信息进行检索与访问。

4.2.2 消息完整性保护

单跳消息的完整性保护方法如算法2所示。消息发送节点ID_i在发送消息m前，首先利用哈希函数$H()$计算动态信息的哈希值，然后利用其私钥对静态消息哈希值与动态消息哈希值进行签名（静态消息哈希值在初始化阶段已计算得到），最后将消息及签名一同发送至消息接收方。

算法3给出了多跳消息的完整性保护方法。首先，消

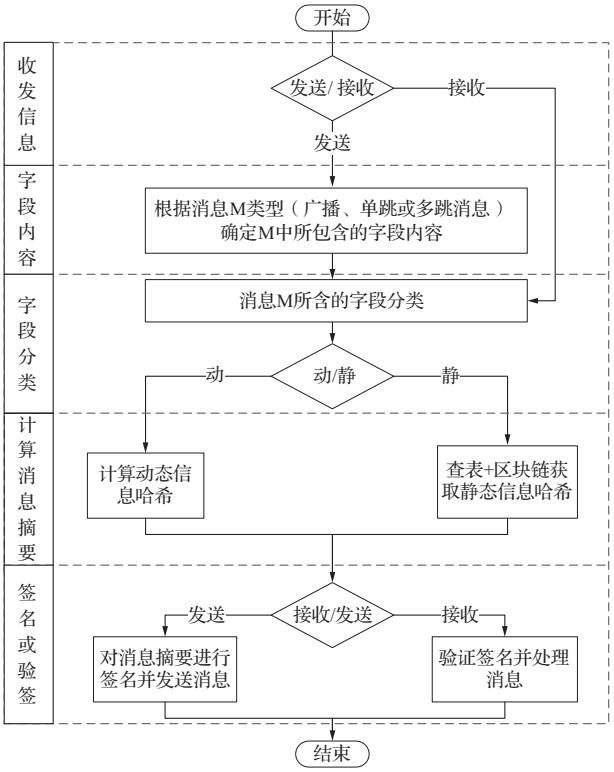

图2 拓扑消息完整性保护流程图

Fig.2 Workflow of topology message integrity protection

算法1 节点ID_i的上链信息计算方法

输入：节点ID_i发送拓扑信息类型数量n，每一类型消息中包含的静态信息$m_{\mathrm{s,T}}$

1. for i=1 to n
2. 计算$H_{\mathrm{s,T}_i}=H(m_{\mathrm{s,T}_i})$
3. //T_i代表第i种拓扑消息的类型
4. end for
5. $\mathrm{SI}_i=\mathrm{ID}_i\|\mathrm{Cert}_i\|H_{\mathrm{s,T}_1}\|\cdots\|H_{\mathrm{s,T}_i}\|\cdots\|H_{\mathrm{s,T}_n}$
6. 请求将SI_i存储于区块链；
7. return；

算法2 单跳消息完整性保护方法

输入：节点ID_i拟发送给节点ID_j的单跳消息$m=m_{\mathrm{s,T}}\|m_{\mathrm{d,T}}$

1. $H_{\mathrm{d,T}}=H(m_{\mathrm{d,T}})$；
2. $D=\mathrm{Sign}(\mathrm{SK}_i,H_{\mathrm{s,T}}\|H_{\mathrm{d,T}})$
3. $m_f=m\|D$；
4. 发送m_f
5. return；

息的发送者 ID_i 根据算法 2 中的方案发送消息，当该消息被转发节点收到后，转发节点首先检查该消息的完整性，如果该消息通过完整性验证，那么转发节点可以确认该消息的内容与发送者发送的内容一致，未遭受篡改、重放等攻击；接着转发节点将对其增加的静态信息与动态信息分别执行哈希运算，最后对静态信息与动态信息的哈希值进行签名，并按照算法 3 中第 10 行的规则更新消息并转发消息至下一跳节点。当消息的目的节点接收到该消息后，将对所收到的消息的完整性进行验证。若验证通过，则利用消息中的信息进行拓扑构建。消息的完整性验证方法将在下文详细介绍。

算法 3　多跳消息完整性保护方法

输入：节点 ID_i 拟发送给节点 ID_j 的多跳消息 $m = m_{s,T}||m_{d,T}$，消息 m 的转发节点集合 $ID_f = \{ID_{f1}, ID_{f2}, \cdots\}$.

1. $H_{d,T} = H(m_{d,T})$;
2. $D = \mathrm{Sign}(SK_i, H_{s,T}||H_{d,T})$;
3. $m_f = m||D$
4. 节点 ID_i 发送 m_f;
5. while $ID_{fx} \in ID_f$ 收到 m_f && $ID_{fx} \neq ID_j$
6. 验证接收到消息的完整性;
7. if 消息完整
8. $H^{fx}_{d,T} = H(m^{fx}_{d,T})$;
9. $H^{fx}_{s,T} = H(m^{fx}_{s,T})$;
10. $D^{fx} = \mathrm{Sign}(SK_{fx}, H^{fx}_{s,T}||H^{fx}_{d,T})$;
11. $m_f = m_f||m^{fx}_{s,T}||m^{fx}_{d,T}||D^{fx}$;
12. 节点 ID_{fx} 发送 m_f;
13. else
14. 丢弃接收到的消息;
15. end while
16. if 节点 ID_j 接收到消息
17. return;

4.2.3 消息完整性验证

如上文所述，当某节点接收到其他节点发来的消息后，首先需要验证该消息的完整性。算法 4 详细给出了消息接收节点（包括消息目的节点与转发节点）验证消息完整性的方法。

算法 4　消息完整性验证方法

输入：节点 ID_j 接收到节点 ID_i 发送的 TYPE 类型的消息 $m_f = m||D$

//m 为消息内容，D 为发送者签名

1. 节点 ID_j 访问联盟区块链获取发送者 ID_i 的静态消息哈希值 $H_{s,T}$ 及证书信息；
2. if ID_i 的证书有效
3. 从 m 中提取动态消息 $m_{d,T}$;
4. $H'_{d,T} = H(m_{d,T})$;
5. if (Verify(PK_i, D, $H_{s,T}||H'_{d,T}$)&& $H(m_{s,T}) == H_{s,T}$)
6. return 验证通过;
7. else
8. return 消息完整性被破坏;
9. end if
10. end if

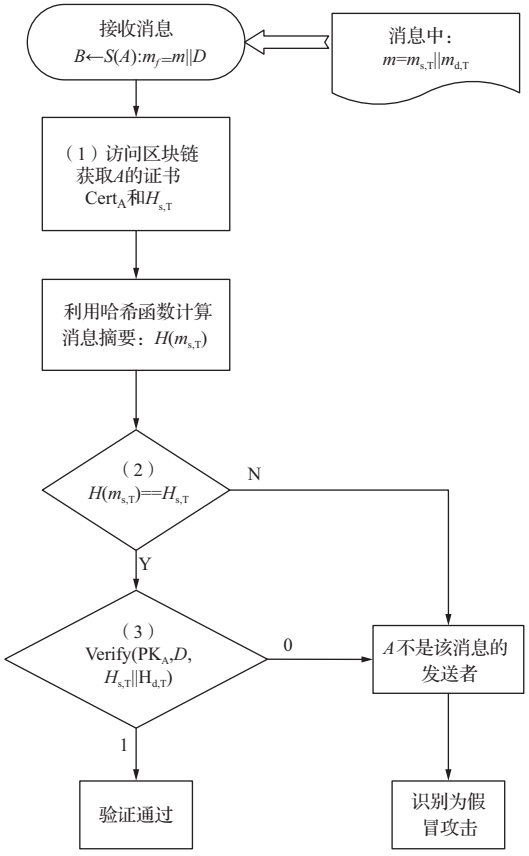

图 3　所提方案抵御假冒攻击的手动分析

Fig.3　Manual analysis results of the proposed scheme against impersonation attacks

5 安全性分析

5.1 手动分析结果

本节将分析所提方案针对常见的完整性破坏攻击的安全性。

5.1.1 假冒攻击

攻击方式：攻击者 S 假冒合法节点 A 伪造新消息发送给节点 B。

分析：假冒攻击的防御过程如图 3 所示。假设攻击者 S 向 B 发送消息 $m_f = m||D$，并声称其身份为 A，其中 $m = m_{s,T}||m_{d,T}$。消息接收者 B 将进行以下验证步骤：(1) B 从区块链中访问 A 的证书及 TYPE 类型消息的哈希值 $H_{s,T}$；(2) 计

算$H(m_{s,T})$并比较$H(m_{s,T})$是否等于$H_{s,T}$，若是相等，则进行下一步，若不相等，则可以推出A一定不是该消息的发送者；(3)利用A的公钥通过函数Verify(·)对D进行验证(验证通过返回值为1，否则返回0)，基于公钥密码学理论可以知道当且仅当签名D通过式(8)得到

$$D = \mathrm{Sign}(\mathrm{SK}_A, H_{s,T}\|H_{d,T}) \tag{8}$$

才有$\mathrm{Verify}(\mathrm{PK}_A, D, H_{s,T}\|H_{d,T}) = 1$成立，然而攻击者$S$无法获得$\mathrm{SK}_A$，因此有$\mathrm{Verify}(\mathrm{PK}_A, D, H_{s,T}\|H_{d,T}) = 0$。$B$可以确认该消息不是由$A$生成并发送的。因此，所提方案可以抵御假冒攻击。

5.1.2 消息篡改攻击

攻击方式：攻击者S截取源节点A发送的消息，增加、删除或篡改任意部分内容后发送给节点B。

分析：消息篡改攻击的防御过程如图4所示。假设节点A发送的消息$m_f = m\|D$，其中$m = m_{s,T}\|m_{d,T}$，被攻击者S截获。S对m_f进行篡改后发送给节点B。下面我们分三种情况来讨论所提方案对该攻击的防御。

(1) S将消息m_f修改为$m'_f = m'\|D, m' \neq m$

由于$m' \neq m$，因此有$H(m) \neq H(m')$，由于$\mathrm{Verify}(\mathrm{PK}_A, D, H, (\mathrm{m}))=1$因此必然存在：$\mathrm{Verify}(\mathrm{PK}_A, D, H(m'))=0$。节点$B$计算$H_{s,T}\|H_{d,T} = H(m')$，若$\mathrm{Verify}(PK_A, D, H(m'))$结果为真，则消息未被篡改，否则消息被篡改。

(2) S将消息m_f修改为$m'_f = m\|D', D' \neq D$

由于$D' \neq D$且$\mathrm{Verify}(\mathrm{PK}_A, D, H(m)) = 1$成立，因此必然有$\mathrm{Verify}(\mathrm{PK}_A, D, H, (\mathrm{m}))=0$。基于此，节点$B$计算$\mathrm{Verify}(\mathrm{PK}_A, D, H, (\mathrm{m}))$，其中$H_{s,T}\|H_{d,T} = H(m)$，若返回结果为真，则消息未被篡改，否则消息被篡改。

(3) S将消息m_f修改为$m'_f = m'\|D', m' = m'_{s,T}\|m'_{d,T}$，且$m' \neq m, D' \neq D$

节点B从区块链中获取A的证书Cert_i及静态哈希值$H_{s,T}$，计算$H(m'_{s,T})$，若m中的静态消息$m_{s,T}$被修改，令$H'_{s,T} = H(m'_{s,T})$，则必然有$H(m'_{s,T}) \neq H_{s,T}$。若m中的静态消息与动态消息均被修改，由于节点B无法获得SK_A，因此$\mathrm{Sign}(\mathrm{SK}_A, H'_{s,T}\|H'_{d,T}) \neq D'$成立，基于此，节点$B$计算$H'_{d,T} = H(m'_{d,T})$，判断$\mathrm{Verify}(\mathrm{PK}_A, D', H'_{s,T}\|H'_{d,T})$是否为真，若结果为真则消息未被篡改，若结果为假，那么消息一定被篡改。因此，所提方案可以验证所接收的消息是否被篡改，从而可以抵御消息篡改攻击。

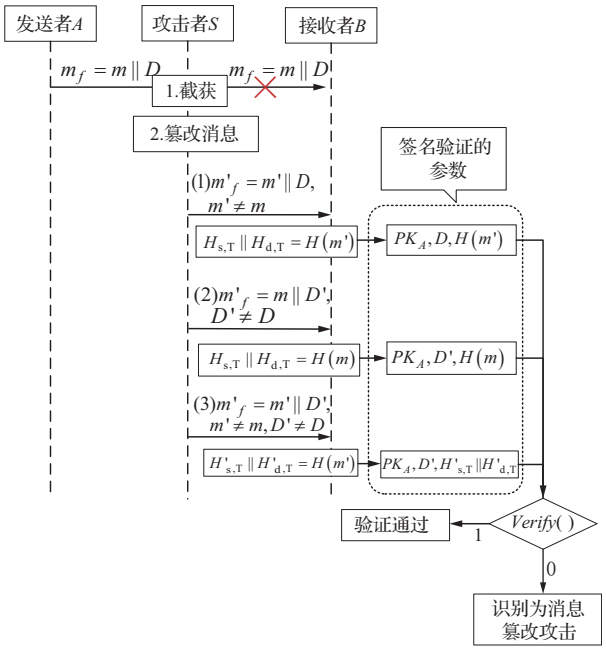

图4 所提方案抵御消息篡改攻击的手动分析

Fig.4 Manual analysis results of the proposed scheme against message tampering attacks

5.2 自动化分析结果

Scyther[28]是一种实现安全协议自动化分析的工具，我们利用Scyther对本文所提方案进行了安全性形式化验证。

首先，定义一个包含两个角色(无人机自组网中任意无人机节点$I,R \in \mathcal{U}$且$I \neq R$)的安全协议Sec及哈希函数等全局变量，协议框架描述如下：

```
1 protocol Sec(I,R){
2 role I{…}
5 role R{…}
8 }
```

其次，角色I,R内部都需要保证协议每一轮执行时动态明文信息、时间戳和随机数(Nonce)的新鲜性(fresh)。

```
1 role I {
2 fresh mI: Mymessage;
3 fresh nI: Nonce;
4 fresh T1: Timestamp;
5 fresh Y1;
6 …
7 }
8 role R {
9 fresh mR: Mymessage;
10 fresh nR: Nonce;
```

```
11 fresh T2: Timestamp;
12 fresh Y2;
13 …
14 }
```

接下来，在通信过程中，每个角色既是发送方也是接收方。第一轮通信事件中，角色I作为发送方首先对动态明文信息、时间戳以及随机数计算消息摘要，然后利用I的私钥SK_I对摘要签名，并执行发送事件send_1()将消息内容与签名一同发送给作为接收方的R；接收方R通过接收事件recv_1()接收来自send_1()的信息，并利用哈希函数和发送方I的公钥进行摘要计算和签名验证，若通过验证，则角色R作为发送方对作为接收方的角色I发起第二轮通信，即执行发送事件send_2()与接收事件recv_2()。

最后，根据本方案对拓扑信息的完整性保护的需求，我们声明协议的三个安全属性：存活性（Alive）：只要角色参与过该协议即满足存活性认证，表明角色可能与任一角色或攻击者通信。非单射一致性（Niagree）：发送方和接收方的协议分析结果中的数据变量集合是一致的，若数据变量集合不满足一致性，则说明有攻击者通过重放攻击成功误导两个参与方主体使得协议结束后数据变量集合的某些变量值不同。非单射同步（Nisynch）：只关注发送和接收事件中消息的内容和顺序，即保证消息完整性的安全需求。如果攻击者不篡改消息内容仅转发消息，这种情况在非单射同步声明中不被认为是攻击）。安全声明描述如下。

```
1 role I {
2 …
3 claim_i1(I, Alive);
4 claim_i2(I, Niagree);
5 claim_i3(I, Nisynch);
6 }
7 role R {
8 …
9 claim_r1(R, Alive);
10 claim_r2(R, Niagree);
11 claim_r3(R, Nisynch);
12 }
```

使用Scyther自动化工具执行验证的结果显示，本文的安全协议在限制范围内没有找到攻击，并且通信双方的安全属性声明（alive, niagree, nisynch）全部满足。证明了通信双方（I,R）基于本方案的通信和认证过程是安全的。

6 试验仿真与分析

6.1 试验设置

基于OPNET平台搭建无人机自组织网络仿真环境，对所提方案进行性能验证。WCA[7]与DCA[10]协议都是基于分簇结构的经典无人机自组网路由协议，路由建立过程中均包括了广播、单跳和多跳消息传输的过程，并且消息中均包含动、静态两种信息，符合所提出的路由协议安全保护机制的假设条件，因此我们选择以上两个协议作为试验分析对象。首先，在仿真平台实现WCA和DCA两个路由协议；然后，分别在以上两种路由协议中引入本方案所提出的完整性保护机制，以此来验证本文所提方案在不同路由协议中的有效性。路由协议的试验仿真参数见表2，试验硬件环境见表3。

表2 试验仿真参数值

Table 2 Parameter values in experimental simulation

参数/单位	取值
节点数/个	10,20,50,100
仿真区域大小/km^2	10 × 10
仿真时间/s	1000
节点移动模型	Gauss-Markov
节点移动速度/（m/s）	[30,50]
单机传输范围/km	1
MAC协议	IEEE 802.11g
数据传输速率/Kbps	1000
哈希算法	SHA256
数字签名算法	ECDSA

表3 试验硬件环境

Table 3 Experiment hardware environment parameters

操作系统	Windows10
CPU	Intel（R）Core（TM）i5-9400F CPU @ 2.90GHz
内存	8.00GB（RAM）

我们通过两个指标对试验对象进行分析：引入本文提出的路由协议安全保护方法（以下简称安全方法）带来的分簇时长增量与内存开销，分别记为ΔT与$\mathrm{MEM}_{\mathrm{Sec}}(\%)$。这两个指标可分别表示为

$$\Delta T = T_{P+\mathrm{Sec}} - T_P \tag{9}$$

$$\mathrm{MEM}_{\mathrm{Sec}}(\%) = \frac{\mathrm{MEM}_{P+\mathrm{Sec}} - \mathrm{MEM}_P}{\mathrm{MEM}_{P+\mathrm{Sec}}} \times 100\% \tag{10}$$

式中：P表示分簇协议WCA或DCA；Sec表示本文所提的安全方案；T_P与$T_{P+\mathrm{Sec}}$分别表示协议P无安全方法和引入安全方案Sec后的网络分簇形成时长；MEM_P与$\mathrm{MEM}_{P+\mathrm{Sec}}$分别表示协议$P$无安全方案保护和引入安全方案后网络所有节

点的内存开销。

6.2 试验结果

在试验过程中，我们设置网络中无人机节点在仿真区域范围内均匀分布、初始速度一致、初始能量一致。WCA与DCA都属于典型的分层次路由协议，满足本文所提安全保护方案的适用范围，我们将本方案引入到以上两个协议，分别称为WCA_Sec和DCA_Sec，来测试方案在整个无人机网络系统的时间开销和内存开销。图5与图6是在上述设置下得到的试验结果。

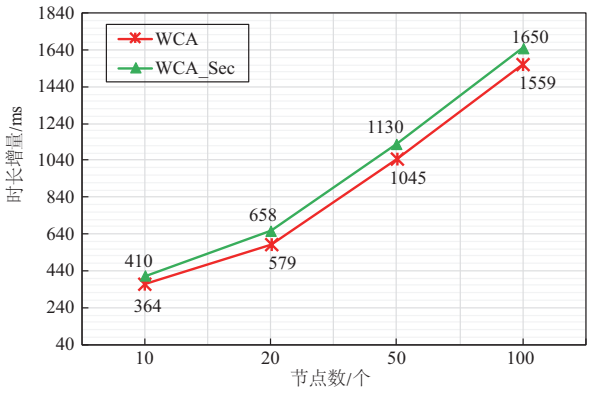

图5 WCA协议引入所提方案后的分簇时长增量

Fig.5 Increment of clustering time of WCA protocol

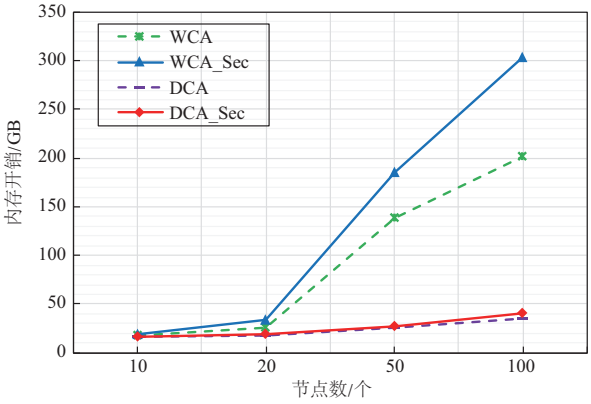

图6 本文所提方案在整个无人机网络系统中的内存开销

Fig.6 Percentage of memory consumption for the proposed scheme in the UAVNET

在不同网络规模下（节点数=10,20,50,100），本方案对WCA和DCA协议的分簇时长的影响如图5所示。可以看出，在WCA路由协议中引入安全方法后（WCA_Sec）的分簇时长增量均小于100ms，引入本文所提安全保护方案对于协议的快速分簇性能影响不大。DCA协议在初始簇划分过程中使用了Lowest-ID分簇算法，该算法由地面站根据无人机节点的ID号迭代执行选举簇头和入簇的过程，不同于WCA路由协议中无人机之间相互通信协作进行自主分簇的过程，所以在DCA协议中引入本文所提安全保护方案对初始簇形成时长没有影响。

图6给出了在不同网络规模下（节点数=10,20,50,100）本文所提安全保护方案在WCA和DCA协议中针对整个无人机网络系统的内存开销情况。当网络节点数为10时，本方案在被测试协议中的内存开销均小于无人机网络系统总开销的5%；当网络节点数为20时，WCA协议中本方案的内存开销占无人机网络系统总开销的24%，DCA协议中本方案的内存开销占无人机网络系统总开销的4%；当网络节点数为50时，WCA协议中本方案的内存开销占无人机网络系统总开销的25%，DCA协议中本方案的内存开销占中无人机网络系统总开销的8%；当网络节点数为100时，WCA协议中本方案的内存开销占无人机网络系统总开销的33.5%，DCA协议中本方案的内存开销占无人机网络系统总开销的11%。结果表明，在两种被测试的路由协议中引入本文所提安全保护方案的内存开销均小于无人机网络系统内存总开销的35%。由于WCA和DCA协议运行时会动态更新无人机网络的分簇结构，拓扑结构的变化导致链路中断的节点频繁使用AODV协议更新路由。在前期研究中发现，相同网络环境下WCA协议的分簇结构更新次数大于DCA协议，网络节点通过AODV协议建立路由开销大于DCA协议，因此WCA协议所带来的开销高于DCA协议。

试验结果表明，本文所提方法通过联盟区块链技术减少了拓扑消息中静态信息的完整性保护带来的传输和加密计算，有效降低了时间和内存开销，使得该方法更加轻量级，其少量的额外开销没有影响路由协议的正常工作。

7 结束语

近年来，无人机自组网在军用与民用领域的应用越来越广，路由协议的安全性是无人机自组网领域面临的重要挑战之一。本文针对无人机自组网分级结构路由协议，重点分析了无人机自组网拓扑信息的特征与协议的安全性需求，提出了针对拓扑消息的轻量级完整性保护方案，保证消息内容不被篡改，从而避免被篡改消息在网络拓扑构建中被利用而形成无效或低效路由。通过非形式化与形式化的安全性分析证明了本文所提方案可以有效抵御假冒攻击和消息篡改攻击。最后，通过试验仿真验证了本方案在时间与内存开销方面对路由协议的影响均在可接受范围内。

参考文献

[1] 卓琨, 张衡阳, 郑博, 等. 无人机自组网研究进展综述[J]. 电信科学, 2015, 31(4): 128-138.
Zhuo Kun, Zhang Hengyang, Zheng Bo, et al. Progress of UAV Ad Hoc network: a survey[J]. Te1ecommunications Science, 2015, 31(4): 128-138. (in Chinese)

[2] 吴兆香, 欧阳权, 王志胜, 等. 基于人工智能的无人机区域侦察方法研究现状与发展[J]. 航空科学技术, 2020, 31(10):57-68.
Wu Zhaoxiang, Ouyang Quan, Wang Zhisheng, et al. Status and development of regional reconnaissance methods of UAV based on artificial intelligence[J]. Aeronautical Science & Technology, 2020, 31(10): 57-68. (in Chinese)

[3] 姜延欢, 杨永军, 李新良, 等. 智能无人系统环境感知计量评价研究[J]. 航空科学技术, 2020, 31(12):80-85.
Jiang Yanhuan, Yang Yongjun, Li Xinliang, et al. Research on environmental perception metrology and evaluation technology of intelligent unmanned system[J]. Aeronautical Science & Technology, 2020, 31(12): 80-85. (in Chinese)

[4] Faraji-Biregani M, Fotohi R. Secure communication between Uavs using a method based on smart agents in unmanned aerial vehicles[J]. The Journal of Supercomputing, 2020, 77(6): 1-28.

[5] Shumeye Lakew D, Sa'ad U, Dao N N, et al. Routing in flying Ad Hoc networks: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(2): 1071-1120.

[6] Zapata M G. Secure Ad Hoc on-demand distance vector routing [J]. Acm Sigmobile Mobile Computing & Communications Review, 2002, 6(3): 106-107.

[7] Maxa J, Mahmoud M S B, Larrieu N. Secure routing protocol design for UAV Ad Hoc networks[C]// 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), 2015.

[8] Maxa J, Mahmoud M S B, Larrieu N. Joint model-driven design and real experiment-based validation for a secure UAV Ad Hoc network routing protocol[C]// 2016 Integrated Communications Navigation and Surveillance (ICNS), 2016.

[9] Maxa J, Mahmoud M S B, Larrieu N. Performance evaluation of a new secure routing protocol for Uav Ad Hoc network[C]// 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), 2019: 1-10.

[10] Perkins C E, Belding-Royer E M. Ad-Hoc on-demand distance vector routing[C]//Workshop on Mobile Computing Systems & Applications, 2002.

[11] Clausen T, Jacquet P. RFC3626 Optimized link state routing protocol (OLSR)[S]. IETF, 2003.

[12] Johnson D. RFC4728 The dynamic source routing protocol (Dsr) for mobile Ad Hoc networks for Ipv4[S]. IETF, 2007.

[13] 孙凌, 罗长远. 基于地理信息的航空自组网安全路由算法[J]. 计算机工程与应用, 2019, 55(12): 77-82.
Sun Ling, Luo Changyuan. Secure geographic information based routing protocol of aeronautical Ad hoc networks[J]. Computer Engineering and Applications, 2019, 55(12): 77-82. (in Chinese)

[14] Lin C R, Gerla M. Adaptive clustering for mobile wireless networks[J]. IEEE Journal on Selected Areas in Communications, 1997, 15(7): 1265-1275.

[15] Basu P, Khan N. Little T. A mobility based metric for clustering in mobile Ad Hoc networks[C]//2001 International Conference on Distributed Computing Systems Workshop, IEEE, 2001.

[16] Sharifi S A, Babamir S M. The clustering algorithm for efficient energy management in mobile Ad-Hoc networks[J]. Computer Networks, 2020, 166: 106983.

[17] Chatterjee M, Das S K, Turgut D. Wca: A weighted clustering algorithm for mobile Ad Hoc networks[J]. Cluster Computing, 2002, 5(2): 193-204.

[18] Ergenc D, Eksert L, Onur E. Dependability-based clustering in mobile Ad-Hoc networks[J]. Ad Hoc Networks, 2019, 93 (OCT): 101926.

[19] Maxa J, Mahmoud M S B, Larrieu N. Performance evaluation of a new secure routing protocol for Uav Ad Hoc network[C]// 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), 2019: 1-10.

[20] Hsiao S J, Sung W T. Employing blockchain technology to strengthen security of wireless sensor networks[J]. IEEE Access, 2021, 9: 72326-72341.

[21] Liu B Y, Xiao L, Chen S, et al. Blockchain based data integrity service framework for IoT data[C]// 2017 IEEE International Conference on Web Services (ICWS), 2017.

[22] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm(Ecdsa)[J]. International Journal of Information Security, 2001, 1(1): 36-63.

[23] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL].[2021-07-01]. https://bitcoin.org/bitcoin.pdf.

[24] Li D, Hu Y, Lan M. Iot device location information storage system based on blockchain[J]. Future Generation Computer Systems, 2020, 109: 95-102.

[25] Zheng Z, Xie S. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[26] 张亮, 刘百祥, 张如意, 等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1-12.
Zhang Liang, Liu Baixiang, Zhang Ruyi, et al. Overview of blockchain technology[J]. Computer Engineering, 2019, 45(5): 1-12. (in Chinese)

[27] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述:原理,进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
Zeng Shiqin, Huo Ru, Huang Tao, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151. (in Chinese)

[28] Cremers C J F. The Scyther tool: verification, falsification, and analysis of security protocols[C]// International Conference on Computer Aided Verification. Springer, Berlin, Heidelberg, 2008: 414-418.

Integrity Protection Method of Routing Message for UAV Ad-hoc Networks

Guo Jingjing[1], Gao Huamin[1], Liu Zhiquan[2], Zhang Xinglong[3]

1. Xidian University, Xi'an 710071, China

2. Jinan University, Guangzhou 510632, China

3. National Key Laboratory of Science and Technology on Integrated Control Technology, AVIC Flight Automatic Control Research Institute, Xi'an 710065, China

Abstract: Security is one of the important challenges that UAV Ad-hoc Networks (UAVNETs) routing protocols is facing. Focusing on the lack of security of topology construction messages on the clustered UAVNETs routing protocols, this paper proposes a security scheme for topology messages of clustered UAVNETs routing protocols (SecUAV). SecUAV can ensure the integrity of the messages exchanged between nodes in the clustered UAVNETs during the topology construction so as to prevent the tampered information from being used in the network topology construction and route creation, and improve the robustness and reliability of routing protocol. Aiming at the static information in the topology message, an integrity verification method based on the consortium blockchain is proposed, which can reduce the calculation and transmission overhead of the entire scheme. We conduct an informal and formal analysis on this scheme, and prove that the scheme could flight against impersonation attack and message tampering attack during the transmission of topology messages. Finally, we simulate and analyze the performance of several UAVNETs clustering protocols with SecUAV. The experimental results show that the time consumption of SecUAV is less than 100ms and the memory cost of SecUAV is less than 35% of the routing cost.

Key Words: UAV Ad-hoc networks; routing protocols; integrity protection; network security

Received: 2021-12-16; **Revised:** 2022-01-14; **Accepted:** 2022-02-08

Foundation item: National Natural Science Foundation of China(62032025,62102167); Aeronautical Science Foundation of China (20185881015)