计算机科学
COMPUTER SCIENCE

基于属性访问控制策略的无人机飞控安全方案

庞宇翔, 陈泽茂

引用本文

庞宇翔, 陈泽茂. 基于属性访问控制策略的无人机飞控安全方案[J]. 计算机科学, 2024, 51(4): 366-372.

PANG Yuxiang, CHEN Zemao. Security Scheme of UAV Flight Control Based on Attribute Access Control Policy [J]. Computer Science, 2024, 51(4): 366-372.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230200135

基于属性访问控制策略的无人机飞控安全方案

庞宇翔　陈泽茂
武汉大学国家网络安全学院空天信息安全与可信计算教育部重点实验室　武汉 430072
(benedict@whu.edu.cn)

摘　要　飞控系统是无人机的核心部件,对无人机的功能和性能起着决定性作用,是无人机信息安全防护的重点对象。文中针对PX4飞控系统面临的恶意代码植入、内部交互数据篡改等安全风险,设计了一种面向位置环境的基于属性的访问控制策略(LE-ABAC),该策略基于访问控制实体属性和无人机外部位置环境信息制定访问控制规则,可以实现对无人机内的数据交互过程进行细粒度控制,保护关键交换数据的机密性与完整性。文中在PX4软件仿真平台上对所提方案进行了攻击仿真实验,结果表明该模型能够在不显著降低无人机飞控效率的前提下,有效保护飞控系统内部交互数据不被窃取和篡改。

关键词:无人机;飞控系统;基于属性的访问控制;信息安全
中图分类号　TP309

Security Scheme of UAV Flight Control Based on Attribute Access Control Policy

PANG Yuxiang and CHEN Zemao
Key Laboratory of Aerospace Information Security and Trusted Computing,Ministry of Education,School of Cyber Science and Engineering,Wuhan University,Wuhan 430072,China

Abstract　The flight control system is the core component of unmanned aerial vehicles(UAVs),which plays a decisive role in the function and performance,and it is a crucial target for information security protection. In this paper,a location-and-environment oriented attribute-based access control(LE-ABAC) policy is designed to deal with the security risks of malicious code injection and internal interactive data tampering faced by PX4 flight control system. The access control policy,based on object entity attributes and external location environment information of the UAV,formulates corresponding rules that enable fine-grained control of the data exchange process within the UAV,protecting the confidentiality and integrity of crucial data exchanges. In the study,attack simulation experiments are conducted on the PX4 software simulation platform to verify the proposed scheme. Finally,the results show that the model can effectively protect the interactive data of the flight control system from theft and tampering without significantly reducing the efficiency of UAV flight control execution.

Keywords　Unmanned aerial vehicle,Flight control system,ABAC,Information security

1　引言

随着通信、信息处理和传感器等技术的进步,无人机已在交通、防灾救援和航道巡查等领域获得广泛应用[1]。无人机在给生产生活带来便利的同时,也不断地暴露出其面临的信息安全威胁。目前,消费级无人机通常更关注无人机飞行功能的正常实现,信息安全防护能力往往比较薄弱,容易受到攻击者的干扰或劫持。为此,需要研究无人机面临的信息安全威胁及其防御技术,在保障无人机正常工作的前提下,保护无人机系统免遭恶意攻击。典型的无人机系统主要由无人机、地面站和通信系统3个部分构成[2-3],面临传感器、无线通信、软件和网络等方面的安全威胁[4]。针对上述安全隐患,现阶段的研究大多聚焦于解决网络通信或者传感器等方面的安全问题,较少考虑无人机飞行控制系统的安全问题。

飞控系统是无人机的核心部件,负责处理来自各传感部件的数据,生成和处理无人机遥测和遥控数据,对无人机飞行的稳定性、数据传输的可靠性以及操作执行的实时性等都有重要影响。随着飞控计算机处理性能的提升,飞控系统的功能也越发的丰富和强大。飞控系统中各软件组件间互相关联和协作,交互频繁。现有的主流飞控系统,往往忽略了飞控系统内部组件交互过程中的安全防护,一旦飞控系统的某些组件存在安全漏洞或被植入恶意软件,攻击者将有机会获取和篡改其中的交互数据流,进而破坏飞控数据的完整性与机密性,损害无人机飞行的稳定性。随着无人机功能进一步变强,

到稿日期:2023-02-17　返修日期:2023-05-11
基金项目:国家自然科学基金面上项目(61872430);国家优秀青年科学基金(42122025)
This work was supported by the National Natural Science Foundation of China(61872430) and National Science Foundation for Outstanding Young Scholars(42122025).
通信作者:陈泽茂(chenzemao@whu.edu.cn)

飞控系统的构成组件的数量势必进一步增多，从而加剧此类安全隐患。

本文以 PX4 开源飞控系统为研究对象，首次将 ABAC 方案应用于飞控系统之中，提出了一种面向位置环境因素的基于属性的访问控制方案(LE-ABAC)，用于保护无人机飞控系统内数据交互过程的信息安全。LE-ABAC 方案综合考虑无人机所处空间位置信息、自然气候干扰等飞行环境因素，通过细粒度的安全策略，约束飞控软件之间数据流动的方向，使无人机在正常执行任务的过程中能够更好地保护数据不被泄露和篡改。本文的主要贡献如下：

1)针对 PX4 开源无人机飞控系统，对其中的软件架构进行了分析，并在此基础上建立其威胁模型，发现其安全问题。

2)设计了一种面向位置环境因素的基于属性的访问控制方案，实现了无人机飞控系统内数据的安全交换与防护。

本文在 PX4 软件仿真平台上实现了 LE-ABAC 方案，分析了其性能，实验结果表明该访问控制机制能对数据的流动方向进行约束，同时在耗时方面相比原系统只增加了 1.4 倍左右，不会对无人机的正常飞行造成影响。

2 相关工作

无人机系统主要面临着传感器安全、通信安全、软件安全以及网络安全等方面的威胁与挑战。Kerns 等[5]的实验研究表明，通过 GPS 欺骗，攻击者能够轻易地捕获和修改无人机数据信息，从而进行拦截和欺骗以完全控制无人机。Kim 等[6]发现，通过创建恶意 TCP 有效载荷，利用无人机内的通信协议能够将其注入无人机的内存，从而在地面站运行的系统上秘密安装恶意软件。文献[7]提出了一种利用超声波来对无人机陀螺仪进行干扰的攻击方法，该方法使无人机失去姿态控制的能力，严重情况下甚至会造成坠机的发生。面对所存在的威胁，研究人员提出了许多的安全方案和策略，其中有关传感器安全[8-10]以及网络通信安全[11-14]等方面的无人机威胁及安全防护的研究较为广泛，但涉及无人机机载软件系统的相关研究较少，尤其是关于飞控系统的安全防护方面。

飞控系统是无人机完成起飞、空中飞行、执行任务、返场着陆等整个飞行过程的核心系统，其安全性至关重要。文献[15]提出了一种通过联合无人机模型的硬件属性、控制算法和物理定律来提取不变量的方法，以实现并插入无人机的控制程序二进制文件中进行不变量检查，以此来检测外部恶意数据对飞控系统的干扰。文献[16]实现了一种虚拟无人机软件架构，提供了监视物理和逻辑系统行为以及检测安全性和安全性违规的机制。当检测到攻击事件后，框架将切换到受信任的控制模式，以覆盖恶意系统状态并防止潜在的安全违规。文献[17]使用可信计算库，提出了一种不变的检查机制来确保物理系统的安全性，以保护具有时序性质的物联网设备免受恶意控制信号的欺骗攻击。尽管上述所提出的安全方案对无人机飞控系统所面临的攻击威胁提出了各种检测与防护手段，但并未对来自无人机飞控系统内部的威胁进行很好的隔离与防护，未关注内部数据交换过程的安全性。

基于属性的访问控制(ABAC)是一种灵活的授权模型，通过对主体属性表达式的描述和运算来实现对客体访问的管理。ABAC 模型在访问控制模型定义、策略描述以及模型的实施中引入了实体属性的概念，通过对主客体及其属性、环境属性以及权限的统一建模来完成对授权的管理，以适应广泛、多样的访问控制需求，并简化了访问控制管理过程。Bhatt 等[18]分析了云化物联网中的访问和通信控制要求，并提出了一种基于属性的访问控制和通信控制框架，以保护物联网架构中各种实体之间的访问和通信。Benson 等[19]提出了一个用于智能汽车生态系统的形式化动态组和基于属性的访问控制模型，不仅考虑了系统范围的安全策略，还考虑了个人用户的隐私偏好。Kim 等[20]首先将 ABAC 应用于无代理发布订阅通信中间件，以改进 DDS 安全模型授权问题。

3 面向位置与环境的 ABAC 模型设计

PX4[21]是一款低成本高性能的高端自驾仪，经过来自工业界和学术界的世界级开发人员多年的开发与完善，目前可支持单旋翼、多旋翼、飞艇等多种载具，在各类民用无人机中获得大量应用。该系统已经形成完善的软件架构，但缺少对内部软件组件间数据交换的安全防护。本章以 PX4 开源飞控系统为研究对象，分析其软件架构，建立其威胁模型，并以此为基础设计相应的访问控制模型。

3.1 PX4 飞控架构

PX4 固件的软件体系结构主要分为 3 层[22]，如图 1 所示。底层为 Nuttx 实时操作系统内核层，负责整个系统的任务调度和设备控制；第二层为中间件层，主要负责机器的通信和硬件的整合，包括用于实现飞控内部进程间数据交换的微对象请求代理器(μORB)；顶层为用户空间层，由各种不同的应用程序组成，能实现飞行控制和数据解算等各类丰富功能。在 PX4 中所有的功能以进程模块为单位进行实现，不同应用进程运算相互隔离，保证各软件模块单元执行过程的独立性与稳定性。然而，尽管每个模块单元独立运行，但模块单元间存在数据交换的需求，共享运行过程中的关键信息，在将其他模块的运算结果作为输入的同时通过自身的运算产生输出。

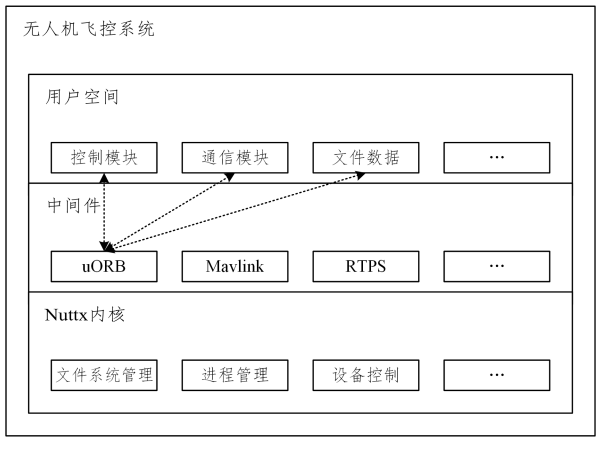

图 1 PX4 飞控架构

Fig. 1 PX4 flight control architecture

μORB 是一套跨进程的 IPC 通信模块，采用了“一对多”的发布订阅模式，以异步通信为基本原则，为飞控系统内不同进程间的通信提供服务[22]，例如传感器数据，地面站控制指令和位置姿态解算结果等数据均由其传递。基于 μORB 机制

的实现，用户空间层的多个进程单元打开同一设备文件，进程间通过此文件节点进行数据交互和共享。在通信过程中，发布者只负责传递数据，订阅者只负责获取数据，进而避免消息的阻塞，降低数据交换的时延。该通信机制能够提高各模块的可控性，也使软件提供商更关注于应用模块的功能设计，加速对应用软件的更新和迭代。

3.2 威胁模型

通过对 PX4 飞控系统软件架构的分析，μORB 作为无人机内部通信机制，承担数据传递的作用。发送数据时，发布者通过 μORB 公告机制创建用于存储数据结构的设备文件，将其作为数据共享的中转站，此后便可通过 μORB 发布机制将数据写入该设备文件。接收数据时，订阅者通过 μORB 订阅机制获取设备文件节点信息，并通过 μORB 拷贝机制将数据内容读取到订阅者模块的数据体中，用于进行后续的运算。通信过程中，发布者只负责数据的发送而不关心数据的去向，订阅者只负责数据的接收而不关心数据的来源，这便使得内部通信过程存在安全隐患。攻击者可以是无人机应用模块的软件供应商或远程软件攻击者，将恶意的代码注入软件进程模块中，如图 2 所示。具体而言，针对存在 PX4 飞控系统 μORB 内部通信的安全威胁有如下两类：

1）机密性攻击。由于发送者只负责数据的发送而不关心数据的接收方，因此进程间共享的数据存在泄露的风险。攻击者通过在飞控应用进程中插入恶意信息订阅者来获取所有的共享消息，并进行数据分析，例如从交互的数据中还原出飞行中的航线信息。

2）完整性攻击。由于接收者只负责数据的获取而不关心数据的发送方，因此进程间的交互数据存在被篡改的风险。攻击者通过在飞控应用进程中插入恶意信息发布者来修改共享消息，使其他正常应用模块获取错误的数据，例如篡改导航模块所获取的 GPS 信息以改变无人机的飞行轨迹。

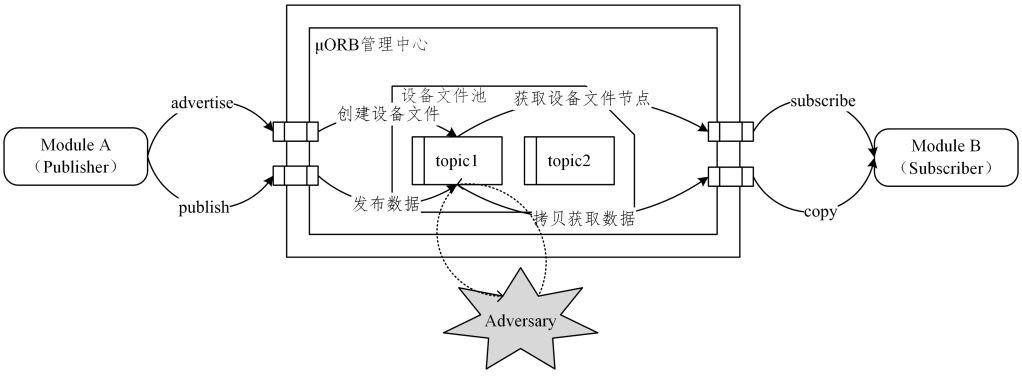

图 2 μORB 通信威胁模型

Fig. 2 μORB communication threat model

无人机在飞行期间时刻采集外部环境数据并时刻监控自身状态，维持稳定状态并实现特定功能。飞行参数和系统日志被存储于飞控系统内部，为无人机飞行计划的实现和安全审计提供服务。μORB 机制所带来的潜在威胁会暴露存储于无人机系统中的关键数据，篡改进程间的交互信息，严重时会导致劫持或坠机的发生。

3.3 LE-ABAC 访问控制模型

为解决飞控系统面临的安全威胁，本节提出了一种面向位置与环境（Location and Environment，LE）的基于属性的访问控制方案（LE-ABAC）。系统管理员能够通过制定相应的访问控制策略，对系统中实体间的数据交换过程进行约束与限制，使恶意数据无法在数据链中随意传输。这些策略需进行统一的管理与调度，同时也受到无人机所处空域和高度等位置与气流风速等环境因素的影响。因此，访问控制模型必须考虑所有实体和 LE 的属性要求，提供细粒度的授权解决方案。LE-ABAC 通过综合考虑无人机所处位置环境信息，为无人机内部的数据交互过程提供更准确的规则约束。

3.3.1 基于属性的访问控制模型

基于属性的访问控制模型通常包括主体、客体、属性和访问控制策略 4 个元素，如图 3 所示。属性用于描述主体和客体的特征，访问控制策略定义了一组规则。策略执行点（PEP）响应主体对受保护客体的访问请求，策略决策点（PDP）将请求中的属性与策略中定义的属性进行匹配，生成决策结果。策略信息点（PIP）是为策略评估提供数据的检索源，助力决策过程。策略管理点（PAP）提供一个用户接口，用于创建、管理策略信息。

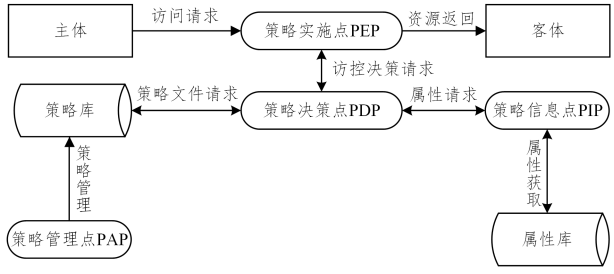

图 3 基于属性的访问控制模型

Fig. 3 Attribute-based access control model

3.3.2 基本元素定义

LE-ABAC 模型如图 4 所示，S，O，OS，OD，LE 分别表示主体、客体、客体集、客体域和位置环境的有限集，OP 表示主体对客体所有操作的有限集。LE-ABAC 为各模型元素定义了属性，SA，OA，OSA，ODA，LEA 分别表示主体、客体、客体集、客体域和位置环境等模型元素的属性值集合。属性是主体、客体或环境条件的特征。LE-ABAC 根据策略规则表达式的描述与运算对主体的访问请求做出批准或拒绝的许可判决。下面结合 PX4 飞控系统，给出了 LE-ABAC 模型元素的定义。

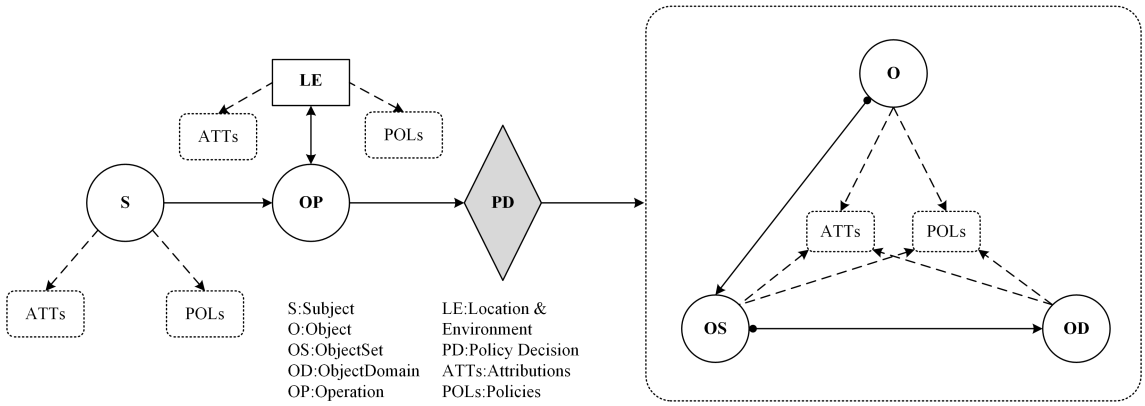

图 4 LE-ABAC 概念模型

Fig. 4 LE-ABAC conceptual model

定义 1(主体，S) 主体是无人机飞控系统中实现功能的应用程序实体，实现无人机的各类功能，执行特定的飞行任务。主体主要包括导航单元、姿态控制单元、位置控制单元、通信单元等软件模块。

定义 2(客体，O) 客体是无人机飞控系统内部进行信息交换的最小数据单元，存储应用模块主体所需的数据内容，例如加速度计的加速度值、高度传感器的高度值等数据。

定义 3(客体集，OS) 客体集是客体中具体数据内容的集合体，在 PX4 内部传输之中被定义为主题，通常由相互关联的数据值构成，形成统一的数据结构体。主体间的数据交互也以此为基础，能够加快传输的速度。例如 GPS 传感器会获取无人机所处位置的经度、纬度等相关数据，这些数据客体会作为一个集合传输到应用程序中，由应用程序自行选择调用。

定义 4(客体域，OD) 客体域是具有相似特征或要求的客体集的逻辑集合。使用客体域可以对客体集进行更好的统一和归约，将属性分配给域成员，简化策略管理人员属性赋值与策略定义等操作过程。例如无人机加速度数据、角速度数据、IMU 数据等客体集通常都为姿态控制所需的数据，可以将其归约到相同的客体域中，赋予共同的属性和策略规则。

定义 5(位置环境，LE) 无人机系统是综合计算、网络和物理环境的多维复杂系统，需要时刻关注所处的位置与环境信息，采取不同的访问控制策略，实现特定功能。位置数据具体表现为地理空间坐标或空域信息，环境数据具体表现为自然气候的干扰，例如可以使无人机在遭遇不同气流的过程中动态智能地选择控制算法，实现更加稳定的飞行。

定义 6(操作，OP) 针对交互数据，操作主要包括对客体的公告、发布、订阅与拷贝等过程。同时，操作还包括访问控制管理行为，例如创建或更新客体、客体集和客体域的属性，制定更新策略规则。

定义 7(属性，ATT) 属性表示其所分配的实体的某些描述性特征，可以被抽象定义为三元组$\langle Attr, Val, Type\rangle$，以表示属性、属性值、属性取值范围的关系。其中，$Attr$ 为唯一标识符，Val 为给定类型的无序原子集或空值集，$Type$ 用于限制原子值的数据类型(例如字符串、整数、布尔值等)。例如，飞控程序主体具有开发者、功能、特权等级等属性，而对象具有作者、所有者、文件功能等属性。

定义 8(属性类型，$attType$) 实体属性取值可以划分为集合或原子值两种类型。$attType: SA \cup OA \cup OSA \cup ODA \cup LEA \rightarrow \{set, atomic\}$定义了属性到属性类型的映射关系，其中 set 表示集合类型，$atomic$ 表示原子值类型。

LE-ABAC 模型定义了在某个位置环境条件下主体可以对客体执行的操作，通过管理授权策略和实体属性，整合不同的实体间信息的流动方向。例如，姿态控制应用程序包括“功能”和“欧拉角”等属性，通过为客体、客体集、客体域赋予“姿态控制”属性，可以使该应用仅获取该领域内所需数据，而不会越权获取例如 GPS 信号等信息。

3.3.3 策略规则

对模型中基本元素的每个属性 $attr$，用 $Range(attr)$ 表示该属性的取值范围。属性获取规则说明如规则 1 所示，定义了实体到属性的映射关系，用于获取每个实体定义的属性内容。

规则 1(属性获取规则) $attr: S \cup O \cup OS \cup OD \cup LE \rightarrow \begin{cases} Range(att), & \text{if } attType(att) = atomic \\ 2^{Range(att)}, & \text{if } attType(att) = set \end{cases}$

属性本质上是动态的，随着无人机的运动与位置环境的变化，属性会被添加或移除，例如 GPS 坐标或速度等数据。管理员或用户制定的策略规则通常表现为静态，只有用于策略配置的属性会影响策略的决策结果，但策略定义仍然相对固定。基于策略管理的便捷性与细粒度考量，主体对对象进行访问操作时需综合对客体、客体集、客体域进行评定，从不同层次上描述访问对象。

规则 2(策略组成规则) $\forall p \in P, Policy_{r_i \in R \wedge r_i \in p}(p) \leftarrow \{permit, deny\}$

规则 3(策略计算规则) $\forall r \in R, \forall op \in OP, \forall le \in LE, Rule_{op,le}(s: SA, o: OA, os: OSA, od: ODA) \leftarrow \{true, false\}$

规则 2 与规则 3 定义了 LE-ABAC 模型的授权策略执行过程。规则 2 定义了每个授权策略由一个或多个不同的判定规则(Rule，R)组成，通过获取组成该策略的所有判定规则的命题结果(True or False)，从而确定该策略执行结果(Permit or Deny)。规则 3 定义了策略中规则的计算方式。对于规则集中的任意规则，当主体处于 le 位置环境下采取 op 操作时，会根据主体和访问对象的属性值计算对应规则的布尔值。

位置环境属性对规则触发的条件进行约束，使处于不同位置以及遭受不同环境干扰下的无人机能返回不同的策略结果。

规则 4（允许覆盖规则）：$Permit\_override_{op,s}(p)=\begin{cases}permit, & \text{if } \bigvee_{r_i\in R\wedge r_i\in p} r_i=\text{true}\\ deny, & \text{other}\end{cases}$

规则 5（拒绝覆盖规则）$Deny\_override_{op,s}(p)=\begin{cases}permit, & \text{if } \bigwedge_{r_i\in R\wedge r_i\in p} r_i=\text{true}\\ deny, & \text{other}\end{cases}$

授权策略采用允许覆盖和拒绝覆盖算法来实现，保证无人机飞控软件模块根据实时的环境信息做出决策判断，使授权策略总能返回允许或拒绝的结果。规则 4 定义了允许覆盖原则策略，对同策略下所有的规则进行析取操作，用“∨”符号表示。如果存在规则的评估结果为真，则合并结果为允许，否则合并结果为拒绝。规则 5 定义了拒绝覆盖原则策略。对同策略下所有的规则进行合取操作，用“∧”符号表示。如果所有规则的评估结果为真，则合并结果为允许，否则合并结果为拒绝。主体满足所有属性规则才能进行访问操作，可使用拒绝覆盖；若主体仅满足某项属性规则，则使用允许覆盖。

例如，用户制定了“飞行高度低于 50m 时，最大飞行速度不超过 40 km/h”的策略，此时当无人机处于该位置环境下时，访问控制机制将会限制导航模块和速度控制模块发送超过规定的数据，在电机驱动模块获取数据消息的过程中也会对数据值进行核查。随着无人机应用场景的丰富，本文提出的访问控制模型可以通过制定细粒度的策略来应对面临的不同环境场景，例如面对航拍无人机侵犯用户隐私问题，无人机管理员可以在特定空域中制定“处于居民楼空域中禁止摄像头驱动接收拍摄命令数据”的策略。

3.3.4 安全性分析

推论 1 $Deny\_override_{sub,s\_a\notin S}(\bigwedge_{r_i\in R\wedge r_i\in p} r_i)=deny$

证明：假定存在恶意的攻击主体 s_a 试图在 le 环境属性条件下未经授权获取关键对象 e 中的数据。此时访问控制系统将读取 s_a 与 e 相关的属性值并利用策略集的规则进行计算，来对订阅流程进行判断，存在如下的形式化表述：

$r_1=Rule_{sub,le}(attr(s\_a),attr(o_e),attr(os_e),attr(od_e))$

由于策略控制管理中并未给攻击主体赋予访问关键对象 e 的权限，规则 r_1 会返回 false 的结论。同时访问控制系统在默认情况下对所有未被策略涵盖中的主体采用拒绝覆盖原则，从而得出推论 1 的结果。因此 LE-ABAC 机制使恶意攻击主体 s_att 无法参与非授权对象的订阅过程，无法越权获取数据，从而保护飞控系统内数据交互的机密性。

推论 2 $Deny\_override_{pub,s\_a\notin S}(\bigwedge_{r_i\in R\wedge r_i\in p} r_i)=deny$

证明：假定存在恶意的攻击主体 s_a 试图在 le 环境属性条件下向未经授权的关键对象 e 发送数据。此时访问控制系统将读取 s_a 与 e 相关的属性值并利用策略集的规则进行计算，来对发布流程进行判断，存在如下的形式化表述：

$r_2=Rule_{pub,le}(attr(s\_a),attr(o_e),attr(os_e),attr(od_e))$

由于策略控制管理中并未给攻击主体赋予向关键对象 e 发送消息的权限，规则 r_2 会返回 false 的结果，并进一步得出推论 2 的结论。因此 LE-ABAC 机制使恶意攻击主体 s_att 无法向非授权对象发布消息，无法篡改正常的数据内容。

通过 LE-ABAC 机制，无人机系统策略管理员能够为运行在其中的应用软件实体和传输数据体赋予属性，并根据飞行计划和目标制定访问控制策略，以约束恶意模块可能的数据篡改和窃听行为，防范无人机飞控系统内部数据交互过程中面临的机密性与完整性威胁。

4 实验及分析

本文基于开源飞控系统 PX4、无人机仿真环境 JMavSim 以及地面站软件 QGroundControl 进行 LE-ABAC 方案实验，以在环仿真的方式验证其安全性与性能。为验证 LE-ABAC 访问控制方案的安全性，我们在 PX4 飞控环境中添加了一个恶意模块，它利用内部通信机制 μORB 破坏其他正常模块间交互数据的完整性与机密性。为了验证该实验方案对无人机系统性能的影响，进行了 LE-ABAC 方案实施前后的飞控系统性能对比。

4.1 实验方案

本节设置的攻击场景为：攻击者利用飞控软件漏洞向其中植入恶意的代码块，并以此为跳板向无人机的姿态控制模块注入恶意数据。算法 1 模拟了攻击者可能采用的一种攻击手段，即：一方面通过订阅数据监听其他模块发布的姿态消息；另一方面将获取的姿态数据按照攻击目的进行修改并发布出去，导致姿态控制模块得到的是被篡改过的异常数据，造成无人机飞行时发生摇摆甚至坠机等后果。算法 1 中第 2—3 行用于订阅设备文件并获取其中的数据内容，第 5—6 行用于对获取的数据体进行修改，最后的循环能够持续地发送篡改的错误信息，使其他订阅该结构体的模块获取的数据在一定时间内总是错误的。

算法 1 攻击者模块模拟代码

输入：原始无人机姿态数据

输出：修改后无人机姿态数据

```
1. 初始化：
2.    Advertise(vehicle_attitude,buffer);
3.    Subscribe(vehicle_attitude);
4. 攻击步骤：
5.    Copy(vehicle_attitude,buffer)
6.    Change_data(buffer);
7.    for i←0 to N do
8.    Publish(vehicle_attitude,buffer);
9.    end
```

针对以上攻击场景，我们基于 LE-ABAC 模型设计了防御方案，防止未授权的主体获得对关键对象的读写权限，对飞控系统内部的数据交换过程实施保护。无人机所处的位置与环境参数对飞行控制十分重要，因此在实验中设置了策略规则触发的位置环境条件，以此为约束进行访问控制方案的实现。为保障飞行安全，姿态控制模块时刻在计算和调整下一时刻的欧拉角，并将该信息与所有需要该信息的模块共享。据此，实验中制定了“当位于 A 空域内且飞行高度低于 3m 时，无人机姿态控制模块只接受姿态状态类数据”这一策略。图 5 给出了该策略的 LE-ABAC 模型的语言描述。

```
permit_override:
{
"Policy":{
  "Rule":{
    Subject:{
      module:{mc_att_control},
      function:{control}
    },
    Object:{
      yaw:{(-5,5)},
     roll:{(-1,1)},
      pitch:{(-1,1)}
    },
   Object Set:{
      theme:{
        vehicle_attitude,
        vehicle_status
},
      usage:{attitude_control}
    },
    Object Domain:{*},
    LE:{
      Height:{3},
      Location:{Airspace-A}
    }
  }
 }
}
```

图 5 LE-ABAC 策略描述示例

Fig. 5 Example of LE-ABAC policy description

4.2 实验结果与分析

图 6(a)给出了在未受到攻击的情况下，悬停状态下无人机姿态控制系统的工作情况，此时 roll 与 pitch 两个方向的欧拉角波动幅度大致在±0.005。如图 6(b)所示，当攻击者模块启动后，将会干扰姿态控制单元对当前无人机姿态信息的判断，破坏输入数据的完整性，使姿态控制模块输出数据也发生错误，此时 roll 与 pitch 两个方向的欧拉角波动较大，无人机的稳定性受到严重干扰，甚至无法维持悬停状态。

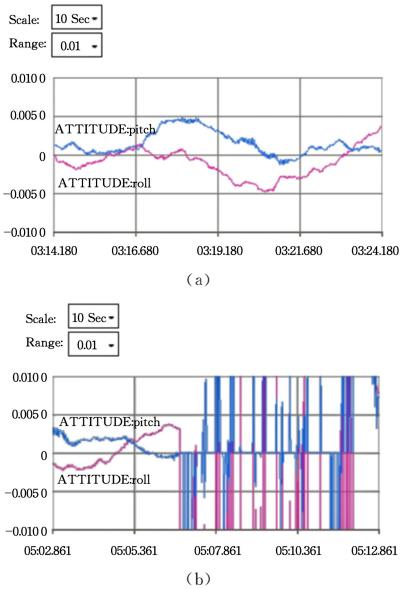

图 6 攻击者模块对姿态数据的影响

Fig. 6 Impact of attacker module on attitude data

图 6 所示的实验结果验证了原系统存在的安全威胁。为解决该问题，在原系统中实现了 LE-ABAC 访问控制机制，制定相应的策略集，对数据的流动方向进行约束。图 7 给出了引入 LE-ABAC 策略后遭受攻击时无人机姿态数据的波动，从中可以看出，roll 与 pitch 两个方向的欧拉角的波动幅度在±0.005 之间，说明此时攻击者已无法将恶意修改的数据内容扩散到其他模块单元。

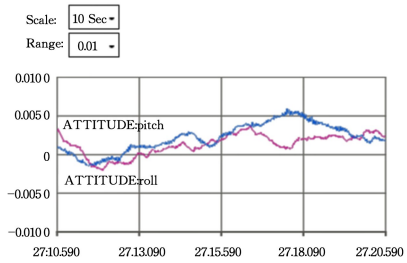

图 7 LE-ABAC 策略防护下受攻击时的姿态数据

Fig. 7 Attitude data when attacked under LE-ABAC protection

本文对 LE-ABAC 方案实现前后飞控系统内部的数据交换性能进行了对比。图 8 给出了 LE-ABAC 方案对原系统可能造成的性能影响。实验结果表明，实施 LE-ABAC 方案会带来一定的时延。若数据交换次数为 100×10^3，则增加了 72.74 ms 的时间，相比原系统延迟了 41.39%，若数据交换次数为 500×10^3，则增加了 364.28 ms 的时间，相比原系统延迟 44.28%，总体而言平均每次数据交换延迟在 40%～50%。从中可以看出，实施 LE-ABAC 方案给飞控系统所带来的额外性能开销很小，不会影响无人机的正常飞行。

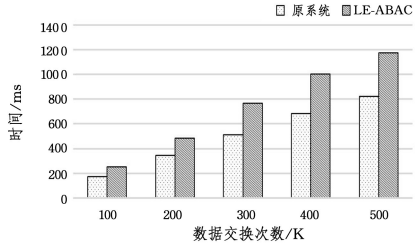

图 8 LE-ABAC 性能评估

Fig. 8 LE-ABAC performance comparison

结束语 本文面向无人机飞控系统内部交互过程的信息安全防护，提出了一种基于属性的访问控制方案 LE-ABAC。该方案为无人机内部数据交换过程中的各个实体建立了相关属性，通过对外部位置环境条件和内部实体属性参数的运算来实现无人机飞控系统内数据的安全交换与防护。实验结果表明，相比未进行任何防护的原系统，LE-ABAC 方案在不影响无人机正常功能的前提下，能够有效缓解飞控系统内部恶意模块对数据交互安全性的威胁。

LE-ABAC 策略和规则的制定需要安全操作员进行管理，针对 PX4 飞控系统中的敏感数据进行区分和标记，这可能会增加系统管理的复杂性。下一阶段需要进行探索以提高系统的可管理性和易用性。同时，该模型目前仅应用于无人机内部数据交互过程，但下一阶段可将其扩展应用于整个无人机系统中或无人机集群中，以更全面地保护无人机系统中的数据资产。

参 考 文 献

[1] LI G. Current Status and Trends of Unmanned Aerial Vehicles [J]. Modern Industrial Economy and Informationization, 2021, 11(3): 12-13, 16.

[2] HE D J, DU XIAO, QIAO Y R, et al. Review of Unmanned Aircraft Information Security [J]. Chinese Journal of Computers, 2019, 42(5): 1076-1094.

[3] AHMED F, MOHANTA J C, KESHARI A, et al. Recent Advances in Unmanned Aerial Vehicles: A Review [J]. Arabian Journal for Science and Engineering, 2022, 47(7): 7963-7984.

[4] IQBAL S. A study on UAV operating system security and future research challenges [C]// 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2021: 759-765.

[5] KERNS A J, SHEPARD D P, BHATTI J A, et al. Unmanned Aircraft Capture and Control Via GPS Spoofing [J]. Journal of Field Robotics, 2014, 31(4): 617-636.

[6] KIM A, WAMPLER B, GOPPERT J, et al. Cyber attack vulnerabilities analysis for unmanned aerial vehicles [M]. Infotech@Aerospace 2012. 2012: 2438.

[7] SON Y, SHIN H, KIM D, et al. Rocking drones with intentional sound noise on gyroscopic sensors [C]// 24th USENIX Security Symposium (USENIX Security 15). 2015: 881-896.

[8] QUINONEZ R, GIRALDO J, SALAZAR L, et al. SAVIOR: Securing autonomous vehicles with robust physical invariants [C]// Usenix Security. 2020.

[9] SHEN J, WON J Y, CHEN Z, et al. Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under GPS spoofing [C]// Proceedings of the 29th USENIX Conference on Security Symposium. 2020: 931-948.

[10] MUNIRAJ D, FARHOOD M. A framework for detection of sensor attacks on small unmanned aircraft systems [C]// 2017 International Conference on Unmanned Aircraft Systems (ICUAS). IEEE, 2017: 1189-1198.

[11] ZHANG L H, WANG S, ZHOU H, et al. Secure communication scheme for UAS based on MAVLink protocol [J]. Journal of Computer Applications, 2020, 40(8): 2286-2292.

[12] HARTMANN K, STEUP C. The vulnerability of UAVs to cyber attacks—An approach to the risk assessment [C]// 2013 5th international Conference on Cyber Conflict (CYCON 2013). IEEE, 2013: 1-23.

[13] JAVAID A Y, SUN W, DEVABHAKTUNI V K, et al. Cyber security threat analysis and modeling of an unmanned aerial vehicle system [C]// 2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE, 2012: 585-590.

[14] TSAO K Y, GIRDLER T, VASSILAKIS V G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks [J]. Ad Hoc Networks, 2022, 133: 102894.

[15] CHOI H, LEE W C, AAFER Y, et al. Detecting attacks against robotic vehicles: A control invariant approach [C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 801-816.

[16] YOON M K, LIU B, HOVAKIMYAN N, et al. Virtualdrone: virtual sensing, actuation, and communication for attack-resilient unmanned aerial systems [C]// Proceedings of the 8th International Conference on Cyber-physical Systems. 2017: 143-154.

[17] HASAN M, MOHAN S. Protecting actuators in safety-critical IoT systems from control spoofing attacks [C]// Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things. 2019: 8-14.

[18] BHATT S, SANDHU R. Abac-cc: Attribute-based access control and communication control for internet of things [C]// Proceedings of the 25th ACM Symposium on Access Control Models and Technologies. 2020: 203-212.

[19] GUPTA M, BENSON J, PATWA F, et al. Dynamic groups and attribute-based access control for next-generation smart cars [C]// Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy. 2019: 61-72.

[20] KIM H, KIM D K, ALAERJAN A. ABAC-based security model for DDS [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 3113-3124.

[21] YANG X C, LIU G, WANG Y T, et al. Overview of Open Source Flight Control Project and Its Aeronautical Application Prospect [J]. Aerodynamic Missile Journal, 2018(4): 25-32.

[22] MEIER L, HONEGGER D, POLLEFEYS M. PX4: A node-based multithreaded open source robotics framework for deeply embedded platforms [C]// 2015 IEEE International Conference on Robotics and Automation (ICRA). IEEE, 2015: 6235-6240.

PANG Yuxiang, born in 1998, postgraduate. His main research interests include information system security and trusted computing.

CHEN Zemao, born in 1975, Ph.D, professor. His main research interests include information system security, trusted computing and equipment information security.

(责任编辑:喻藜)