2020年第八届IEEE移动云计算、服务和工程国际会议（MobileCloud）。

基于硬件安全的全球安全的无人机认证系统

Dominic Pirker*†, Thomas Fischer*†, Christian Lesjak†, Christian Steger*
电子邮件。{dominic.pirker, thomas.fischer3, christian.lesjak}@infineon.com, steger@tugraz.at
*奥地利格拉茨技术大学技术信息学研究所，格拉茨，奥地利
格拉茨#研究中心，Infineon Technologies AG，格拉茨，奥地利

摘要--
无人机在其通常的爱好者、区域记录和监视服务的市场之外，通过云计算的应用和其巨大的综合计算能力获得了吸引力。这些应用使无人机市场迅速增长，从而提高了安全解决方案的优先级。巨大的事件，如伦敦的空中交通中断（2018年12月），提高了对无人机识别、认证和跟踪的认识和需求。为了防止这类事件，航空当局，如FAA或EASA，目前正在制定适当的法规。法规的实施需要可靠的技术解决方案。

本文基于可靠的安全机制和标准化的协议，提出了一个安全的、全球可操作的无人机认证系统。因此，这个系统必须提供相互和强大的加密认证。首先，TLS协议被用于相互认证和保护通信。然后，实施硬件安全，将必要的密钥和证书存储在一个受保护的存储器中，从而支持TLS握手，以避免对纯软件实现的常见攻击。最后，介绍了一个保护传感器值的概念。所提出的无人机认证概念通过概念验证的方式进行了展示，对性能进行了评估，并与现有的解决方案进行了比较。

***Index Terms-UAV*, authentication, protected sensor values, TLS, hardware-security**

I. 简介

无人驾驶飞行器（UAV）的识别是一个日益受到关注的问题，尤其是在这些天，由于发生了几起国际上的重大事件。最重要的一个方面是防止无人机飞入或飞过关键区域。这些区域可能是机场、发电厂、拥挤的地方、石油管道等。

在这项工作中，我们提出了一个用于商业无人机的全球安全无人机认证系统的概念，并对其与其他解决方案进行了评估。建议的系统为无人机的飞行控制提供可靠的认证。由于使用了标准化的协议、经过认证的硬件安全模块（HSM）和全球可用的物理链路，建议的认证系统对即将出台的法规具有吸引力。在图1中，描述了无人机认证系统的一般用例图。一个飞行员想操纵一个无人机。无人机，也就是它的飞行员，必须进行认证，并将其位置信息发送到由地区当局管理的飞行控制服务器。如果无人机出现了被禁止的运动或行动，飞行控制服务器需要根据地区当局制定的法规和规则通知飞行员。

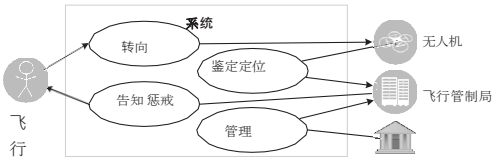

图1. 认证的无人机转向的用例图

II. 最先进的技术

到目前为止，还没有关于无人机数字识别的法规需要考虑。在这种情况下，认证是一种加密的可验证的识别。关于无人机认证的法规是不存在的。无人机是欧盟层面上讨论最多的话题，欧盟航空安全局（EASA）是负责的机构，联邦航空管理局（FAA）是美国的对应机构。从2019年年中开始，关于无人机操作的规定已经逐步发布，EASA预计到2022年将完全适用[1]。

独立于当局的法规草案，一些系统正在开发中，以控制日益增长的民用无人机市场。正在开发的系统的概念各不相同，但大多数概念是不合适的，原因有二。首先，大多数系统需要在实际识别之前进行检测，例如基于雷达的方法。第二，大多数系统需要基站，导致巨大的基础设施成本，因为每个要观察的区域必须在基站的范围内。

这项工作的主要贡献是。

- 提出一个全球性的、安全的无人机认证系统，其传感器值受到远程攻击的保护。
- 设计和实施一个由HSM支持的拟议系统的概念验证
- 对照现有系统进行评估并分析潜在的威胁

A. 沃达丰RPS

沃达丰正在开发一个名为沃达丰无线电定位系统（RPS）的系统，该系统基于4G。该系统要求无人机配备一个4G调制解调器和一个用户身份模块（SIM），以实现关键功能，如跟踪和识别。追踪算法从蜂窝网络中提取位置信息

978-1-7281-1035-6/20/$31.00 ©2020 I E E
DOI 10.1109/MobileCloud48802.2020.00020

通过结合检测到的小区信息。由4G调制解调器收集的基于小区的位置信息被发送到服务器，在那里数据与无线电指纹数据库相结合，以估计无人机的位置[2]。无人机的识别是基于与移动网络的SIM卡建立连接时进行的认证过程。

B. 基于控制信号的系统

通过从控制信号中提取information，可以对无人机进行识别和跟踪。无人机的收发器会广播遥测数据和其他信息，如序列号和位置信息。如果无人机在基站的范围内，这些系统就会收集这些信息。范围是有限的，取决于连接到接收单元的天线。基于控制信号的系统是专有的，因为无人机制造商不遵循任何控制信号的共同标准。为了监测关键地区的全球空中交通，必须从头建立一个基础设施。唯一可用的商业系统是大疆的AeroScope，它的探测范围可达50公里[3]。除了大疆的AeroScope，还有许多其他基于控制信号的系统。在[4]中，数据包的长度被用来区分不同类型或供应商的无人机。

C. 基于雷达的解决方案

另一种实验性的无人机定位方法是基于雷达系统的。这种方法有很多困难，因为无人机的物理尺寸很小，使得检测和分类对传统的雷达来说具有挑战性。在[5]中，分类问题得到了部分解决，但识别问题仍未得到支持。

D. 替代概念

在[6]中提出了一个使用人工智能的基于图像的检测和识别系统。这是一个两步程序，首先在图像上检测无人机，然后将无人机分类为供应商模型。[7]中也提出了一个类似的方法，即用声波来区分不同的无人机供应商。这两个系统不能识别单个无人机，只能识别类型和供应商。

一个有前途的无人机识别和监测概念是基于自动识别系统（AIS），该系统被用于船舶和船只的交通服务[8]。在[9]中，对基于AIS系统的威胁进行了识别。这些威胁分为基于软件和基于射频的威胁，其中欺骗、劫持和可用性破坏是可能的攻击载体。

E. 现有系统的主要弊端

总而言之，基于控制信号或雷达的系统的主要弱点是缺乏识别能力和仅有本地覆盖。沃达丰的RPS缓解了这些问题，但由于识别功能依赖于4G，它不支持最先进的安全机制，如数据完整性和认证。

III. 全球和安全的认证系统

本文提出的认证系统应抵制现有的问题和最先进系统的弱点。在此基础上，确定了以下要求。

- *认证*不仅是识别，这意味着必须有一个证明身份的可能性。提供受保护的传感器值，对远程攻击具有防篡改性。
- *全球供应*是避免区域性亲货币系统的必要条件。
- 为履行安全和隐私义务，需要有真实性、可信性和完整性的*保护性通信*。
- *主管部门接受的机会很高*，因为只有这些部门可以要求无人机制造商实施和使用所建议的系统。

A. 一般概念

考虑到一般用例（图1），两个重要的当事方是无人机和监测无人机活动的飞行控制。在图2中，显示了与无人机HSM扩展一起的连接概况。

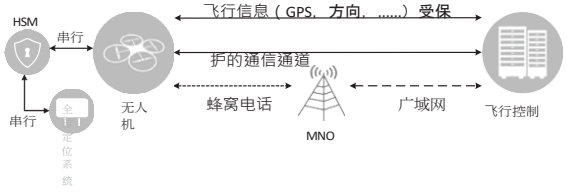

图2.无人机和飞行控制之间的连接概述

为了满足全球连接的要求，不需要再花费昂贵的基础设施费用，同时也要有一个无线连接，无人机通过蜂窝网络连接到互联网。如图2中的连接概述所示，必须建立一个受保护的通信通道以满足安全要求。拟议的无人机认证系统的关键点之一是结合传输层安全（TLS）认证程序，并通过安全的通信渠道交换可信的位置信息和额外的无人机信息。TLS协议是一个最先进的、成熟的、经IETF批准的安全协议，它提供保密性、真实性和完整性。TLS协议的纯软件实现很容易受到传统的网络和旁门左道的攻击，这都会导致提取机密信息[10]。直接在主机控制器上存储机密信息会引发密钥提取或身份克隆攻击。因此，本系统使用的TLS协议是由连接到无人机的HSM支持的。HSM为认证密钥和证书提供了一个受保护的存储空间，这对于执行TLS协议中的认证程序是必要的。认证程序使用X.509证书，其中包含了关于以下方面的信息

产权人，这也被用来验证产权人的身份。

除了保护数字钥匙和防止钥匙被攻击外，HSM还被用来向主控制器提供受保护的传感器值。如图2所示，包含无人机位置信息的飞行信息数据是通过受保护的通信通道进行交换的。

B. 协议栈

为了在数据传输过程中明确划分责任，并允许高效的跨平台实施，需要一个通信协议栈。根据ISO/OSI模型，图3描述了通信协议栈，它与HSM的接口一起被扩展到拟议的无人机认证系统中。

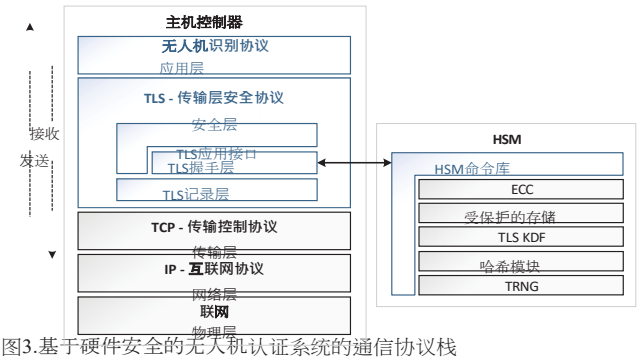

图3.基于硬件安全的无人机认证系统的通信协议栈

1) 应用层。在这个应用中，无人机ID协议代表飞行信息数据。它包含全球定位系统（GPS）的坐标，这些坐标必须在无人机和飞行控制之间传输。

一个控制了主机控制器的对手可以试图改变发送到飞行控制服务器的GPS值。为了缓解这个问题，传感器的值通过I2C总线直接连接到HSM，而主机控制器是无法访问的。

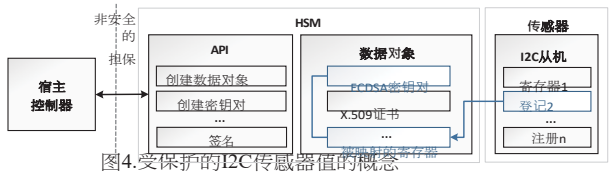

图4.受保护的I2C传感器值的概念

如图4所示，相应的传感器寄存器被映射到HSM的一个数据对象。一个ECDSA密钥对被永久地链接到这个数据对象上，这意味着只有这个特定的数据对象可以用这个密钥签名。每个传感器的输出都用私钥签名，然后提供给主控制器作进一步处理。有了这项措施，主控制器只接收经过签名的传感器值。因此，系统可以确保在每一个时间点上，传感器

价值（本例中的GPS）没有被篡改。非证书，如时间戳或序列号，可以减轻重放攻击。

为了通过通信渠道传输传感器的数值，需要进行数据序列化，将数据对象转化为数据流。一些具有不同目的的数据序列化格式已被定义和标准化。因此，大多数应用可以建立在现有的标准之上。在评估章节中给出了四种常见格式的比较（见V-B节）。

2) 安全层。为了保护通信渠道，在安全层使用了TLS协议，它能够进行相互认证。该协议的主要组成部分是记录层、握手层和应用接口，如图3所描述。

记录层提供的安全属性是保密性、真实性和完整性，如[11]中所述。这个TLS协议的实现是由HSM支持的，因此TLS层在主机控制器和HSM之间被分割。分区取决于应用和HSM的功能。一个典型的TLS在[12]中描述了分区的情况。

图5描述了由HSM支持的服务器和客户端之间的握手序列。在相应的RFC[11]中给出了详细的分步描述。在本节中，与HSM交互的步骤与认证所需的三个步骤一起被描述（在图5中强调）。

关于无人机认证系统的第一个关键步骤是*CertificateRequest*消息（*客户认证步骤*）。(图5中的（1）），它迫使客户发送一个用于相互认证的证书。根据TLS标准[11]，该信息是可选的，但在建议的概念中是必须的。客户端的*认证*信息（图5中的步骤（2））包含了从HSM的受保护认证存储中获取的客户认证。它被用来验证无人机与飞行控制服务器的关系。接收后，服务器对收到的证书进行验证。*验证*信息（图5中的步骤3）包含HSM使用私钥计算出的签名，以及到目前为止发送和接收的所有TLS握手信息的散列（由HSM创建）。这可以验证客户拥有与用于认证的证书相对应的私钥，并防止信息重复使用[11]。服务器使用之前收到的证书上的公钥，来验证客户端使用私钥生成的签名。

这意味着无人机（客户端）验证的基本信息是。*认证请求（CertificateRequest）*信息、客户*认证（Certificate）*信息、*认证验证（CertificateVerify）*信息（在图5中强调和列举）。任何可能的握手流产都发生在相应的消息解析过程中。

*3) 物理层。LTE Advanced*是最先进的无线通信技术，覆盖面积大，特别是在文明附近，因此被选择用于拟议的系统。由于*LTE Advanced*仅用于通信，并与上层明确分开，它很容易被5G取代。

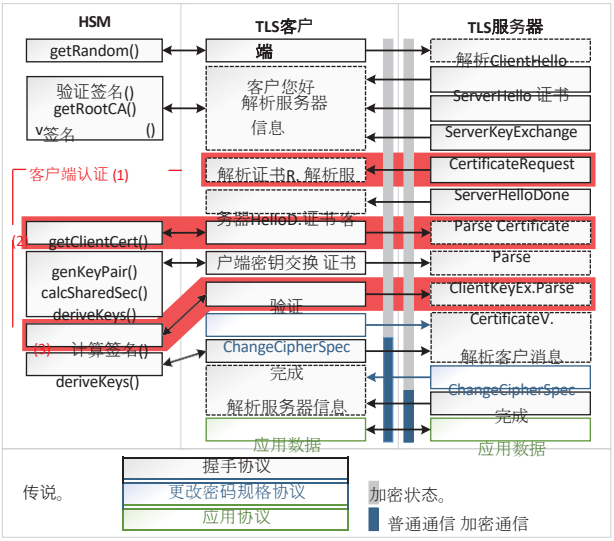

图5.基于硬件安全支持的TLS握手序列（修改自[13]）。

IV. 概念验证

A. 证书供应架构

对于概念验证的实施，使用了一个简单的公钥基础设施（PKI）。提供证书的根是拥有根CA证书的CA机构（Certificate Authority）。无人机和飞行控制服务器都必须存储CA证书。此外，CA向无人机和飞行控制服务器提供相应的证书。CA证书的公钥被用来通过验证计算出的签名来检查对方的有效性。证书的交换和验证是在TLS握手过程中完成的，如*安全层*第III-B2节所述。

B. 软件架构

1) 无人机软件结构。所选HSM的现有命令库是用C语言编写的，因此在无人机上运行的应用程序也是用C语言编写的，以避免重新编写命令库或编写一个包装器。无人机应用程序有两个任务。UAV ID和RC中继。遥控中继任务通过UART将收到的转向命令转发给飞行控制器。在概念验证中，转向命令是由飞行控制服务器发送的。在实践中，转向命令将由操作员的远程控制来传输。无人机ID任务从GPS模块或任何使用的定位系统中提取位置信息，按照CBOR格式将其序列化，并将数据发送到飞行控制服务器。为了明确区分这些任务的责任，每个任务都使用一个专门的TLS安全的TCP/IP套接字进行通信。

2) 飞行控制服务器软件结构。飞行控制服务器软件的结构类似于无人机上运行的软件结构。该应用程序由一个GUI扩展，用于交互。

C. 硬件架构

用于概念验证的无人机硬件如图6所示，由放置在电池和碳架上的叠加模块组成。电机控制板（ESC板）、Raspberry Pi和LTE模块在市场上可以自由购买。飞行控制器板*Larix Edu*是*Innsbruck管理中心*和*Infineon技术公司*的一个多旋翼项目[14]。该板是围绕着Infineon 32位工业微控制器建立的。它根据通过UART连接的Raspberry Pi的远程控制命令，使用脉冲宽度调制（PWM）来控制ESC板。LTE基座是根据[15]重新设计的。该基座的主要组件是一个嵌入式SIM（eSIM）和HSM。LTE模块本身通过一个Mini PCIe连接器连接到基础屏蔽上。

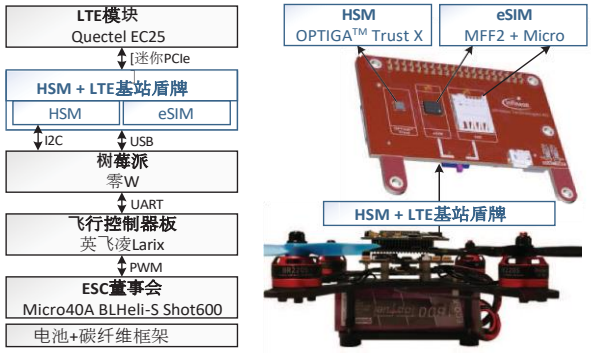

图6.无人机硬件实现

飞行控制服务器是用Raspberry Pi 3和一个用于交互的触摸屏显示器实现的。由于服务器不是这项工作的重点，所以不作详细描述。

V. 评价

A. 威胁模式

拟议系统的威胁分为物理攻击和远程攻击。对于物理攻击，对手必须对无人机硬件进行篡改。侧信道攻击可以被用来从HSM中提取密钥材料[10]。拟议的系统通过整合HSM与受保护的密钥材料存储，来加强对这些攻击的防范。如果对手篡改了硬件，其余的保护措施会将钥匙保存在HSM中，并防止钥匙被克隆。

远程攻击是指对手无法从物理上接触到无人机的威胁。为了防止远程软件损坏，需要采取安全启动等措施。通过使用受保护的I2C传感器值的概念，可以防止针对主机控制器的远程攻击，以改变从GPS接收的数值。这个概念的缺点是对每个传感器输出进行必要的签名而引入的延迟。功耗也增加了，因为在操作过程中也需要HSM，而不仅仅是在TLS连接建立期间。

建议的系统安全性不依赖于4G的安全措施，因为4G链接只用于运输。如果4G干扰被用来干扰控制链路，无人机的*故障安全*模式将被触发。如果无人机的ID受到干扰攻击的影响，控制链路的插座可以被关闭，以便也触发*故障安全*模式。

建议的系统可以适用于非商业或专有的无人机，但如果没有这个系统，就不可能阻止无人机发射，只能通过法律强制执行。由于商用无人机的市场份额是定制无人机的七倍，因此，这种解决方案的必要性是尖锐而不可避免的。然而，如果对手想要执行被禁止的行动，要么可以从头开始制造无人机，要么可以对商用无人机进行软件修改或对硬件进行篡改。为了减轻这些威胁，可以考虑在高度关键地区使用基于雷达的解决方案，这也可能检测到没有认证系统的无人机。

B. 序列化格式

移动应用，如无人机认证系统，通常资源有限，因此，编码数据的大小是一个关键属性。这意味着，所选择的数据序列化格式应该对给定的应用具有最小的编码开销。此外，系统被接受的机会应该最大化，这意味着应该使用一个完善的、标准化的格式。所选择的实现方式的序列化速度和易用性也是至关重要的因素。为了选择数据序列化格式及其具体实施，对几种广泛传播的标准化格式和实施方案进行了比较，如表一所示。为了进行比较，我们使用了一个大小为26字节的原始数据集，其中包含位置信息和一个额外的8字节的字符串。

表一
数据序列化格式的比较

格式	ASN.1	CBOR	ÄÄÄ	XDR
原始[字节]	26	26	26	26
编码[字节]	34	31	57	32
开销[字节]	8	5	31	6
间接费用[%]	31	19	119	23
编码[ms]	0.622	0.045	0.500	0.258
解码[ms]	0.405	0.041	0.160	0.101
Python库	淘宝网	cbor	bson	xdrlib
图书馆版	0.122.0	1.0.0	0.5.6	0.0.0
标准化	ISO	RFC	BSON规格	RFC

表一显示，与ASN.1、BSON和XDR相比，CBOR的编码开销最低，使用测试库对测试数据的编码和解码速度最快。如果信息在无线信道上每秒发送数次，如拟议的无人机认证系统的情况，这些都是关键的效率特性。由于根据CBOR标准提供了用于编码和解码的软件库，避免了大量的库实施。CBOR规定了字段的类型，但没有规定其用途。因此，对原始数据字段的正确排序是必要的，这是通过在传输层使用TCP来解决这个问题。CBOR被IETF作为RFC推广（见[16]），这增加了当局接受的机会。基于这些优势，CBOR被选择作为应用层的序列化格式。

C. 间接费用评估

开销评估是在Raspberry Pi 3（Model B+）上用Wireshark完成的。服务器和无人机之间发送的数据包被捕获和分析。

在概念验证的实施中，TLS握手的总开销为1500字节。每个椭圆曲线
密码学（ECC）证书的大小为~500字节。该
概念验证的实现只在每台设备上使用一个认证。
鉴别的一方。这意味着每个证书链，在TLS与客户和服务器握手期间发送
*认证*信息，只包含一个认证。这导致了10000字节的证书。其他握手方式
信息占用了剩余的500字节。

建议的三个基本握手信息为
图5中强调的无人机认证系统，在TLS标准中是可选的，因为它的错误。这意味着，通常是可选的，但在这种情况下是强制性的TLS功能的开销
导致总长度为1500字节中的600字节（ECC证书为500字节）。

在记录层，应用数据是加密的
并发送。由于概念验证的实施所选择的序列化格式是CBOR，如表一所示，示例应用数据的大小为31字节。考虑到用于原型的密码套件（TLS ECDHE ECDSA WITH AES 128 GCM SHA256）。
记录层的开销是由头（5字节）¯、最大填充大小¯（AES128：最大15字节）和MAC的大小（SHA-
256：32字节）组成。这导致记录层的每个消息的总大小为83字节。

总开销被认为是，因为开销的主要部分是在TLS握手过程中产生的，这在连接建立过程中只发生一次。

D. 与最先进的系统比较

表二描述了无人机认证系统的基本属性，以及最先进系统和拟议系统的可用性。

拟议的无人机认证系统是基于标准化的协议和最先进的硬件安全。使用标准化的协议进行认证（TLS）和数据序列化（CBOR），而不是使用专有协议，可以增加向权威机构（如FAA或EASA）提交所提出的系统以影响未来法规的机会。在这种情况下，无人机的认证是至关重要的部分。TLS协议不仅用于认证，而且还用于保障通信渠道的安全。首先，主机和HSM之间的TLS层分区为密钥和证书提供了一个受保护的存储空间。其次，这个设计决定允许缓解

表二
无人机认证系统的比较

	沃达丰RPS	大疆创新的Aero Scope	基于雷达的	基于图像的	基于AIS的	文件中建议
可利用性	全球 (4G)	当地	当地	当地	当地	全球 (4G*)
基础设施类型	服务器	基站	基站	基站	基站	服务器
安全机制	4G	符号。加密	没有	没有	没有	4G，TLS（带HSM）
识别/认证	是的/是的	是/否	没有/没有	没有/没有	是/否	是的/是的
必须进行无人机硬件改造	是	是（除大疆外）。	没有	没有	没有	是
可能的额外数据载荷	没有	是	没有	没有	没有	是
受保护的ID存储	没有	没有	没有	没有	没有	是

主控制器不需要处理昂贵的加密图形操作，而且对旁门左道的攻击更加有力。就未来即将出台的法规而言，认证的安全性是一个基本属性。在拟议的系统中，使用了通用标准认证的EAL6+硬件，即Infineon OPTIGA™ Trust X。

这个系统是一个*认证*系统，与大疆的AeroScope相反，它只是一个探测和跟踪系统。也就是说，AeroScope系统需要先探测到一个无人机，才能进行跟踪和识别。另一个缺点是探测范围有限，最多不超过50公里[3]，因为每个需要观察的区域都需要配备一个基站。与基站相比，沃达丰的RPS和拟议的无人机认证系统需要服务器来进行通信，并进一步分析所接收的数据。

与Vodafones的RPS系统相比，其优势在于*LTE Advanced*仅用于通信，而不是authentication（表二中用*表示）。这意味着物理信道在任何时候都可以很容易地被未来的任何其他通信信道所取代（例如5G）。如果发生主动认证过程，拟议系统的一个缺点是必须对无人机系统进行修改，这是不可能规避的。它必须配备*LTE Advanced*（或其后续版本），但这也带来了其他可能的使用情况，如超出视线的转向或传输高质量的视频流。此外，额外的软件组件必须在无人机上实现。这些可以被定义为一个标准，以限制无人机制造商的额外实施工作。额外的系统模块带来的另一个缺点是电池持续时间的减少。然而，由于安全方面的巨大提升，这些缺点是可以接受的。

VI. 结论和未来工作

在这项工作中，我们提出了一个基于硬件安全的全球安全的无人机认证系统，用于商业的、不受干扰的无人机。然而，高度敏感地区需要额外的检测，例如基于雷达的检测，以检测少数无人机，在未来不需要认证系统。

由于认证是在连接建立时进行的，用于跟踪的定期消息只需包含位置信息，而不包含识别信息。这就降低了定期数据的开销。使用HSM支持的TLS协议，飞行员的位置数据和隐私受到保护。此外，传感器直接连接到HSM上，而HSM则直接连接在传感器上。

在到达非安全环境之前，对每个传感器的输出进行加密签名，以保护传感器值免受远程攻击。

如图1的用例图所示，飞行控制必须由一个制定法规的机构来管理。这些规定是根据地区而定的，因此有不止一个机构负责管理基础设施。因此，未来的工作将研究一个更复杂、更灵活的信任供应过程，以确保无人机连接到一个可信的、与位置相关的飞行控制。

参考文献

[1] 欧洲安全局。(2019) 民用无人机（无人驾驶飞机）。[在线]。Available: https://www.easa.europa.eu/easa-and-you/civil-drones-rpas

[2] Vodafone.(2007) 沃达丰超越视线的无人机试验报告。[在线].Available: https://www.vodafone.com/content/ dam/vodafone-images/media/Downloads

[3] 大疆，"DJI AeroScope"，https://www.dji.com/at/aeroscope，[在线；ac- cessed 2019-07-30]。

[4] P.Kosolyudhthasarn, V. Visoottiviseth, D. Fall, and S. Kashihara, "Drone Detection and Identification by Using Packet Length Signature," in *2018 15th International Joint Conference on Computer Science and Software Engineering（JCSSE）*, July 2018, pp.

[5] M.Jian, Z. Lu, and V. C. Chen, "Drone detection and tracking based on phase-interferometric Doppler radar," in *2018 IEEE Radar Conference (RadarConf18)*, April 2018, pp.1146-1149.

[6] D.Lee, W. Gyu La, and H. Kim, "Drone Detection and Identification System using Artificial Intelligence," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2018, pp.1131-1133.

[7] N.Siriphun, S. Kashihara, D. Fall, and A. Khurat, "Distinguishing Drone Types Based on Acoustic Wave by IoT Device," in *2018 22nd International Computer Science and Engineering Conference（ICSEC）*, Nov.

[8] N.Molina, F. Cabrera, V. Araa, M. Tichavska, B. P. Dorta, and J. A. Godoy, "A Wireless Method for Drone Identification and Monitoring Using AIS Technology," in *2018 2nd URSI Atlantic Radio Science Meeting（AT-RASC）*, May 2018, pp.

[9] M.Balduzzi, K. Wilhoit, and A. Pasta, in *A Security Evaluation of AIS*, Trend Micro Incorporated, 2014.

[10] Marcus Janke, Dr. Peter Laakmann, in *Attacks on Embedded Devices*, Embedded World Conference Nurenberg, 2016.

[11] R.E. Dierks T., "传输层安全（TLS）协议版本 1.2，"互联网征求意见稿，RFC编辑，RFC 5246，2008年8月。[在线]。见：https://tools.ietf.org/html/rfc5246

[12] L.Qi 等人，"A Secure End-to-End Cloud Computing Solution for Emergency Management with UAVs," 2018年12月。

[13] 托马斯-菲舍尔，*设计和实现一个带有BLE和NFC的安全个人助理设备*。格拉茨理工大学，2016年。

[14] 因斯布鲁克管理中心，"Infineon Multi- copter Demoboard的维基"，https://github.com/ManagementCenterInnsbruck/Multicopter-LARIX/wiki，[在线；2019-08-26访问]。

[15] Sixfab, "Raspberry Pi Iot Shields Sources," https://github.com/sixfab/Sixfab_RPi_3G-4G-LTE_Base_Shield, [Online; accessed 2019-07-30].

[16] B.C.和H.P.，"简明二进制对象表示法（CBOR）"，互联网征求意见，RFC编辑器，RFC