Journal of Computer Applications
计算机应用,2020,40(8):2286 - 2292
ISSN 1001-9081
CODEN JYIIDU
2020-08-10
http://www.joca.cn

文章编号:1001-9081(2020)08-2286-07
DOI:10.11772/j.issn.1001-9081.2019122160

基于MAVLink协议的无人机系统安全通信方案

张凌浩[1],王　胜[1],周　辉[2],陈一凡[3],桂盛霖[3*]
(1. 国网四川省电力公司 电力科学研究院,成都 610000; 2. 国网四川省电力公司 检修公司,成都 610041;
3. 电子科技大学 计算机科学与工程学院,成都 611731)
(*通信作者电子邮箱 shenglin_gui@uestc.edu.cn)

摘　要:MAVLink是一种应用于无人机(UAV)与地面站(GCS)之间的轻量级通信协议,它定义了一组包括UAV状态和GCS控制命令的UAV与GCS交互的双向消息。针对MAVLink协议缺乏足够的安全机制,存在可能导致严重威胁和隐患的安全漏洞的问题,提出了一种基于MAVLink协议的UAV系统安全通信方案。首先,UAV持续交替广播连接请求。然后,GCS向UAV发送公钥,双方利用DH算法进行密钥协商计算出共享密钥,并使用AES算法对MAVLink消息包进行加密通信,完成身份认证;若UAV在规定时间内未收到GCS发送的公钥或对MAVLink消息包解密错误则主动断开连接,更新公钥后重新广播连接请求。另外,针对UAV系统存在被恶意篡改的安全问题,在启动引导时对UAV系统固件进行了自校验。最后,基于形式化验证工具UPPAAL证明了所提方案具有活性、可连接性以及连接唯一性,并对UAV PX4 1.6.0与GCSQgroundControl3.5.0的通信过程进行抓包测试。结果表明,所提的UAV系统安全通信方案能够防止在UAV与GCS通信过程中存在的恶意窃听、篡改消息、中间人攻击等恶意攻击,并且对UAV性能影响较小,较好地解决了MAVLink协议存在的安全漏洞。

关键词:无人机;安全功能;安全通信;自校验;形式化验证
中图分类号:TP311.5　　**文献标志码**:A

Secure communication scheme of unmanned aerial vehicle system based on MAVLink protocol

ZHANG Linghao[1], WANG Sheng[1], ZHOU Hui[2], CHEN Yifan[3], GUI Shenglin[3*]
(1. *Electric Power Research Institute, State Grid Sichuan Electric Power Company, Chengdu Sichuan* 610000, *China*;
2. *Maintenance Company, State Grid Sichuan Electric Power Company, Chengdu Sichuan* 610041, *China*;
3. *School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan* 611731, *China*)

Abstract: The MAVLink is a lightweight communication protocol between Unmanned Aerial Vehicle (UAV) and Ground Control Station (GCS). It defines a set of mutual bi-directional messages between UAV and GCS, including UAV states and GCS control commands. However, the MAVLink protocol lacks sufficient security mechanisms, and there are security vulnerabilities that may cause serious threats and hidden dangers. To resolve these problems, a security communication scheme for the UAV system based on the MAVLink protocol was proposed. First, the connection requests were broadcasted by the UAV constantly and alternately; then the public key was sent to the UAV by the GSC, and the DH algorithm was used by both sides to negotiate a shared key, and the AES algorithm was used to encrypt the communication on MAVLink message packages, achieving identity authentication. If the UAV did not receive the public key sent by the GCS within the specified time or a decryption error on MAVLink message package happened, the UAV would actively disconnect and update a new public key to rebroadcast the connection request. In addition, concerning the security problem of the UAV system being maliciously tampered with, the system firmware was self-checked during booting. Finally, based on the formal verification platform UPPAAL, it has been proved that the proposed scheme has the security properties of liveness, connectability and connection uniqueness. Results of the communication process between UAV PX4 1.6.0 and GCS QgroundControl 3.5.0 show that the proposed secure communication scheme of UAV system can prevent malicious eavesdropping, message tampering, man in the middle attack and other malicious attacks in the communication process between UAV and GCS, and solve the security vulnerabilities of MAVLink protocol well with little effect on UAV performance.

Key words: Unmanned Aerial Vehicle (UAV); security function; secure communication; self-checking; formal verification

收稿日期:2019-12-24;**修回日期**:2020-02-25;**录用日期**:2020-03-11。　**基金项目**:国网四川省电力公司科技资助项目(521997170017)。
作者简介:张凌浩(1985—),男,山东威海人,工程师,博士,主要研究方向:电力信息安全; 王胜(1987—),男,四川达州人,工程师,硕士,主要研究方向:网络安全; 周辉(1985—),男,四川遂宁人,工程师,主要研究方向:网络安全; 陈一凡(1996—),男,福建泉州人,硕士研究生,主要研究方向:嵌入式软件; 桂盛霖(1983—),男,重庆人,副教授,博士,CCF会员,主要研究方向:嵌入式软件、信息安全。

0　引言

随着科学技术的发展,无人机(Unmanned Aerial Vehicle, UAV)已经成为一项新兴技术,在多个行业获得了广泛应用,如智能城市、边境监视、自然灾害监控[1]、实时物体跟踪[2]和货物运输[3-4]等。UAV[5]在飞行时可以被地面控制站(Ground Control Station, GCS)进行远程控制,也可以通过预先编程的任务进行自动控制。当受到远程控制时,UAV和GCS之间需通过通信协议进行通信。微型飞行器链路(Micro Air Vehicle Link, MAVLink)协议[6]是一种灵活、轻量级的开源通信协议,被Ardupilot、PX4等多个无人机系统作为无人机与地面站之间的通信协议,实现无人机和地面站之间的双向数据交换。

但是,MAVLink协议没有引入足够的安全机制,且未使用任何加密算法,因此容易受到包括窃听、消息伪造和中间人攻击等多种恶意攻击[7-8]。为了保证MAVLink协议的通信安全,研究者们提出了一些通信安全方案,如使用凯撒密码[9]对无人机与地面站的之间的通信数据进行加密,但是,已有文献较多关注通信内容加密,缺乏系统性安全增强机制,具有较大的局限性。因此,本文基于MAVLink协议,提出了一种无人机系统安全通信方案,不仅解决了MAVLink协议的安全性以防止窃听拦截之类的攻击,同时增加了无人机和地面站的身份认证机制防止中间人的恶意攻击。本文的方案模型在形式化验证工具UPPAAL平台上经过形式化验证,证明它具有活性、可连接性及连接唯一性,并且在PX4 1.6.0与地面站QgroundControl 3.5.0平台上进行了开发和实现。

1　相关工作

无人机的现有安全防护措施主要包括传感器安全、软件安全、通信安全三个方面[10]。

传感器是无人机系统探测自身及周围环境数据的重要组成部分。目前,针对无人机传感器的攻击形式主要是全球定位系统(Global Positioning System, GPS)欺骗。文献[11-13]中通过使用一种GPS信号自动增益控制来检测是否接收到GPS欺骗信号;而文献[14]中则通过判断信号强度和噪声值来检测GPS欺骗。针对飞控软件是否受到了恶意代码的入侵,文献[15-16]中采用机器学习技术通过处理软件的特征码以及软件行为的数据,依据该信息得出该软件是否为恶意软件的结论。在通信安全方面,无人机和地面站之间的通信存在中间人攻击、窃听、伪造等安全威胁,而现有文献的工作大多集中在对通信内容进行加密,如文献[17]中介绍了一种无人机与传感器等智能实体通信的协议,使用了证书签名机制对通信内容进行加密;文献[18]中使用加密机制RC5来保护MAVLink通信协议;文献[19]中对MAVLink协议进行了漏洞分析,使用了多种加密算法来保护MAVLink身份协议的通信内容。而对于无人机与地面站的认证机制仅有少量论文进行研究,如文献[20]中使用DH(Diffie-Hellman)密钥交换/协议对无人机与地面站进行身份认证,但是并未对其进行形式化证明。本文对该方案使用UPPAAL进行形式化建模和验证,发现存在认证漏洞的可达性路径(见第4章)。

基于上述分析,目前缺乏对MAVLink协议的系统性安全机制的研究,如文献[17-18]中没有对与无人机交互的实体作身份认证;文献[19]中仅提供协议的描述,没有给出测试和实现的特定细节。因此,本文基于MAVLink 2.0通信协议设计了无人机系统的一种安全通信方案,其中在建立连接阶段取消了MAVLink 2.0中无人机无安全保证的确认连接操作,并新增了密钥协商机制生成共享密钥,双方使用加密的MAVLink 2.0消息包进行通信并完成身份认证。为了防止系统固件被恶意篡改,还对无人机系统固件进行了引导时自校验。最后经过形式化建模,证明了本文改进后的无人机系统安全通信方案能够保证无人机系统的活性、可连接性以及认证唯一性。

2　基于DH算法的MAVLink协议

2.1　MAVLink协议

MAVLink是一种开源、轻量级且仅包含标头的协议,常用于GCS和UAV之间的双向通信。MAVLink 1.0于2009年初由Lorenz Meier以宽通用公共许可证(Lesser General Public License, LGPL)首次发布[21]。MAVLink 2.0协议[22]于2017年初发布,是当前最新的版本,它与MAVLink 1.0版本向后兼容,并在MAVLink 1.0版本的基础上进行了多项改进。

图1给出了MAVLink 2.0消息包的结构,每个MAVLink 2.0消息包都包含头部信息、内容信息和校验信息,具体字段包括:数据包开始标记字段(packet Start Sign, STX)、有效负载长度字段(payload LENgth, LEN)、不兼容标志字段(INCompat FLAGS, INC FLAGS)、兼容标志字段(CoMPat FLAGS, CMP FLAGS)、数据包序列号字段(packet SEQuence, SEQ)、系统ID字段(SYStem ID, SYS ID)、组件ID字段(COMPonent ID, COMP ID)、消息ID字段(MeSsaGe ID, MSG ID)、校验和字段(CHECKSUM)、签名(SIGNATURE)和有效负载字段(PAYLOAD)。其中PAYLOAD大小是可变的,其长度取决于在通信期间发送或接收的参数,最大长度为255 B。MAVLink 2.0消息类型由消息包上的MSG ID字段标识,并且PAYLOAD字段依据MSG ID产生不同的内容。其中,MSG ID字段为0X00的消息包为心跳包(Heartbeat)。请求连接时,无人机会首先向地面站发送心跳包请求连接,若地面站收到该请求,则发送对应的控制命令确认连接。此后,无人机定期(通常每秒)向地面站发送心跳包,以提供其状态的反馈(指示无人机处于活动状态且仍处于连接状态)。图2给出了MAVLink 2.0中无人机和地面站的连接过程。

STX (1 B)	LEN (1 B)	INC FLAGS (1 B)	CMO FLAGS (1 B)	SEQ (1 B)	SYS ID (1 B)	COMP ID (1 B)	MSG ID (3 B)	PAYLOAD (0~255 B)	CHECKSUM (2 B)	SIGNATURE (13 B)

图1　MAVLink 2.0的消息包结构

Fig. 1　Message package structure of MAVLink 2.0

事实上,由于MAVLink 2.0协议并没有提供足够的安全机制来保护通信数据,也没有身份认证机制,因此只要使用匹配的无线数传硬件,任何第三方地面站都可以与无人机通信并将命令注入到现有会话中,无人机系统很容易被黑客入侵和控制,存在较大的安全风险。

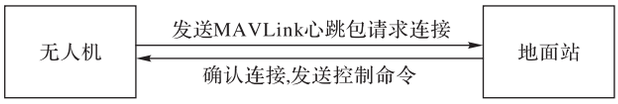


图2　MAVLink 2.0中无人机和地面站的连接过程

Fig. 2　Connection process between UAV and GCS in MAVLink 2.0

2.2 基于MAVLink的无人机系统安全通信方案

针对基本的MAVLink 2.0中的安全问题，本文方案至少要达到以下三个目标：

1）无人机以密文形式传输消息，防止恶意窃听及篡改消息；

2）无人机和地面站进行身份认证，防止恶意中间人攻击；

3）对协议的通信过程需建立形式化模型，证明其安全性质。

在基本MAVLink 2.0协议的基础上引入了高级加密标准（Advanced Encryption Standard，AES）算法和DH算法，其中：AES加密算法保证了无人机以密文形式传输消息，防止了恶意窃听和篡改消息；DH算法则实现了无人机和地面站的密钥协商和身份认证。

本文设计的无人机系统安全通信方案可分为四个阶段：

1）无人机请求连接；

2）无人机和地面站密钥协商与身份认证；

3）无人机与地面站加密通信；

4）无人机与地面站断开连接。

图3给出了无人机和地面站的上述4个交互阶段。定义1给出了描述无人机或地面站在交互过程中状态变化的六元组的定义。

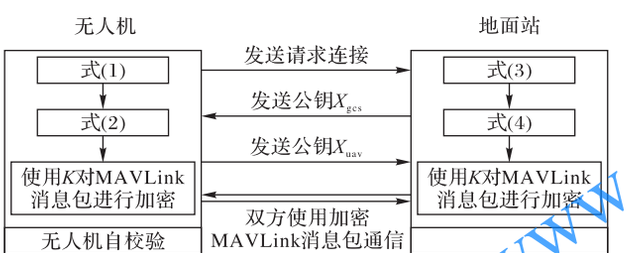


图3 无人机与地面站交互过程

Fig. 3 Interaction process between UAV and GCS

定义1 通信实体状态可由一个六元组$\langle L, L_0, A, C, I, E\rangle$表示。其中：$L$表示有穷位置集；$L_0$表示初始位置，$L_0 \in L$；$A$表示有穷事件集，其中$a?(a \in A)$表示接收了一个来自其他实体的事件，$a!(a \in A)$表示向其他实体发出了一个事件；$C$表示时钟变量集；$I$：$L \to B(C)$表示一个映射，用于为$L$中的每个元素指定一个时间约束，其中，时钟约束集$B(C)$是形如{$c0 \sim n$或$c1 - c2 \sim n$, $c0, c1, c2 \in C, n \in N, \sim \in \{<, <=, =, >=, >\}$的不等式集合；$E \subseteq L \times A \times B(C) \times 2^C \times L$，表示边集，边$(l, a, b, R, l') \in E$表示满足事件$a$和时钟约束$b$时，从位置$l$迁移到位置$l'$，同时时钟集合$R$中的时钟变量被重置。

2.2.1 无人机请求连接阶段

在连接请求阶段，无人机持续交替广播MAVLink 2.0心跳包与公钥包X_{uav}，请求与地面站连接，其中心跳包格式与MAVLink 2.0中定义的一致，公钥包的MSG ID为3，并将公钥X_{uav}填充至其有效负载字段。图4给出了无人机与地面站在请求连接阶段的六元组$\langle L_{uav}, L_0, A, C_{uav}, I_{uav}, E_{uav}\rangle$和$\langle L_{gcs}, L_0, A, C_{gcs}, I_{gcs}, E_{gcs}\rangle$描述，其中两个六元组共享同一事件集$A$。

在无人机端，无人机初始化后进入idle空闲位置（idle $\in L_{uav}$）并交替发送心跳包与公钥包X_{uav}（将其记为原子事件“request!”(request $\in A$)），然后进入wait_public_key位置（wait_public_key $\in L_{uav}$）等待接收地面站的公钥包X_{gcs}，同时将时钟变量$c1$清零。在该位置上，最多只能停留5个时钟单位（记为不变式“$c1 <= 5$”($c1 \in C_{uav}$)）。若未在5个时钟单位内收到地面站的公钥包X_{gcs}则返回idle位置。在地面站端，若收到无人机发送的心跳包或公钥包X_{uav}，则进入parse_request位置（parse_request $\in L_{gcs}$）。

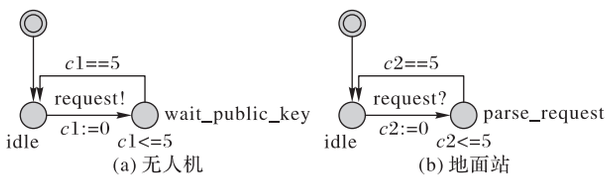


图4 无人机和地面站在请求连接阶段的状态变化关系

Fig. 4 State transition relationship between UAV and GCS in stage of requesting connection

2.2.2 无人机和地面站密钥协商与身份认证阶段

本文设计的方案和基本的MAVLink 2.0协议相比，还增加了密钥协商与身份认证过程。无人机发起请求连接后，若在5个时钟单位内收到地面站发送的公钥X_{gcs}，则通过式(1)、(2)计算共享密钥K。

$$Y_{gcs} = a^{X}_{gcs} \bmod q \tag{1}$$

$$K = (Y_{gcs})^{X}_{uav} \bmod q \tag{2}$$

式中：a、q为无人机和地面站预先协商的共同参数。在地面站端，收到无人机发送的公钥X_{uav}后通过式(3)、(4)计算共享密钥K。

$$Y_{uav} = a^{X}_{uav} \bmod q \tag{3}$$

$$K = (Y_{uav})^{X}_{gcs} \bmod q \tag{4}$$

通过密钥协商，无人机和地面站生成了安全的共享密钥K。在此后的一轮通信中，无人机和地面站使用AES算法对MAVLink 2.0消息包中的PAYLOAD字段进行加密。

若无人机收到地面站发送的加密MAVLink 2.0消息包对其PAYLOAD字段解析错误，则地面站未通过身份认证，无人机与其断开连接；若对加密的MAVLink 2.0消息包解析正确，则双方身份认证成功，可继续通信。图5给出了无人机与地面站在密钥协商与身份认证阶段的六元组描述。

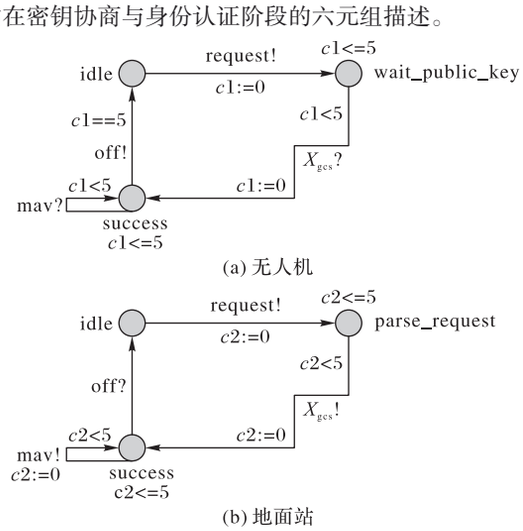


图5 无人机和地面站在密钥协商和身份认证阶段的状态变化关系

Fig. 5 State transition relationship between UAV and GCS during stage of key negotiation and identity authentication

本阶段开始时,无人机处于wait_public_key位置,若在5个时钟单位内收到地面站发送的公钥包X_{gcs}(记为事件"X_{gcs}? "($X_{gcs} \in A$))后进入位置success (success $\in L_{uav}$)表示成功收到公钥包X_{gcs}。该位置中,若收到地面站使用共享密钥K加密的任何MAVLink 2.0消息包(记为事件"mav? "(mav $\in A$))则表示身份认证成功继续保持通信,否则到达5个时钟单位后断开连接进入idle位置重新发起新的会话(记为事件"off!"(off $\in A$))。在地面站端,地面站在本阶段开始前已经处于parse_request位置,向无人机发送公钥包X_{gcs}(记为事件"X_{gcs}! ")进入success位置表示密钥协商成功。该位置中,地面站使用共享密钥K加密任何要发送的MAVLink 2.0消息包(记为事件"mav!")。

2.2.3　无人机与地面站加密通信

无人机与地面站使用共享密钥K对MAVLink消息包加密通信。若收到恶意攻击者发来伪造的MAVlink 2.0消息包导致解密失败,则无人机断开连接。在断开连接之后,若无人机和地面站需要建立新的连接,则动态更新X_{uav}和X_{gcs}重新生成新的共享密钥K,进一步保证了密钥的安全性。此外,为了保持连接状态,无人机定期向地面站发送心跳包,对其中的PAYLOAD字段进行加密。

本文所提出的无人机系统安全通信方案继续保留了MAVLink 2.0的以下安全机制:

1)时间戳机制:自2015年1月1日格林威治标准时间以来,时间戳以10 μs为单位。对于特定连接上的每个消息,时间戳必须单调增加。注意,这意味着如果数据包速率平均每秒超过100 000个数据包,则时间戳可能会超过实际时间。

2)重传机制:MAVLink 2.0协议在发送端启动一个定时器,如果在特定的时间内没有收到响应,则请求的消息会被重新发送一次。该重传过程会重复数次,如果在最后一次的重传超时后仍然没有收到响应,则认定该消息发送失败。

3)丢包机制:在发送端,MAVLink 2.0消息包中的SEQ字段在每次发送消息包后都会递增,以此检测是否丢包。

2.2.4　无人机和地面站断开连接

无人机与地面站满足以下条件之一时断开连接:

1)在无人机和地面站进行通信过程中,若对地面站发送的加密MAVLink消息包解析错误,则主动断开连接并进入idle位置(记为事件"off!");

2)无人机或地面站主动发送MSG ID为5的消息包,则断开连接。

3　无人机自校验

为保证无人机系统不被篡改,本文还设计了引导时的自校验机制,并在PX4 1.6.0系统进行开发,实现PX4系统在上电初始化后进行Hash校验,若校验成功,系统正常运行;否则,系统停止加载并退出。该机制的实现过程如下:

1)原px4src_1.6.0\Firmware\Tools\px_uploader.py文件中的def __program(self, label, fw)函数中定义了变量size记录固件的大小,因此本文在此函数中新增根据PX4系统固件的起始地址(BootLoader_v2在配置文件BootLoader_v2/hw_config.h中定义起始地址为0x08004004)计算终止地址为0x08004004+size-4。

2)在Bootloader_v2根目录中新增md5.c与md5.h文件,实现了MD5(Message-Digest Algorithm 5)算法[23]用于计算PX4系统固件Hash值。本文使用PX4系统固件作为MD5算法的输入参数并计算出Hash值,存储在Bootloader_v2\bl.c文件下hash_data[n]数组中。

3)原Bootloader_v2\bl.c文件中包含了初始化硬件的各类函数,本文在该文件中新增了函数GetFlashMD5(unsigned char decrypt[], int n),用于在PX4上电初始化完成后调用md5.c文件中实现的MD5算法完成对PX4系统固件的Hash值计算并与预先存储的Hash值hash_data[n]进行比较,若检验正确,系统正常运行;否则,系统停止加载并退出。

4　形式化证明与测试

4.1　形式化证明

本文使用由瑞典Uppsala大学和丹麦Aalborg大学联合开发的形式化工具UPPAAL对无人机系统安全通信方案进行了形式化证明。该工具由模型编辑器、模拟器和验证器三部分组成。其中:系统编辑器用于对待验证实体进行建模;模拟器用于检查所建立的模型是否存在错误;验证器用于验证模型是否满足计算树逻辑(Computation Tree Logic, CTL)公式描述的性质。另外,UPPAAL使用位置集(L)、初始位置(L_0)、事件集(A)、时钟变量集(C)、不变式(I)、边集(E)六元组来描述通信实体状态,并为属性描述提供了简化版的计算树逻辑(CTL)公式,它由路径公式和状态公式两部分组成,前者量化模型的路径或轨迹,而后者则描述单独的状态。此外,UPPAAL还提供了"deadlock"关键词用来描述死锁状态。

为验证文献[19]中所提出的安全通信协议存在认证漏洞,本文基于UPPAAL工具对文献[19]中的技术方案在存在恶意中间人攻击的场景中进行了形式化建模,如图6所示,其中:图(a)给出了无人机(UAV)的状态变化模型,图(b)和(c)分别给出了恶意中间人地面站(Malice Ground Control Station, GCS_M)和正常地面站(GCS)的状态变化模型。注意,图6(b)的恶意中间人地面站伪装成一个正常地面站,因此具有与正常地面站相同的状态变化模型。但是,在实际攻击场景中,恶意攻击地面站可能采用不同精心设计的攻击策略。

攻击场景:文献[19]中身份认证过程中存在某一时刻,GCS与UAV已经建立连接并等待身份认证时,GCS_M抢先发送公钥X_{gcs_m}与UAV完成身份认证并实现控制UAV,导致与UAV已经建立连接关系的GCS失去对UAV的控制权。该过程可由式(5)表示:

$$E<>\ UAV.\ connected\ and\ GCS\_M.\ success\ and\ GCS.\ connected \tag{5}$$

对图6和式(5)进行形式化验证,结果显示该性质成立,因此存在认证漏洞的可达路径。而本文设计的方案在UPPAAL中进行形式化建模后如图7所示,其中:图(a)给出了无人机(UAV)的状态变化模型,图(b)和(c)给出了恶意中间人地面站(GC1S_M)和正常地面站(GCS)的状态变化模型。

本文使用了三个关键安全属性,使用计算树逻辑(CTL)公式表示如下:

1)活性。

在本文方案中,若UAV和GCS在某个通信时刻进入了死锁状态,则表示整个协议是无法正常运行的。因此,系统的活性是基本性质之一。在UPPAAL中,式(6)描述了系统的活性。经验证,本文方案满足该性质。

A[ ] not deadlock (6)

2)可连接性。

UAV 和 GCS 身份认证过程中,双方必须能够在一定时间周期内成功连接。式(7)描述了可连接性。经验证,本文方案满足该性质。

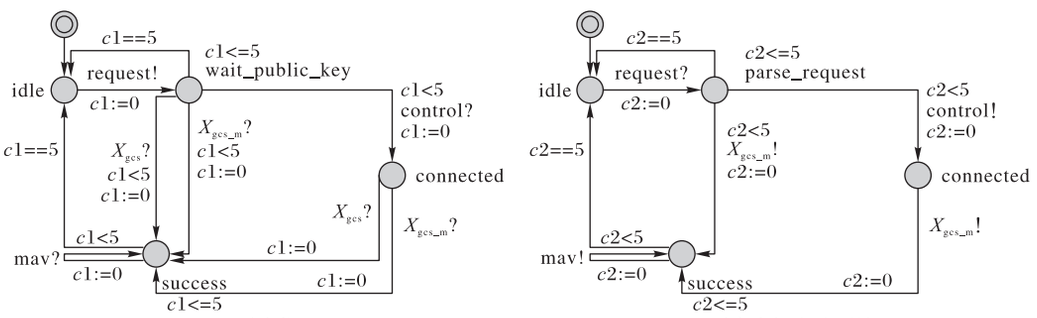
E<> UAV. success and GCS. success (7)

3)连接唯一性。

在 UAV 和 GCS 连接到身份认证成功期间,若存在某一时刻 GCS_M 同时也能够与 UAV 连接或进行身份认证,式(8)给出了连接唯一性的表示。

E<> UAV. success and GCS. success and
GCS_M. success (8)

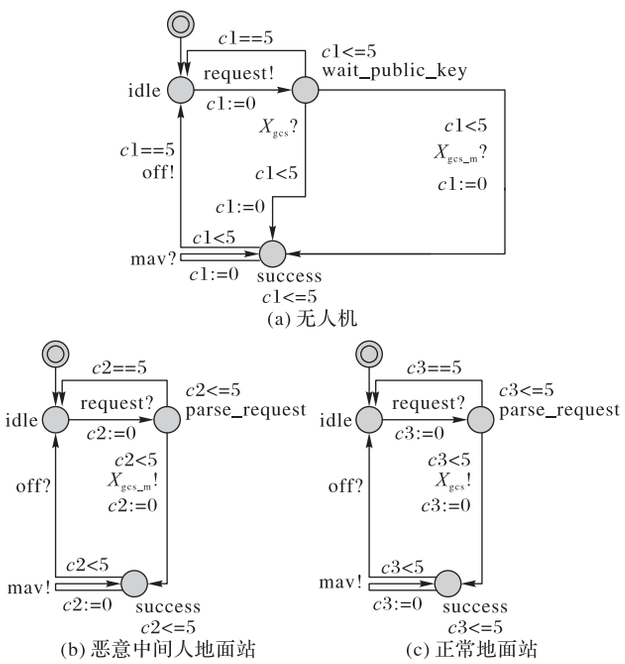
式(8)在 UPPAAL 中验证不满足,因此本文的无人机系统安全通信方案不存在文献[20]中认证漏洞的可达性,防止了恶意中间人的攻击。表 1 给出了本文无人机系统安全通信方案的安全机制。



(a) 无人机 (b)恶意中间人地面站 (c)正常地面站

图 6 文献[19]的状态变化模型

Fig. 6 State transition model of literature [19]



(a) 无人机 (b) 恶意中间人地面站 (c) 正常地面站

图 7 本文方案的状态变化模型

Fig. 7 State transition model of the proposed scheme

4.2 抓包测试

本文所使用的开发与测试平台为无人机 PX4 1.6.0 与地面站 QgroundControl 3.5.0,其中,QGroundControl 地面站是由 Lorenz Meier 开发并用 C++编写的开源地面控制站(GCS)软件应用程序。本文按照 2.2 节中定义的 4 个阶段修改了 MAVLink 2.0 的相关源代码,并按第 3 章的实现过程在 BootLoader_v2 中增加了无人机系统固件进行引导时自校验功能,最后重新编译了 QgroundControl 3.5.0、PX4 1.6.0 以及 BootLoader_v2 的源代码,形成了 qgroundcontrol-start. sh、px4fmuv2_bl. bin 与 px4fmuv2. px4 可执行文件。

本节使用 Bus Hound 抓包工具在 Ubuntu16.04 对 PX4 1.6.0 和 QgroundControl 3.5.0 通信时进行了抓包分析,以说明开发的有效性。表 2、3 给出了 PX4 1.6.0 与 QgroundControl 3.5.0 在各个阶段抓取的部分 MAVLink 消息包内容,说明本文基于 MAVLink 的无人机系统安全通信方案具有防篡改、防窃听的安全性质

表 2、3 分别给出了 PX4 1.6.0 与 QgroundControl 3.5.0 在 MAVLink 协议改进前后的消息包内容。在加密通信阶段,控制命令原始消息包 PAYLOAD 为 0f 38 97 c6 e3 d1 59 7f 75 b8 89 48 0b 8a 95 71,通过加密后得到的有效负载为 6a 49 67 03 7f 73 a6 10 3a 91 8a 17 a5 89 e6 92,有效防止了恶意中间人的窃听,并且和 MAVLink 中的校验字段结合可有效防止恶意中间人的篡改。

表 4 测试了改进前后加密通信阶段 PX4 1.6.0 与 QgroundControl 3.5.0 在相同时间内传输消息包的数量,说明

了改进后无人机与地面站传输的消息包有少量减少，此方案对无人机性能开销影响较小。

表1　无人机系统安全通信方案的安全机制

Tab. 1　Security mechanisms of UAV system secure communication scheme

安全性质	性质表示	UPPAAL结果	安全功能
安全性	A[ ] not deadlock	通过	保证协议正常运行
可连接性	E<> MAV. success and GCS. success	通过	保证无人机和地面站可正常连接
认证唯一性（防中间人攻击）	A[ ] not GCS. success and GCS_M. success	通过	防止身份认证过程中的恶意中间人攻击
防篡改	—	—	由加密通信机制实现
防窃听	—	—	由加密通信机制实现

表2　改进前各阶段MAVLink消息包内容

Tab. 2　Contents of original MAVLink message packages in different stages

阶段	无人机（改进前）	地面站（改进前）
建立连接	心跳包编码：fd 09 00 00 01 01 01 00 00 00 00 00 01 00 02 0c 51 00 03 35 6b	控制命令编码：fd 21 00 00 03 01 01 00 00 4c 00 00 80 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a1 d1
通信	状态包编码：fd 02 00 00 1c 01 01 00 00 f5 00 00 f7 40	控制命令编码：fd 10 00 00 0a 01 01 00 00 2f 0f 38 97 c6 e3 d1 59 7f 75 b8 89 48 0b 8a 95 71 2b 75

表3　改进后各阶段MAVLink消息包内容

Tab. 3　Contents of improved MAVLink message packages in different stages

阶段	无人机（改进后）	地面站（改进后）
请求连接	心跳包编码：fd 09 00 00 01 01 01 00 00 00 00 00 01 00 02 0c 51 00 03 35 6b 公钥 X_{uav} 消息包编码：fd 10 00 00 06 01 01 00 00 03 0a 0c 01 07 05 0d 0f 02 03 03 31 0b 19 00 03 06 09 b7	—
密钥协商	—	公钥 X_{gcs} 消息包编码：fd 10 00 00 03 01 01 00 00 03 2c 03 19 00 01 1e 0a 0d 03 06 11 09 08 00 03 00 06 0e
加密通信	状态包编码：fd 10 00 00 1c 01 01 00 00 f5 1a 0c 3d 0a 18 13 06 21 6a 3c 5d 11 6c c1 a1 01 c3 9b	控制命令编码：fd 10 00 00 0a 01 01 00 00 2f 6a 49 67 03 7f 73 a6 10 3a 91 8a 17 a5 89 e6 92 03 ce

表4　加密通信阶段消息包传输数量

Tab. 4　Number of transmitted message packets in encrypted communication stage

时间/s	消息包传输数量		时间/s	消息包传输数量	
	改进前	改进后		改进前	改进后
10	1 631	1 569	70	8 637	8 560
30	4 628	4 531	90	11 207	10 915
50	6 313	6 251			

5　结语

本文针对MAVLink 2.0协议存在的安全漏洞，设计并实现了一种基于MAVLink协议的无人机系统安全通信方案。无人机首先广播连接请求，然后使用DH算法与地面站进行密钥协商及身份认证，并使用AES算法对MAVLink消息包进行加密传输。此外，无人机与地面站断开连接后会动态更新公钥。经过形式化证明和抓包测试，结果表明本文提出的方案能够防止无人机与地面站通信过程中潜在的恶意窃听、消息篡改等攻击，并且与文献[20]中的技术方案相比，本文方案避免了MAVLink协议存在中间人攻击等安全漏洞，未来还会针对本文方案作进一步完善。

参考文献（References）

[1] BENJDIRA B, KHURSHEED T, KOUBAA A, et al. Car detection using unmanned aerial vehicles: comparison between faster R-CNN and YOLOv3[C]// Proceedings of the 1st International Conference on Unmanned Vehicle Systems-Oman. Piscataway: IEEE, 2019: 1-6.

[2] KOUBÂA A, QURESHI B. DroneTrack: cloud-based real-time object tracking using unmanned aerial vehicles over the internet[J]. IEEE Access, 2018, 6: 13810-13824.

[3] PAJARES G. Overview and current status of remote sensing applications based on Unmanned Aerial Vehicles (UAVs)[J]. Photogrammetric Engineering and Remote Sensing, 2015, 81(4): 281-329.

[4] HAYAT S, YANMAZ E, MUZAFFAR R. Survey on unmanned aerial vehicle networks for civil applications: a communications viewpoint[J]. IEEE Communications Surveys and Tutorials, 2016, 18(4): 2624-2661.

[5] 刘炜，冯丙文，翁健. 小型无人机安全研究综述[J]. 网络与信息安全学报，2016, 2(3): 39-45. (LIU W, FENG B W, WENG J. Survey on research of mini-drones security[J]. Journal of Network and Information Security, 2016, 2(3):39-45.)

[6] LI J, ZHOU Y, LAMONT L. Communication architectures and protocols for networking unmanned aerial vehicles[C]// Proceedings of the 2013 IEEE Globecom Workshops. Piscataway: IEEE, 2013: 1415-1420.

[7] KOUBÂA A, QURESHI B, SRITI M F, et al. Dronemap planner: a service-oriented cloud-based management system for the internet-of-drones[J]. Ad Hoc Networks, 2019, 86: 46-62.

[8] KWON Y M, YU J, CHO B M, et al. Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles[J]. IEEE Access, 2018, 6: 43203-43212.

[9] RAJATHA B S, ANANDA C M, NAGARAJ S. Authentication of

MAV communication using Caesar cipher cryptography [C]// Proceedings of the 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials. Piscataway: IEEE, 2015: 58-63.

[10] 何道敬,杜晓,乔银荣,等. 无人机信息安全研究综述[J]. 计算机学报, 2019, 42(5):1076-1094. (HE D J, DU X, QIAO Y R, et al. A survey on cyber security of unmanned aerial vehicles[J]. Chines Journal of Computers, 2019, 42(5):1076-1094.)

[11] AKOS D M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via Automatic Gain Control (AGC)[J]. Navigation: Journal of the Institute of Navigation, 2012, 59(4): 281-290.

[12] BASTIDE F, AKOS D, MACABIAU C, et al. Automatic Gain Control (AGC) as an interference assessment tool [C]// Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation. Manassas, VA: Institute of Navigation, 2003: 2042-2053.

[13] WARNER J S, JOHNSTON R G. GPS spoofing countermeasures [J]. Homeland Security Journal, 2003, 25(2): 19-27.

[14] JAHROMI A J, BROUMANDAN A, NIELSEN J, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements [J]. International Journal of Satellite Communications and Networking, 2012, 30(4): 181-191.

[15] SCHMIDT A D, BYE R, SCHMIDT H G, et al. Static analysis of executables for collaborative malware detection on android [C]// Proceedings of the 2009 IEEE International Conference on Communications. Piscataway: IEEE, 2009: 1-5.

[16] SHABTAI A. Malware detection on mobile devices [C]// Proceedings of the 11th International Conference on Mobile Data Management. Piscataway: IEEE, 2010: 289-290.

[17] WON J, SEO S H, BERTINO E. A secure communication protocol for drones and smart objects[C]// Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2015: 249-260.

[18] BUTCHER N, STEWART A, BIAZ S. Securing the MAVLink communication protocol for unmanned aircraft systems [EB/OL]. [2020-03-13]. https://pdfs. semanticscholar. org/4ce0/68b40089549f3d445d30e45fe8b53a141c88. pdf.

[19] MARTY J A. Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft [EB/OL]. (2014-03-14) [2019-11-05]. https://scholar. afit. edu/cgi/viewcontent. cgi?article=1613&context=etd.

[20] PRAPULLA N, VEENA S, SRINIVASALU G. Development of algorithms for MAV security [C]// Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology. Piscataway: IEEE, 2016: 799-802.

[21] ATOEV S, KWON K R, LEE S H, et al. Data analysis of the MAVLink communication protocol [C]// Proceedings of the 2017 International Conference on Information Science and Communications Technologies. Piscataway: IEEE, 2017: 1-3.

[22] ANDREW TRIDGELL M L. Some proposals for MAVlink 2.0 [EB/OL]. [2019-11-12]. https://docs. google. com/document/d/1XtbD0ORNkhZ8eKrsbSIZNLyg9sFRXMXbsR2mp37KbIg/edit#heading=h. ovqxr52ozscu.

[23] RACHMAWATI D, TARIGAN J T, GINTING A B C. A comparative study of Message Digest 5 (MD5) and SHA256 algorithm [J]. Journal of Physics: Conference Series, 2018, 978(1): No. 012116.

This work is partially supported by the Science and Technology Project of State Grid Sichuan Electric Power Company (521997170017).

ZHANG Linghao, born in 1985, Ph. D., engineer. His research interests include power information security.

WANG Sheng, born in 1987, M. S., engineer. His research interests include network security.

ZHOU Hui, born in 1985, engineer. His research interests include network security.

CHEN Yifan, born in 1996, M. S. candidate. His research interests include embedded software.

GUI Shenglin, born in 1983, Ph. D., associate professor. His research interests include embedded software, information security.