无人机遥测数据加解密方法的设计①

温 欣 王喜发 岳云天 (信息工程大学 电子技术学院 河南 郑州 450004；空军电子技术研究所 北京 100195)

摘 要： 针对无人机无线通信遥测数据帧的结构特点，以及传输实时性和高质量的需求，提出了基于自同步流密码的数据加解密方法。该方法具有加密强度高，错误扩散小，无信息扩散，实现简单等特点。经硬件 FPGA 实现，证明了该方法的可行性和可靠性。

关键词： 无人机; 遥测数据; 自同步流密码; 加解密; FPGA

Design of an Encryption Method of Telemetry Data in UAV System

WEN Xin, WANG Xi-Fa, YUE Yun-Tian

(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China; Air Force Electronics Technology Institute, Beijing 100195, China)

Abstract: Considering the structure characteristic of telemetry data frames of UAV wireless communication and the requirements of real time and high quality, this paper presents an encryption method based on self-synchronizing stream cipher. This encryption method is not only higly secure，but can also be easily realized with few error-spreading and no message-spreading. The realization of FPGA shows that the design of the scheme has higher feasibility and trustiness.

Keywords: UAV; telemetry data; self-synchronizing stream cipher; encryption and decryption; FPGA

无人机是一种由无线电遥控操纵或自主程序控制、无人驾驶的一种可重复使用的航空器。它具有结构简单，造价低廉，生存能力强，机动性好，能够完成有人驾驶飞机不能完成的任务等优点。无人机可用于气象探测、灾害监测、农药喷洒、地质勘测、地图测绘、交通管制、边境控制、情报侦察、校射、电子战、通信中继等各种场合[1]。

由于无人机飞行环境的复杂性和无线传输信息的开放性，在数据的下行链路传输过程中，遥测信息的传输会受到各种各样的干扰和破坏。遥测数据中含有大量的图像侦察信息，若没有任何安全措施保护这些信息很容易被第三方窃取。因此，为了保证无人机遥测数据信息的安全，我们必须采取相应的数据加密技术。

本文提出了适合无人机遥测数据帧特点的基于自同步流密码的数据加解密方法，该方法的使用确保了无人机的安全飞行，正常进行战略侦察，同时又不会向敌人泄露侦察信息和战略意图。经过硬件的实现，证明了该方法的可行性和可靠性。

1 序列密码加密原理

密码按加密形式分为序列密码和分组密码，分组密码用固定的变换处理明文序列的分组数据，加密较复杂，而且存在误码扩散和一定的延时，一般用于通信传输信道质量较好或具有数据重发等功能的场合；序列密码对明文序列逐位或逐块地加以随时间变化的变换。其硬件加密速度快，且实现容易，对信号加密具有低延时，无误码扩散等特点，因此序列密码在实际中得到广泛的应用[2]。

无人机系统通信对数据传输的实时性要求很高，例如地面控制站是每 20 ms 接收一帧的遥测数据,每 80 ms 发送一帧的遥控指令，所以必须采用具有低延时特性的序列密码加密方法。

根据序列密码的密钥序列与明、密文的关系，可将序列密码分为自同步序列密码和同步序列密码[3]。

① 收稿时间:2009-10-21;收到修改稿时间:2009-12-09

密钥序列与已经产生的一定数量的密文有关的序列密码被称为自同步序列密码，而密钥序列与明密文无关的序列密码被称为同步序列密码[4]。

采用同步序列密码加解密时，收发双方的密钥发生器必须同步，因此就需要精确的同步电路；如果在密文数据传输中丢失一个或若干字符，收发双方必须重新同步密钥发生器才能保持继续通信，同时也会造成错误扩散；此外，采用同步法时要保证密钥序列不能含有重复的部分，这样就导致了密钥规模过大。给密钥管理带来了一定的难度。

采用自同步序列密码加解密时，收发双方不需要精确的同步电路[5]，接收方的每个解密密钥都是由它前面的 n 个密文导出，如果在传输过程中丢失或改变了一个密文比特，将导致错误向后扩散 n 个分块，但在连续正确接收到 n 个密文后，系统又能自动的恢复同步．因此只要台理地选择 n 的大小，就能将错误扩散限制在容许的范围内。因此，本文提出了对无人机数据链路通信保密系统中的遥测帧使用自同步序列加密算法。

2　遥测数据加解密

无人机在数据终端系统中的链路层进行遥测数据的加密操作，使用面向位的链路控制协议，根据协议内容，无人机系统数据链路通信中的遥测数据帧的格式如图 1 所示。

标志段	数据段	帧校验段

图 1　遥测帧格式

遥测帧主要由标志段、数据段和帧校验段组成。标志段主要用于遥测帧的搜索捕获及帧的分离存储，数据段主要包括飞机的状态信息和图像数据信息，帧校验段采取 RS 码的校验方式。

2.1 加密实现

在无人机数据链路通信中使用的自同步加密算法中充分利用了遥测数据帧结构的特点，以帧长为单位更新初始密钥，以字长为分块单位进行序列加密．遥测数据经过信道编码后字长均为 m 比特 ，帧长为 N，约束长度取 n，其加密过程如图 2 所示。

在每帧数据开始时，先由初始密钥发生器产生初始密钥 $K_1,K_2,K_3,\cdots,K_n$，并与保密字 T_0 生成初始密文 C_0；同时该初始密钥控制密码发生器产生密码数据 Z_1；Z_1 与第一个明文字 M_1 模 2 加生成密文 C_1；C_1 与 T_1 模 2 加生成 R_1，R_1 与 $K_2,K_3,\cdots,K_n$ 构成新的 n 个密钥去控制密码发生器产生新的密码数据 Z_2 ;Z_2 与第二个明文字 M_2 模 2 加产生密文 C_2；C_2 与 T_2 模 2 加生成 R_2，R_2 与 $K_3,K_4,\cdots,K_n$ R_1 构成新的 n 个密钥去控制密码发生器产生新的密码数据块 Z_3，如此类推，直到由 C_{N-n} $C_{N-n+1}\cdots C_{N-1}$ 构成的密钥去控制密码发生器产生密码数据模块 Z_N，Z_N 与 M_N 模 2 加产生密文 C_N,从而完成对一帧数据的加密。其中的 M_i、K_i、C_i、Z_i、T_i 均为一个字长 m 比特。

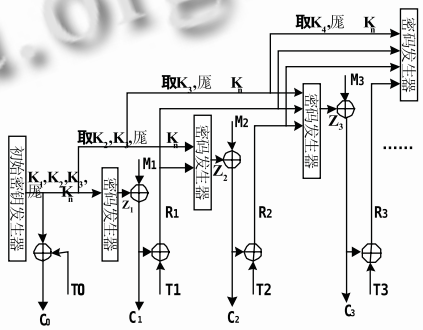

图 2　加密框图

初始密钥发生器是由噪声源产生乱数，每次加密都需要更新。密码发生器主要由若干个数据存储器构成，其复杂的算法用 C 语言编程来实现，密码算法存储与密码芯片外部的 FLASH 中，进行加密操作时由 DSP 控制密码芯片调用该密码算法。K_i 、C_i、T_i 经过具体算法运算由密码发生器产生密码数据 Z_i，Z_i 与 M_i 模 2 加产生密文 C_i。为了防止初始密钥被截获，本文用保密字 T_0 对其加密，中间的密文反馈也没有直接利用密文,而是先用保密字 T_i 进行加密之后再移位反馈。保密字 T_i 是存在密码芯片 SRAM 中，该密码芯片使用 Altera 公司的低成本 Cyclone 系列 FPGA 芯片来实现，使设计资源得到了极大的优化利用，降低了整个的设计成本。

2.2 解密实现

遥测数据的解密过程与加密过程基本相同，首先对收到的密码字 C_0 进行解密，从而恢复初始密 $K_1,K_2,K_3,\cdots,K_n$，由该密钥控制密码发生器产生密码数据 Z_1，Z_1 与密文 C_1 模 2 加生成明文 M_1，如果在信道传输的过程中密文 C_1 出错，而 Z_1 是正确的，错误则同样反应在 M_1 中，对 M_1 进行纠错译码产生 M_1'，M_1'

与 Z_1 模 2 加生成 C_1'，由选择器判断 M_1 中的出错数是否大于纠错能力，若出错数大于纠错能力，令 $C_1''=C_1'$，这样可以消除 C_1''出错带来的影响；否则令 $C_1''=C_1$，从而消除 Z_1 出错带来的影响。解密框图如图 3 所示。

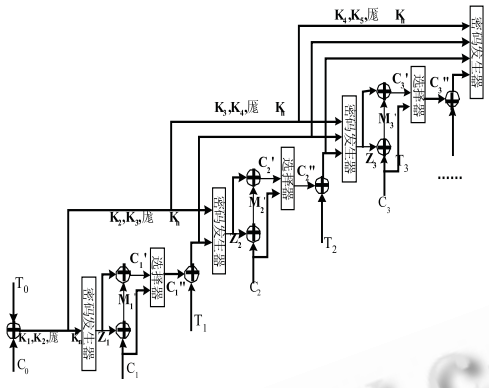

图 3　解密框图

3 遥测数据加解密方法的特点

(1)加密强度高

在加密过程中，尽管每个密钥都是从它前 n 个密文计算得到，但从原理上讲，每个密钥都依赖于它之前的全部明文和初始密钥，因此每个密文也都依赖于它之前的全部明文和初始密钥。这样明文和初始密钥的统计特性分散到全部的密文上，即所谓“置乱扩展”，从而使得密码分析者难以破译。通过使用保密字对初始密钥和中间密钥进行加密，降低了密码分析者截获分析初始密钥和中间密钥的概率。在字长为 m 比特，并且约束长度为 n 的情况下，密钥被截获的概率为 2^{-mn}。并且为加强保密性,在无人机每次升空执行任务前，都要更新保密字 T_i。

由于每帧数据都更新初始密钥，并且下次的初始密钥由密文 C1 随机化，这实际上利用了以前全部明文和初始密钥的统计信息。由于不同的初始密钥将产生不同的密码数据流，从而使得每帧密码数据流各不相同，呈现随机性。即使每路明文数据没有任何变化，对应的密文也将表现为随机或伪随机，致使第三方难以根据密文推断各路遥测数据的性质，加之不具备帧格式的相关信息，所以难以对遥测数据进行侦破。

虽然密钥存储器的容量有限，但由于在该加密方法中，对地址的产生具有足够的随机性。不同的地址组合将导致不同的密码数据流产生，也就保证了密码数据流的随机性。另外，即使密码破译者根据密文序列能够解出对应的部分密钥(其可信度仅为 2^{-mn})，也会由于不知道对应的明文性质和加密过程，也就难以形成对密钥存储器的查找表，因而无益于保密工作。

(2)错误扩散小

密文在传输过程中发生了错误，如果错误数在信道编码的纠错能力以内，就不会造成错误扩散；如果超出了纠错能力，错误扩散也不会造成一帧数据被丢失，只会向后扩散 n 个字长．这对遥测来讲，是可以容忍的．并且，这种错误扩散也并并不一定是缺点，适当应用这一特性，可以用于鉴别密文的真伪，以防第三方的篡改 。

(3)无信息扩散

该遥测加密方法仅仅对明文和密码作模 2 加运算，没有增加任何冗余数据，故没有信息扩散，从而降低了信息传输速率，节省了信道资源。

(4)实现简单

硬件上主要是使用 FPGA 和 DSP 芯片来完成控制和加密操作。软件只需要完成一些读取、控制操作，以及一些复杂的运算。

4 结语

本文介绍了无人机遥测数据传输中所采用的加解密方法．该方法充分考虑了遥测数据字、帧结构的特点以及遥测信道编码的因素，在保证了高加密强度的同时，还具有加解密实现简单，错误扩散小，无信息扩散等特点．经过硬件实现，证明了该方法的可行性和可靠性。

参考文献

1 吴汉平,等译.无人机系统导论.北京:电子工业出版社, 2003. 52－75.

2 Trappe W, Washington LC. Introduction to cryptography wit coding theory. Science Press, 2004.35－90.

3 卢铁城.信息加密技术.成都:四川科学技术出版杜, l989.18－33.

4 章照止.现代密码学基础.北京:北京邮电大学出版社, 2004.35－86.

5 罗启彬,张健.流密码的现状和发展.信息与电子工程, 2006,4(1):75－80.