# CCSDS 空间遥控链路异常行为检测算法

张 磊　安成锦　张 权　唐朝京
(国防科技大学电子科学与工程学院　长沙　410073)

**摘　要**：空间通信网络的开放性使其面临巨大的安全威胁，在空间遥控链路中应用认证或加密等密码学算法以增强空间遥控数据传输的安全性成为该领域的主要研究方向。由于 CCSDS 空间遥控链路 COP-1 协议与所加入的认证机制对传输错误均具有敏感性，而恶意攻击或信道误码均能引起数据接收端的重传请求，使得数据发送端无法对链路中的协议异常行为进行检测。该文提出了一种新的重传请求机制，改进了现有的 COP-1 传输控制协议，并建立了空间遥控链路中恶意攻击者的攻击行为模型，基于假设检验的策略提出了 CCSDS 空间遥控链路异常行为检测算法。仿真实验结果表明，所提出的算法能够在各种信道状态下准确、无误地检测到链路中攻击者的存在。

**关键词**：空间通信网络；通信安全；异常行为检测
**中图分类号**：TN915.08　　**文献标识码**：A　　**文章编号**：1009-5896(2010)02-0290-06
**DOI**: 10.3724/SP.J.1146.2009.01020

# Misbehavior Detection Algorithm in CCSDS Space Telecommand Link

Zhang Lei　An Cheng-jin　Zhang Quan　Tang Chao-jing
(*School of Electronic Science and Engineering, National University of Defense Technology, Changsha* 410073, *China*)

**Abstract**: Accessibility has enlarged the security threats in modern space communication network, various authentication and encryption solutions are to be considered and tested for possible adoption in the space context, based on widely used space link protocols. As adopted authentication mechanism andARQ characteristic of COP-1 are both error sensitive, most of the solutions proposed previously are designed oblivious of the protocol misbehavior distinguish between attack and normal interference in space channel. An innovative misbehavior detection algorithm is proposed for CCSDS TC systems, to address this problem with a hypothesis test approach based on the model of attacker's behavior and space fading channel. The simulation results show the proposed algorithm can detect the attack behavior successfully and without false alarm, when facing malicious security attacks against TC transmissions towards the spacecraft.

**Key words**: Space communication network; Communication security; Misbehavior detection

## 1　引言

遥控信息安全是遥控系统设计和任务实施过程中的关键问题之一。遥控信息的传输要经过空间链路，使得遥控系统具有开放性的特征。在对航天器实施遥控的过程中，攻击者可以通过技术手段截获所发送的遥控信号，分析和窃取遥控信息的内容，并通过篡改遥控信息对航天器进行攻击破坏。

CCSDS 安全工作组 (security working groups) 一直致力于针对空间任务的安全需求研究。2006 年，CCSDS 制定了 Security Threats Against Space Missions[1]和 The Application of CCSDS to Secure Systems[2]建议书，描述了空间任务所面临的安全威胁并提出了基于 CCSDS 标准的各类航天任务安全框架。CCSDS 建议对遥控信息进行认证保护是最基本的要求，将不同密码学算法应用到 CCSDS 分包遥控系统中成为 CCSDS 近两年的研究重点之一[3]。其中，Fischer 等人分析了数据保护机制在分包遥控系统中的实现位置[4,5]，并提出在分段层实现数据保护的局限性和在数据链路层实现数据保护机制可能产生认证循环与分包遥控系统中的 COP-1 闭环之间的冲突；Susanna 等人提出在 ESA 遥控系统的分段层中采用 EAX 认证加密模式[6]对遥控信息进行加密和认证的联合数据保护；本文作者提出了在 CCSDS 分包遥控系统链路层采用 GCM 认证加密模式，通过对数据帧导头进行认证保护、对数据域进行认证与加密双重保护的方法解决了认证循环与 COP-1 闭环之间的冲突[7,8]。

密码学算法能够保证空间链路数据的安全性，却无法检测空间链路中是否存在恶意攻击者。攻击者在成功接入物理信道后，除了采取针对密码学算法的攻击手段之外，还可以发起拒绝服务攻击，大

2009-07-17 收到，2009-11-16 改回
国家高技术研究发展计划项目(2008AA7010417)资助课题
通信作者：张磊　zlnudt@126.com

量消耗有限的空间链路带宽资源、降低数据传输效率。因此，在空间通信网络中进行入侵检测是非常必要的。然而，由于空间通信信道状态的不可预测性与链路的高误码率、长延时等特点，空间通信环境中的自然噪声所产生的误码具有随机性，误码会引发 COP-1 协议的 ARQ 机制要求重传，针对数据帧的伪造攻击也会引发认证循环的重传请求，这就使得数据发送端无法判断重传请求的原因是正常的误码还是恶意攻击。一般来说，如果地面操作控制中心检测到链路中有攻击行为发生，会切断现有链路并改变物理信道参数重新建立传输链路。因此，有别于地面通信网络的入侵检测，空间链路中入侵检测的风险性更高，断开链路重建物理连接所付出的代价巨大，这就要求对空间链路入侵检测的虚警概率的控制非常严格。

现有的研究成果论证了不同认证算法在 CCSDS 分包遥控系统中应用，但是并没有解决这一问题。考虑到空间信道状态的多变性及其入侵检测兼有信道状态估计的特殊性，借用无线传感器网络中的异常行为检测的概念，本文基于一种新的重传请求机制改进现有的 COP-1 传输控制协议，并通过建立空间遥控链路中恶意攻击者的攻击行为模型，基于假设检验的策略提出了 CCSDS 空间遥控链路异常行为检测算法。

## 2　CCSDS 空间遥控链路安全框架

分包遥控[9]是由空间数据系统咨询委员会(CCSDS)的建议书所规定的空间数据系统数据传输体制。在分包遥控系统中，不同信源、不同速率的数据通过动态管理形成统一的数据流，通过上行信道传输，包括航天器平台和有效载荷在内的各种应用过程通过这种方式获得灵活、透明和高效的数据传输业务。为了保证星地操作中上行数据链路的可靠性，分包遥控在传送层定义了命令操作步骤(COP-1)[10]，它负责数据在对等层之间进行无差错、按序、无遗漏及无重复的闭环操作，是 CCSDS 分包遥控中的重要组成部分。COP-1 基于 go-back-n ARQ 策略的滑动窗口流控制机制使用帧序列计数的接收和重传，是 CCSDS 建议书中实现遥控闭环控制的关键。发送端的帧操作步骤(FOP-1)组织遥控帧的同时启动一个向上的序列计数器，接收端的帧接收和汇报机制(FARM-1)只接收到达帧序列计数与星上的帧序列计数相符合的传输帧，如果计数不匹配，FARM-1 将拒收后续到达的一系列帧，并通过下行链路返回 CLCW 要求 FOP-1 重传。FOP-1 检测 CLCW 是否有帧被拒收，如果有，则从 FARM-1 所期待的帧序列号开始重新发送。COP-1 保证遥控数据在有噪信道中正确、完整、顺序地传输。

CCSDS 相关标准建议对遥控信息进行认证保护是最基本的要求[1]，由前一阶段研究成果[7]，本文通过在分包遥控系统的数据链路层应用 GMAC[11] 算法以保证数据的完整性及其来源的合法性。GMAC 是 GCM 认证加密模式的特例，GMAC 只具有产生消息认证码的功能，而不具有加密功能。其输入包括密钥(KEY)、初始化向量(IV)和数据，输出消息认证码(MAC)，即 GMAC(KEY, IV, Data)=MAC，其安全目标是保证消息的认证性。其中，惟一的 IV 确保能够抵抗重放攻击。为了更好地利用 GMAC 算法的高效性，将遥控传输帧中原 8-bit 的帧序列号(frame sequence number)字段扩展为 96 bit，作为 GCM/GMAC 认证算法的初始化向量(Initial Vector, IV)；为了降低附加的消息认证码所占用的链路带宽，使用 GMAC 允许的最小密钥长度 64 bit 产生相同长度的消息认证码，消息认证码的产生过程如图 1 所示。

由于信道的自然噪声所产生的误码与基于协议的恶意攻击均能使得星上数据接收端的 FARM-1 传输控制单元发出重传请求，本文改进了原有的下行链路命令链路控制字(Command Link Control Word, CLCW)结构，如图 2 所示。将原 CLCW 结构中的 2-bit 的空闲位设置为“重传请求原因标记”(Retransmission Request Reason Flag, R.R.R. Flag)，若由于 FARM-1 的“帧有效性检查”或“帧接受检查”失败，则 R.R.R. Flag=“10”；若由于消息认证码验证失败，则 R.R.R. Flag=“01”。相应地，由于加入了数据帧认证保护处理过程，需要对原有的 COP-1 传输控制协议进行修改，以避免 COP-1 闭环与认证循环之间的冲突。改进后的 COP-1 协议流程图如图 3 所示。

传统的CCSDS TC协议利用信道编码层的差错控制编码与传输层定义的帧有效性检查步骤保护数据的正确性。到达星上数据接收端的所有数据帧都要经过帧有效性检查，包括帧导头的有效性与CRC校验值的正确性。如果数据帧通过了帧有效性检查，才会传送给FARM-1单元进行帧接受检查，确保数据帧的序列性。本文将传统的FOP-1协议单元分为两个部分：FOP-1 帧生成单元完成帧导头参数的生成，FOP-1传输控制单元执行数据帧的传输控制，如向下层协议单元传送数据帧、接收FAMR-1发送的CLCW等。而GMAC认证单元位于FOP-1 帧生成单元与FOP-1传输控制单元之间，生成消息认证码。

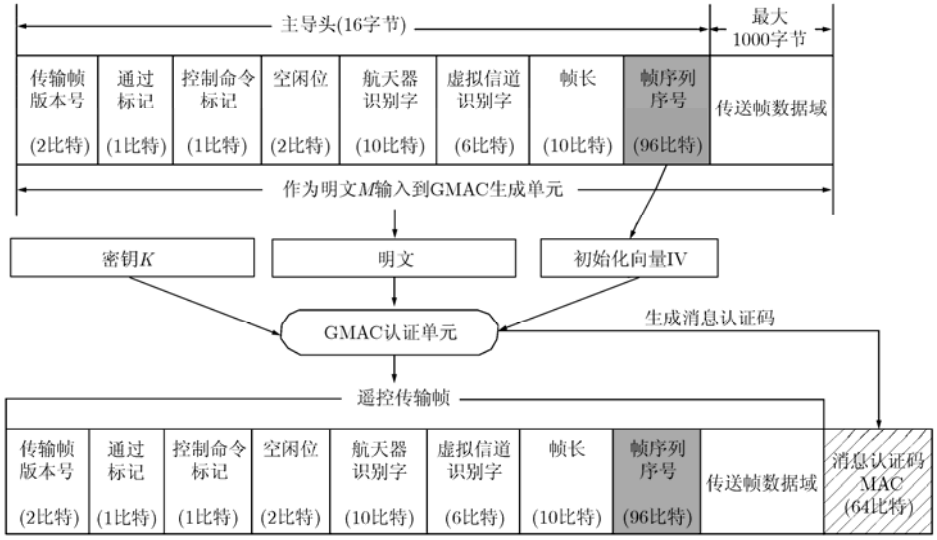


图1 GMAC消息认证码生成流程图

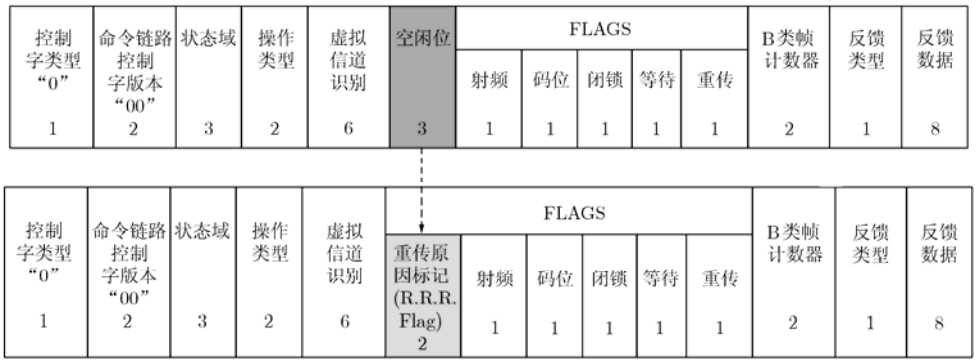


图2 CLCW字段结构修改图

由图3所示，在FOP-1传输控制单元中，设有两个计数器 $R_1$ 、 $R_2$ 分别统计在一定时间内所接收到的

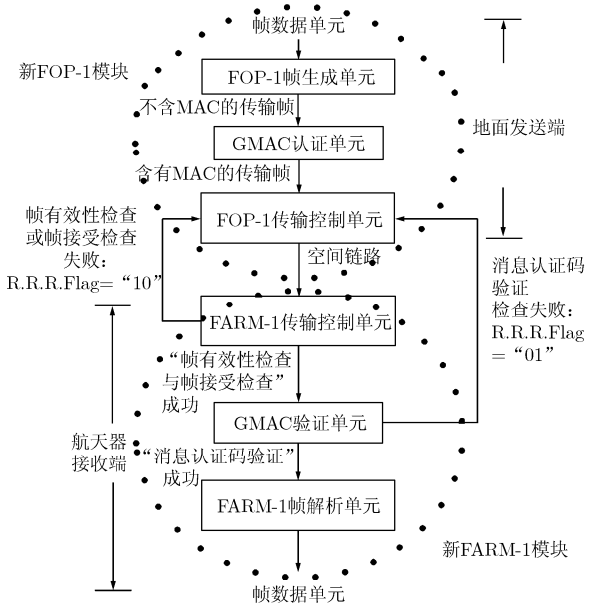


图3 改进后的COP-1协议传输控制流程图

CLCW中 R.R.R. Flag="01" 与 R.R.R. Flag="10" 的数量，以进行基于假设检验策略的空间遥控链路异常行为检测。

## 3 CCSDS 空间遥控链路异常行为检测算法

### 3.1 空间通信网络攻击行为模型

在本文中，假设空间链路中的攻击者具有以下能力：

(1)攻击者掌握航天器的轨道参数等知识，能够成功的接入物理信道；

(2)攻击者掌握遥控传输帧的帧结构，并能对传输帧进行帧结构解析；

(3)攻击者能够截获遥控链路传输帧；

(4)攻击者能够丢弃所截获的传输帧，并且能够篡改传输帧的各个字段进行伪造攻击。

与针对地面通信网络进行攻击不同，空间通信链路中的攻击行为同样受到通信环境高误码率、长延时的影响，恶意攻击的难度加大，攻击者不会轻易地仅仅发动拒绝服务攻击破坏天地间的正常通

信，其最高目标是通过攻击得到对航天器的控制权。因此，伪造攻击成为空间遥控链路攻击行为中的主要表现形式，一次针对空间遥控链路的伪造攻击包括以下攻击行为：攻击者截获遥控传输帧，识别链路层协议并解析帧结构，篡改其中的字段并重组数据帧发送给航天器以破坏航天器与地面控制中心的正常通信。根据篡改字段位置的不同，存在以下 3 种情况：

(1)攻击者篡改帧导头部分字段。帧有效性检查与帧接受检查在检测到帧导头部分受到篡改后，丢弃传输帧，并向发送端发送重传请求；R.R.R. Flag =“10”。

(2)攻击者篡改帧数据域部分或(与)消息认证码部分。篡改后的帧能够通过帧有效性检查与帧接受检查，接收端在重新计算消息认证码后检测到篡改，丢弃传输帧，并向发送端请求重传； R.R.R. Flag =“01”。

对于一个最优策略攻击者而言，为了获得对敌方航天器的控制权限，由于修改帧导头字段只会降低目标通信性能的降低，故其最主要的攻击方式是通过寻找 GMAC 中单向散列函数的冲突(即进行“碰撞攻击”)来实施后续的重放攻击、中间人攻击等，即第(2)种攻击行为的发生概率在所有伪造攻击中是最高的。在 3.2 节中，本文将针对第(2)种攻击行为，结合第 2 节对现有分包遥控数据结构的改进，基于假设检验的策略提出一种异常行为检测算法。

### 3.2 异常行为检测算法

**定义 1**　观测事件 E 为一遥控帧在通过“帧有效性检查”及“帧接受检查”后是否需要重传。定义 $M$ 为发送端在一次传输过程中发送的帧数量，则观测帧数量 $N = M - R_1$。

**定义 2**　定义假设 $H_1$ 为空间遥控链路中存在攻击者，假设 $H_0$ 为无攻击者。定义虚警概率 $P_F$，$\eta_1$ 为对应的虚警判决门限；漏警概率 $P_M$，$\eta_2$ 为对应的漏警判决门限。

**定义 3**　以 $z_i$ 表示第 $i$ 帧的观测值，即观测一遥控帧是否需要重传。定义：

$$z_i = \begin{cases} 0, & \text{GMAC(Data}') = \text{MAC} \\ 1, & \text{GMAC(Data}') \neq \text{MAC} \end{cases} \tag{1}$$

其中 Data 和 Data′ 分别表示发送发送端发出的数据与接收端接收到的数据，即

$$\left.\begin{array}{l} \text{Data=FramePrimaryHeader}||\text{FrameDataField} \\ \text{Data}'\text{=FramePrimaryHeader}'||\text{FrameDataField}' \end{array}\right\} \tag{2}$$

由定义 1 知，该遥控帧通过“帧有效性检查”及“帧接受检查”，即其导头部分在传输过程中无错误，故

$$\text{FramePrimaryHeader} = \text{FramePrimary Header}'$$

按照第 2 节中的定义，$R_1$，$R_2$ 分别统计在发送的 $M$ 帧中所接收到的 CLCW 中 R.R.R. Flag=“01”与 R.R.R. Flag=“10”的数量，故有下式存在：

$$R_2 = \sum_{i=0}^{N} z_i \tag{3}$$

下面分别按照 $z_i = 0$ 与 $z_i = 1$ 两种情况进行分析。

(1) $z_i = 0$ 时，观测帧不需要重传，存在以下两种可能情况：

(a) 自然噪声引起的误码未落在帧数据域及消息认证码(MAC)内，并且链路不存在攻击(此处假设攻击者智能化，只攻击帧结构中的数据域)；

(b)伪造攻击成功(攻击者成功找到 GMAC 中的碰撞)；

(2) $z_i = 1$ 时，观测帧需要重传，同样存在以下两种可能情况：

(a) 自然噪声引起的误码可能落在帧数据域或 MAC 内；

(b)攻击者有攻击帧数据域的行为发生，但攻击没有成功。

为表述方便，本文以 noise = 0 表示自然噪声引起的误码未落在帧数据域及消息认证码(MAC)内的情况， noise = 1 表示自然噪声引起的误码落在帧数据域或消息认证码(MAC)内的情况。

由上述分析可知，在 $H_1$ 情况下，链路中存在攻击但不需要重传的概率为

$$\begin{aligned} P(z=0|H_1) &= P(z=0,\text{noise}=0) \\ &\quad + P(z=0,\ \text{noise}=1) \\ &= P(z=0|\text{noise}=0)\cdot P(\text{noise}=0) + 0 \\ &= (B+1)\cdot 2^{-L_m}\cdot(1-P_b)^{L_d+L_m} \end{aligned} \tag{4}$$

其中 $P_b$ 为空间信道的误码率， $L_d$ 和 $L_m$ 分别表示帧数据域与 MAC 字段的长度(bit)，$B = (L_d + L_m)/64$ 为帧数据域与 MAC 字段所包含的 64-bit 分组数，$(B+1)\cdot 2^{-L_m}$ 为 GMAC 碰撞攻击的最大成功概率[7]；$P(z=0,\text{noise}=0)$ 即为自然噪声产生的误码未落在帧数据域及 MAC 内、并且攻击成功的联合概率；$P(z=0,\text{noise}=1)$ 表示自然噪声产生的误码落在数据域或 MAC 内、并且不需要重传的联合概率，显然为 $P(z=0,\text{noise}=1)=0$。

则 $H_1$ 情况下，链路中存在攻击并且需要重传的概率为

$$\begin{aligned} Q &= P(z=1|H_1) = 1 - P(z=0|H_1) \\ &= 1-(B+1)\cdot 2^{-L_m}\cdot(1-P_b)^{L_d+L_m} \end{aligned} \tag{5}$$

同理，在 $H_0$ 情况下，链路中无攻击、并且不需

要重传的概率为 $P(z=0|H_0)=(1-P_b)^{L_d+L_m}$；链路中无攻击、并且需要重传的概率为

$$P=P(z=1|H_0)=1-P(z=0|H_0)=1-(1-P_b)^{L_d+L_m} \tag{6}$$

故，由定义 2 及式(5)，式(6)，可得

$$P_F=P(R_2\geq\eta_1|H_0)=1-P(R_2<\eta_1|H_0)$$
$$=1-\sum_{i=0}^{\eta_1}C_N^iP^i(1-P)^{N-i} \tag{7}$$

$$P_M=P(R_2\leq\eta_2|H_1)=\sum_{i=0}^{\eta_2}C_N^iQ^i(1-Q)^{N-i} \tag{8}$$

对于确定的虚警概率 $P_F$ 和漏警概率 $P_M$，可由式(7)，式(8)求得响应的虚警判决门限 $\eta_1$ 和漏警判决门限 $\eta_2$。根据观测到的 $R_2$ 值，制定异常行为检测算法的判决规则如下：

$$\left.\begin{array}{rcl} R_2\geq\eta_1 & \Rightarrow & \text{假设}H_1\text{成立} \\ R_2\leq\eta_2 & \Rightarrow & \text{假设}H_0\text{成立} \\ \eta_2<R_2<\eta_1 & \Rightarrow & \text{其他} \end{array}\right\} \tag{9}$$

## 4 仿真实验与分析

本节通过计算机仿真验证所提出的异常行为检测算法的有效性。采用 Gilbert-Elliott 信道模型[12,13]来模拟空间信道的衰落特性。设置在一次传输过程中随机发生 20 次篡改帧数据域的攻击行为。实验观测 $K=100$ 次帧传输过程，每次传输过程发送 $M=200$ 帧。相关实验参数设置如表 1 所示。

**表 1 仿真实验参数设置**

| 参数名称 | 表示符 | 数值 |
|---|---|---|
| 帧导头长度(bit) | $L_h$ | 128 |
| 消息认证码长度(bit) | $L_m$ | 64 |
| 传输延时(s) | $T_p$ | 0.02 |
| 链路带宽(bps) | $C$ | 150 k |
| CLCW 间隔时间(s) | $T_c$ | 0.01 |
| 虚警率 | $P_M$ | $1\times10^{-4}$ |
| 漏警率 | $P_F$ | $1\times10^{-1}$ |

为了更加全面的测试提出的异常行为检测算法，分别针对不同质量的信道进行了测试，在质量较好的信道中，设置 Gilbert-Elliott 信道模型的状态转移概率使得信道平均误码率为 $P_b=1\times10^{-6}$；信道质量较差时，设置使得信道平均误码率达到 $P_b=1\times10^{-3}$。在仿真过程中，为了更加清晰地表示异常行为的检测结果，本文将未检测到攻击存在时的吞吐量效率值设为“1”，在检测到伪造攻击时的吞吐量效率值设为“0”。仿真实验结果如图 4、图 5 所示，图中实线表示的是在没有应用提出的异常行为检测算法时，COP-1 协议的吞吐量效率在链路受到攻击时的变化情况。图中实心的“圆点”表示伪造攻击随机发生点，“圆圈”与“圆点”重叠的点即表示异常行为检测算法成功检测到的攻击点，由仿真结果可知，在信道质量较好时，提出的算法对于伪造攻击的检测无虚警、无漏警；而在信道质量较差时，在 22 次随机发生的攻击中，检测到了 19 次。一方面，这是由于信道质量较差时，自然噪声引起的误码较多，相应的帧数据域或 MAC 内存在自然噪声误码的概率增大，即伪造攻击与自然噪声误码同时存在于帧数据域或 MAC 内的概率大大增加，导致提高了数据接收端的重传请求数量，造成漏警；另一方面，本文实验参数设置时将漏警概率设为 0.1，就是考虑到空间通信环境的多变所造成的链路间歇性特点，防止异常行为检测算法将临时的链路中断判断为攻击继而采取不必要的行动；并且，不同于地面网络中的入侵检测系统，对于空间链路中的异常行为检测，所加入的认证算法能够保证足够高级别的安全，所以相比漏警而言，虚警造成的后果更加严重。因此，空间链路中的异常行为检测应以无虚警的检测到攻击者的存在为主要目标。

综上所述，本文提出的异常行为检测算法能够在各种信道状态下准确、无虚警的检测到链路中攻击者的存在。

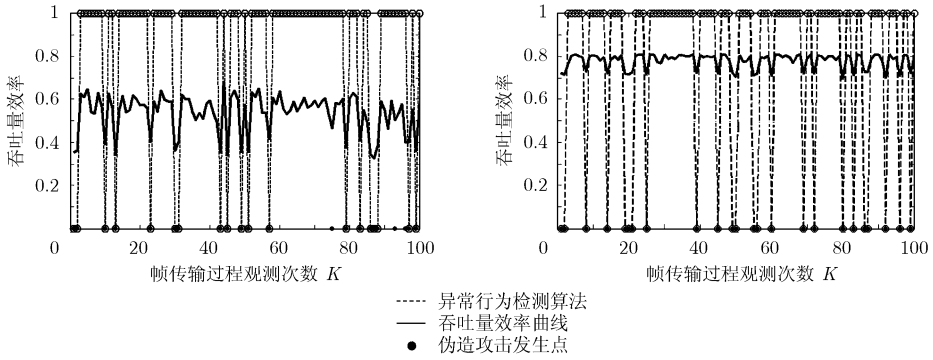


图 4 仿真结果图($P_b=1\times10^{-3}$)　　图 5 仿真结果图($P_b=1\times10^{-6}$)

## 5　结束语

CCSDS 空间遥控链路中 COP-1 协议的 go-back-n ARQ 机制与加入的认证保护的错误重传机制对遥控帧的传输错误均具有敏感性，而自然噪声与恶意攻击均能产生重传错误，导致数据发送端无法识别重传请求的原因，进而无法检测空间遥控链路中是否有攻击者存在。为解决这一问题，本文建立了空间遥控链路中的攻击行为模型，通过在原有 CLCW 数据结构中添加“重传请求原因”字段设计了一种新的重传请求机制，改进了原有的 COP-1 协议，进而基于假设检验的策略提出了一种空间遥控链路异常行为检测算法。基于对 COP-1 协议的改进，结合提出的异常行为检测算法，设计了一种跨层空间遥控链路安全框架。仿真实验结果表明，所提出的算法能够准确的、无虚警地检测出空间遥控链路中存在的攻击行为。

## 参 考 文 献


[1] CCSDS 350.1-G-1. Security threats against space missions [S]. Washington USA, National Aeronautics and Space Administration, 2006.

[2] CCSDS 350.0-G-2, The application of CCSDS to secure systems [S]. Washington USA, National Aeronautics and Space Administration, 2006.

[3] CCSDS Security Working Group. Recommended practice for authentication [S]. http://cwe.ccsds.org/sea/docs/, March 2007.

[4] Fischer D, Merri M, and Engel T. Introducing a generic security extension for the packet TM/TC protocol stack [C]. 4th ESA International Workshop on Tracking, Telemetry and Command Systems for Space Applications, Darmstadt, Germany, 2007: 235–242.

[5] Fischer D, Engel T, and Merri M. Approach of the integration of data security in the CCSDS packet TM/TC standards [C]. Ninth International Conference on Space Operations (Spaceops), Rome, Italy, June 19–23 2006: 524–531.

[6] Spinsante S, Chiaraluce F, and Gambi E. New perspectives in telecommand security: The application of EAX to TC segments [C]. Proc. Data Systems In Aerospace (DASIA), Naples, ITALY, 2007: 296–303.

[7] Zhang L, Spinsante S, Tang C, and Gambi E. Application and performance analysis of various AEAD techniques for space telecommand authentication [J]. *IEEE Transactions on Wireless Communications*, 2009, 8(1): 308–319.

[8] 张磊, 周君, 唐朝京. 认证加密算法在 CCSDS 遥控协议中的应用研究 [J]. 电子与信息学报, 2009, 31(2): 343–348.
Zhang Lei, Zhou Jun, and Tang Chao-jing Research on Application of AEAD Techniques for CCSDS Telecommand Protocol. *Journal of Electronics & Information Technology*, 2009, 31(2): 343–348.

[9] CCSDS 232.0-B-1, TC Space data link protocol [S]. Washington USA, National Aeronautics and Space Administration, 2003.

[10] CCSDS 232.1-B-1, Command operation procedures-1[S]. Washington USA, National Aeronautics and Space Administration, 2003.

[11] McGrew D and Viega J. The security and performance of the Galois/Counter Mode (GCM) of operation [J]. *Lecture Notes in Computer Science*, 2004, 3348: 343–355.

[12] Gilbert E N. Capacity of a burst-noise channel [J]. *Bell System Technical Journal*, 1960, 39(9): 1253–1265.

[13] Elliot E O. Estimates of error rates for codes on burst-noise channels[J]. *Bell System Technical Journal*, 1963, 42(9): 1977–1997.



张　磊：　男，1981 年生，博士生，研究方向为空间信息网络安全.

安成锦：　女，1982 年生，博士生，研究方向为信号处理.

张　权：　男，1974 年生，副教授，研究方向为通信网安全协议分析.

唐朝京：　男，1962 年生，教授，博士生导师，研究方向为通信网信息安全与对抗.