一种空间信息网络中改进的SCPS-SP

廖 勇[1,2] 陈鸿宇[3] 沈轩帆[1]
(重庆大学飞行器测控与通信教育部重点实验室 重庆 400044)[1]
(西安电子科技大学陕西省网络与系统安全重点实验室 西安 710071)[2]
(重庆大学计算机学院 重庆 400044)[3]

摘 要 在互联网安全协议(IPSec)和空间通信协议规范-安全协议(SCPS-SP)的基础上,针对空间信息网络中SCPS-SP在安全级别自适应、抗重放攻击方面对数据保护的不足,提出一种改进的SCPS-SP(M-SCPS-SP)。该协议可以满足不同空间信息网络用户的安全级别需求,同时还具有扩展性,支持不同的高效加密和认证算法。最后,搭建基于SCPS参考实现的仿真平台,验证了所提M-SCPS-SP的可行性和有效性。

关键词 空间信息网络,安全,SCPS-SP,加密,认证,抗重放,SCPS参考实现
中图法分类号 TN918 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.06.026

Modified SCPS-SP for Space Information Network

LIAO Yong[1,2] CHEN Hong-yu[3] SHEN Xuan-fan[1]
(Key Laboratory of Aerocraft TT&C and Communication, Ministry of Education, Chongqing University, Chongqing 400044, China)[1]
(Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an 710071, China)[2]
(College of Computer Science, Chongqing University, Chongqing 400044, China)[3]

Abstract Based on IP security (IPSec) and space communication protocol specification-security protocol (SCPS-SP), a modified SCPS-SP (M-SCPS-SP) was proposed to fill up the deficiency of data protection in following aspects for space information network, including security level adaptation and anti-replay attacks. The M-SCPS-SP can meet different space information network users' needs of security level, moreover it is expandable to support efficient encryption and authentication algorithms. Finally, we built a simulation platform based on the SCPS reference implementation, and then verified the feasibility and effectiveness of the proposed M-SCPS-SP.

Keywords Space information network, Security, SCPS-SP, Encryption, Authentication, Anti-replay, SCPS reference implementation

1 引言

空间信息网络成为近年来国内研究的热点,天空地一体化网络也是未来网络发展的重要趋势[1-2]。与地面通信系统相比,空间通信系统的覆盖范围更广,拓扑结构变化更加频繁,数据在传输过程中更容易受到攻击;针对空间任务延迟大、传输误码率高、前向和后向链路差异大等特点,传统的地面通信因特网安全协议(IPSec)并不适用于空间通信系统[3-4]。

为适应空间信息网络的特性,空间数据系统咨询委员会(CCSDS)以TCP/IP分层结构为模型,制定了空间通信协议规范(SCPS)[5]。在SCPS协议簇中,SCPS-SP是空间安全协议[6],类似于IPSec,其主要功能是提供无连接的端到端的安全保护,可以提供机密、完整性、鉴别中的一项或全部服务。

SCPS-SP最主要的特点是提供一种端到端的安全保护,主要包括完整性保护、身份认证保护和数据机密性保护,它借鉴了地面IPSec的保护机制,通过对网络层的数据进行重新封装后组成安全报文(S-PDU)再传送到信道中来达到安全保护的目的,近年来其得到了研究人员的广泛关注[7-14]。但是它尚有不足:1)在空间网络通信中,如果涉及到中继通信,则可能被恶意的第三方在中继设备上对源节点传输的报文进行身份认证的破坏,进而对目的节点进行重放攻击[15];2)虽然在SCPS-SP中定义了安全等级[9]的概念,但是没有给出具体的使用标准,使得安全等级概念没有得到实际的体现。

针对上述问题,为了提高空间信息网络通信的安全性和可靠性,本文在前期研究工作的基础上[16],提出一种SCPS-SP多安全等级及抗重放功能的设计方法,并结合开源的SCPS参考实现进行仿真验证。

到稿日期:2016-05-09 返修日期:2016-09-20 本文受国家自然科学基金重大研究计划培育项目(91438104),国家自然科学基金项目(61571069),陕西省网络与系统安全重点实验室开放基金(NSSOF1500101),重庆大学中央高校基本科研业务费重点项目(CDJZR165505)资助。
廖 勇(1982—),男,博士,副研究员,CCF高级会员,主要研究方向为宽带无线通信与网络,E-mail:liaoy@cqu.edu.cn;**陈鸿宇**(1995—),男,主要研究方向为无线网络安全;**沈轩帆**(1994—),男,硕士生,主要研究方向为宽带无线通信。

2 改进的 SCPS-SP

为了克服现有 SCPS-SP 的不足，本文针对 SCPS-SP 提出了两点改进：1）具体化了 SCPS-SP 中的分等级安全保护概念，根据用户的不同服务需求将数据的安全保护分为 A，B，C 3 等，还根据采用算法的不同将每一等级分为 3 个水平值，用户可以选择自己需要的安全等级来实现通信的保护；2）在 SCPS-SP 现有的服务上增加抗重放功能。

2.1 安全等级划分

根据所能提供的不同服务将安全等级分为 A，B，C 3 类，其中又根据所使用算法的不同将每一类分为 3 个安全水平 1，2 和 3，为每一个安全水平分配唯一的安全标签值，如表 1 所列。

表 1 安全等级划分具体情况表

等级	提供的服务	子等级	使用的算法	安全等级标签
A	认证，完整	A1	MD5	1010 0001
		A2	SHA-1	1010 0010
		A3	MD2	1010 0011
B	加密	B1	AES	1011 0001
		B2	3DES	1011 0010
		B3	DES	1011 0011
C	认证，完整，加密	C1	AES，MD5	1100 0001
		C2	3DES，SHA-1	1100 0010
		C3	DES，MD2	1100 0011

本文规定的安全等级标签域的长度为 8 bit，可以提供 2^8 个安全等级，各个安全等级独立存在，由用户根据业务需要自主设定，而本文目前暂定义其中 9 个，将余下的如 0000 0000～1010 0000，1010 0100～1011 0000，1011 0100～1100 0000，1100 0100～1111 1111 等未使用的标签做预留用。

2.2 抗重放服务

2.2.1 报文结构设计

如图 1 所示，在 SCPS-SP 报文保护头中增加了 8 bit 抗重放标识符，来控制抗重放服务功能的使用与否，十六进制 0X16 表示使用。同时，在 SCPS-SP 保护头中添加一个 32 bit 的抗重放域，存放一个单调递增的序列号，该序列号在安全联盟(SA)创建时为 0，若中途报文被非目的端用户所篡改，则抗重放域序号将根据被篡改的次数递增。另外，空间信息网络中报文的通信有连续通信和间断通信。当飞行器工作在连续通信模式时，若出现第三方恶意的重放攻击，则会在收发端规定一个最大的重放攻击值，该数值可以为不大于 2^{32} 的任一整数。若重放攻击的次数达到规定的最大值，则此时双方中断链路的通信。

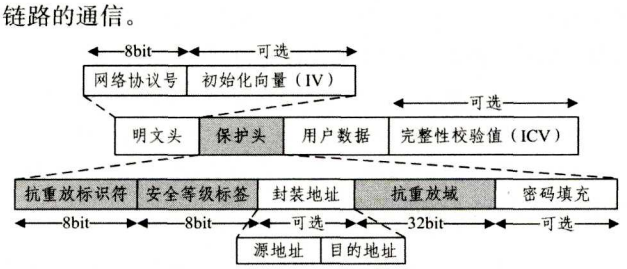

图 1 改进的 SCPS-SP 报文格式

2.2.2 抗重放功能实施过程

在收发双方启动抗重放域功能的情况下，在接收端建立一个长度为 64 字节的抗重放序号缓冲窗口，一个报文序号最大占用 4 个字节，抗重放序号缓冲窗口工作的起始报文序号为 N，该窗口可以向右滑动，如图 2 所示，接收端对接收到的数据进行以下处理来实现抗重放服务。

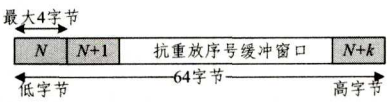

图 2 抗重放序号缓冲窗口

具体处理过程如下：

(1)在抗重放域序号没有达到最大重放序号，且接收端收到的抗重放域序号未增加的条件下，将 SA 的序列号(记为 n)与此缓冲窗口序号进行比对。

若 $n<N$，则判定接收到的报文序列号在缓冲窗口左侧，此报文在之前已成功接收，直接丢弃该报文。

若 $n>N+k(16\leqslant k\leqslant 63)$，则判定接收到的报文序列号在缓冲窗口右侧，此报文目前为非正常顺序接收，先缓存在接收端，然后等待序号缓存窗口滑动到此序号区间再进行处理。

若 $n\in[N,N+k]$，则判定接收到的报文序列号在缓冲窗口内部，进而检查缓冲区是否有接收过该报文，若没有则接收此报文，若有则丢弃此报文。当整个抗重放缓冲窗口装填满 64 字节之后，窗口往右侧滑动，进入下一个序号缓冲区。

(2)在抗重放域序号未达到最大收发双方规定的最大约定序号时，接收端连续收到的报文头中抗重放域增加，此时接收到的报文需要丢弃。

(3)如果抗重放域序号已经达到最大收发双方规定的最大约定序号，则通信中断。

3 基于 SCPS 参考实现的安全协议仿真与分析

3.1 协议栈编译

此次实验在 Red Hat 9.0 虚拟系统下进行，实验前的必要操作是将开源代码 SCPS_RI_1_1_132 压缩包[17]导入 Red Hat 9.0 系统中，采用 SecureCRT 连接 VMWare 虚拟机，并将其压缩文件导入系统。

接下来进行 SCPS 参考实现(SCPS_RI)的安装编译[18]，其具体步骤为：1）进入 SCPS 文件中的 apps 目录；2）运行./configure 命令；3）返回上一层目录；4）进入 source 目录；5）运行 make clean；make 指令。

图 3 为 SCPS_RI 成功编译之后的截图。

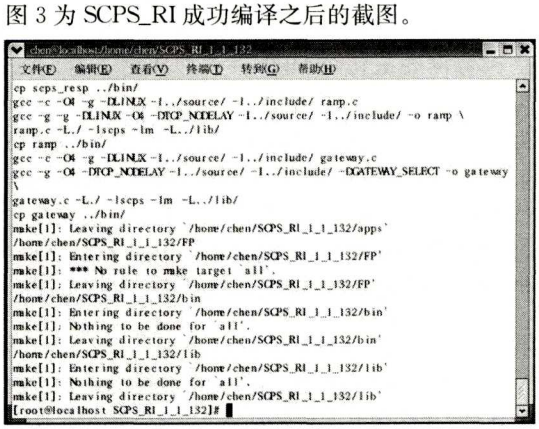

图 3 SCPS_RI 协议栈成功编译的结果

3.2　主要代码修改

若需对 SCPS-SP 进行改进，则应该首先对 SCPS 协议中关于安全协议部分的函数功能进行分析，然后再在此基础上进行适应性修改。

在 SCPS_RI_1_1_132/source 中经过观察分析发现，SCPS-SP 实现主要出现在 scps_sp. h，scps_spc. c 和 scps_sp. c 3 个代码文件中，接下来对这 3 个文件进行修改。

3.2.1　服务质量和安全等级定义

服务质量和安全等级定义出现在 scps_sp. h 中，作为一个头文件，此代码进行了两种说明。

(1)服务质量分为 4 个等级：保密、验证、安全标签和完整性，服务质量由明文头的低 4 位决定，如图 4 所示。

```
/* Quality-of-Service flags for scps_sp to be found in the 4 low-order
    bits of the clear header */
#define CONFIDENTIALITY 0x01
#define AUTHENTICATION 0x02
#define SECURITY_LABEL 0x04
#define INTEGRITY 0x08
```

图 4　服务质量分级定义

(2)安全等级默认分为 3 个安全等级，在改进时将 3 个安全等级加以细化，同时标注出不同安全等级的加密和认知算法，如图 5 所示。

```
void log_sp_error (enum ERRORS error);
#define SECURE_GATEWAY_NO_SECURITY  0
#define A1 1010 0001 //MD5
#define A2 1010 0010 //SHA-1
#define A3 1010 0011 //MD2
#define SECURE_GATEWAY_ON_DEMAND  1
#define B1 1011 0001 //AES
#define B2 1011 0010 //3DES
#define B3 1011 0011 //DES
#define SECURE_GATEWAY_STRICT_SECURITY  2
#define C1 1100 0001 //AES,MD5
#define C2 1100 0010 //3DES,SHA-1
#define C3 1100 0011 //DES,MD2
#endif /* scpssp */
```

图 5　安全等级定义

3.2.2　认证加密处理

认证加密功能主要出现在 scps_spc. c 中，为便于理解，将此源代码的内容分为 3 个模块：计算完整性检查值(ICV)、加密/解密功能和改进添加的高级安全标准，函数执行流程如图 6 所示。

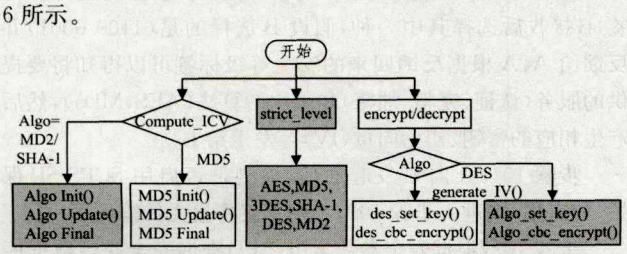

图 6　加解密处理流程图

(1)计算 ICV。此模块为每一个数据包计算 ICV，计算 ICV 的算法和密钥由 SA 决定。原文件中仅提供了 MD5 的算法，本文在此基础上添加了 MD2 和安全散列算法-1(SHA-1)，使其有更多的选择和更佳的认证功能，同时继续保留 MD5 算法，使 ICV 的计算具有更好的兼容性。

(2)加密/解密。在加密/解密功能中，仍然是由 SA 决定算法。源代码中仅涉及了数据加密标准(DES)算法和简单的异或(XOR)算法。若执行 DES 算法，则将 generate_IV()函数产生的向量作为变量，调用 des_set_key()等函数继续执行；执行 XOR 算法，则会调用 kxor()函数。在改进的过程中，将简单的 XOR 算法替换为高级加密标准(AES)、3DES 等更优算法，使其具有更好的保密性。

(3)高级安全标准。原代码中并无此项功能，此功能系改进添加。在将安全等级细化划分的过程中，原代码并未对第 3 等级进行详细描述。在改进中，为其添加了 3 种混合算法，分别为 AES 与 MD5，3DES 与 SHA-1 和 DES 与 MD2，以更好地完成认证、完整、加密服务。

3.2.3　抗重放功能实现

图 7 示出了添加抗重放功能的 SA 流程图，这部分功能函数在 scps_sp. c 文件中，其主要函数功能描述如下：1) sp_request，发送请求；2) sp_get_template，构建面向连接的用户模板；3) get_SAinfo，获取 SA 信息；4) test_decrypt，解密测试；5) log_sp_error，返回安全协议中的错误类型报告；6) sp_trequest，有 5 种功能，即安全网关设置、设置时间戳、检索安全关联值、安全网关调试和加密新构造的数据包；7) sp_ind，有 4 种功能，即检索数据包(未调用函数)、确定发送请求的安全网关的模式、保密功能和测试解密功能。如图 7 所示，按照 2.2.2 节抗重放功能的实施原理，在发送端添加了抗重放处理模块，在接收端通过抗重放窗口进行报文检测。

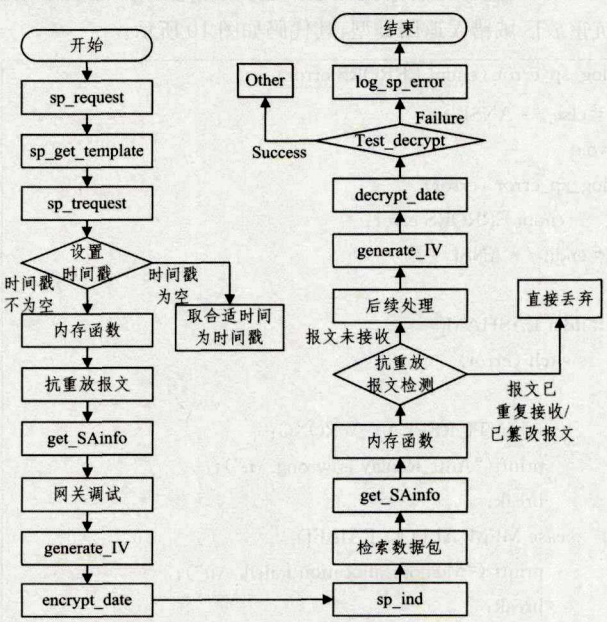

图 7　添加抗重放功能的 SA 流程图

在 scps-sp 源代码中修改的报文结构及添加抗重放报文检测的对应代码如下。

(1)报文结构修改。在 scps_sp. h 头文件的安全选项标

示符中定义抗重放选项：ANTI_REPLAY，其代码如图 8 所示。

```
/* Bitflags indicating presence or absence of optional fields within
the
    protected header.
*/
#define ICV_APPEND 0x01
#define PADDING 0x02
#define ENCAPS_NP_ADDR 0x04
#define SEC_LABEL 0x08
#define ANTI_REPLAY 0x16
```

图 8 修改的报文头定义

(2)抗重放操作。在 scps_sp. c 源文件的保护头中添加抗重放功能，其代码如图 9 所示。

```
/*-----
 * ANTI REPLAY - add a anti replay label to the project header
 *-----
*/
if ((rqts->sprqts & ANTI_REPLAY) || (SAinfo. QOS & ANTI_REPLAY))
  {
  Protected_Header |=ANTI_REPLAY;
  ws[data_len++] = SAinfo. anti_replay_len;
  memcpy((char *) &(ws[data_len]),(char *)(SAinfo. anti_replay),SAinfo. anti_replay);
  data_len += SAinfo. anti_replay_len;
 }
```

图 9 抗重放功能操作

(3)抗重放功能错误处理。在 log_sp_error 函数中添加抗重放区域错误返回类型，其代码如图 10 所示。

```
log_sp_error (enum ERRORS error)
#else /* ANSI */
void
log_sp_error (error)
    enum ERRORS error;
#endif /* ANSI */
{
#ifdef LASHAM
  switch (error)
    {
    case ANTI_REPLAY_WRONG:
      printf("Anti_Replay is wrong. \n");
      break;
    case MEM_ALLOC_FAILED:
      printf ("Memory allocation failed. \n");
      break;
    case DATA_OVERFLOW:
      printf ("Data overflow. \n");
      break;
```

图 10 抗重放功能出错处理

至此，在上述已有 SCPS-SP 源代码的基础上，按照第 2 节提出的改进的 SCPS-SP 协议的设计思路，分别在 SCPS_RI 程序上进行了修改，并且重新完成了编译，即在已有的 SCPS-SP 的基础上增加了一种可选的增强型的安全协议 M-SCPS-SP。

3.3 仿真实验

为验证所提 M-SCPS-SP 的有效性，基于开源 SCPS_RI 平台，以铱星系统作为空间通信应用场景。铱星系统的主要参数如表 2 所列[14]。

表 2 铱星系统的主要参数

名称	数值
高度/km	780
轨道周期/s	6026.9
轨道面	6
每个轨道卫星数	11
倾斜度	86.4
同轨内卫星隔离度/°	31.6
每个卫星的星间链路数	4
ISL 带宽/Mbps	25
上下行带宽/Mbps	1.5
越缝 ISL	无

仿真的网络拓扑如图 11 所示。

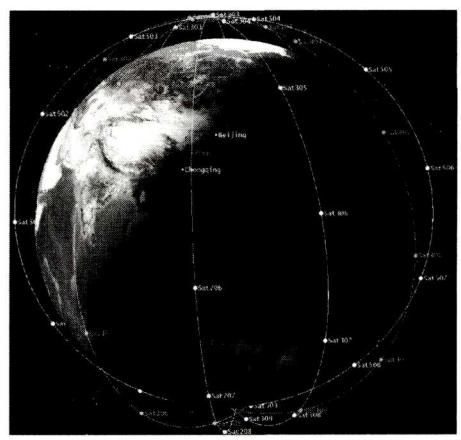

图 11 卫星通信网络仿真拓扑

如图 11 所示，在地球表面设置了两个铱星终端，分别在重庆 A(N 29.35°，E 106.33°)和北京 B(N39.92°，E 116.46°)，A 为发送端，B 为接收端，两个终端不能直接通过地面网络通信，必须通过星地、星际链路经过铱星系统完成数据通信，路由协议采用最短路径算法。同时，在西安(N34.27°，E188.88°)放置了一个地基干扰源，可定期向中继的铱星进行重放攻击。

如图 12 所示，A 和 B 通信的步骤如下：

步骤 100：首先建立 SA，A 向 B 发送一系列安全等级标签，B 接收后选择其中一种，假设 B 选择的是(1100 0001)并反馈给 A，A 根据反馈回来的安全等级标签可以得知将要提供的服务(认证、完整、加密)和采用的算法(AES，MD5)，然后产生相应的密钥、初始向量(IV)等发送给 B。

步骤 101：A 向 B 发起通信，检测是否启用 SCPS-SP 保护，如启用，则进入步骤 102，否则直接将报文传输到下一层。

步骤 102：根据安全参数索引(SPI)查询安全联盟数据库(SADB)来查找相应的 SA，若找到则根据 SA 的参数对用户

数据进行封装，进入步骤 103，若未找到则调用密钥管理协议(KM-P)进行 SA 协商。

步骤 103：1)填充首部信息，如 IV、安全选项标识符(0001 1111)、安全等级标签(1100 0001)、封装地址域(源地址＋目的地址)、抗重放域(序列号)；2)加密数据，由 SA 的参数可知本次通信确定使用的加密算法，然后根据加密算法和密钥 IV 等加密数据；3)计算 ICV；4)将封装好的 S-PDU 传输到空间信道。

步骤 104：B 接收 A 发送过来的 S-PDU，首先根据 SPI 查找相应的 SA，若找到 SA 则进入步骤 105，否则直接丢弃 S-PDU。

步骤 105：解封装 S-PDU，检查序列号，与 SA 中的序列号相比较，相同则接收报文，然后解密数据；不同则说明信息是重放信息，将其丢弃。

步骤 106：检查封装地址，对通信双方的身份进行认证，身份验证正确再检查完整性校验值，首先计算接收到的数据报的 ICV，与数据报尾部封装的 ICV 值比较，若相同则说明数据是完整的，进入步骤 107；若不同则说明数据不完整，将其丢弃。

步骤 107：将解封装出来的数据报(PDU)传送到上一层。

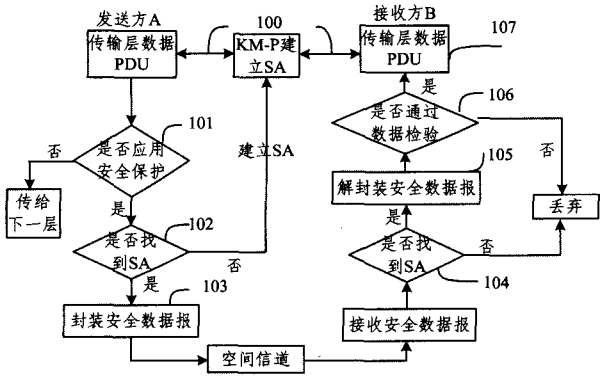

图 12　A,B 通信流程示意图

仿真传输的数据业务类型有文件、图像，对应表 1 中的 C1 和 B1 安全等级，仿真总时间为 600s，前 300s 传输的是文件，后 300s 传输的是图像。星地链路上/下行的带宽均为 1.5Mbps，星间链路的带宽为 25Mbps。传输文件时，报文大小为 1000 字节，其传输基于 SCPS-TP[19]；图像数据的传输基于无连接协议，发送端原始数据的发送率为 1.2Mbps。在仿真中每隔 30s 统计一次平均吞吐量，共统计 20 次，采用 MATLAB 作图，SCPS-SP 和 M-SCPS-SP 的有效吞吐量仿真结果如图 13 所示。此处定义有效吞吐量为单位时间内接收端接收到来自发送端的原始而未经重放攻击篡改的数据。

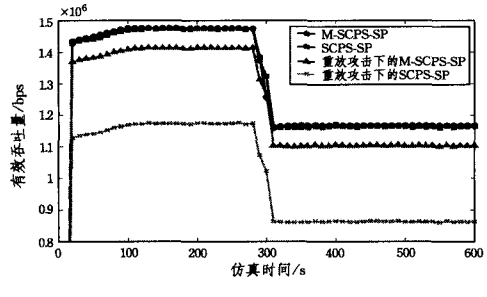

图 13　M-SCPS-SP 和 SCPS-SP 有效吞吐量的仿真对比

如图 13 所示，SCPS-SP 在传输数据的过程中一般按照默认的加密(DES)和认证算法(MD5)进行实施，显然灵活度不够高，而 M-SCPS-SP 能对不同业务进行认证和加密算法的区分，在本实验中对文件业务提供具有认证、加密和完整的 C1 服务，采用 AES 和 MD5 算法；对普通数据提供具有加密的 B1 服务，采用 AES 算法。从实际传输效率来看，不管在前 300s 进行文件传输还是在后 300s 进行普通数据传输，采用不同安全等级的 M-SCPS-SP 具有更好的自适应性，相较于 SCPS-SP，在没有重放攻击的影响下，报文在收发两端对数据的加密、认证处理时间略有增加，但对吞吐量几乎没有影响。

但是在重放攻击的影响下，传统的 SCPS-SP 由于不具备抗重放功能，报文在中继节点处被地基干扰源所攻击篡改，其有效吞吐量性能下降明显，较没有重放攻击条件下的有效吞吐量的性能下降约 20%；而 M-SCPS-SP 不仅在加密、认证和完整性方面的性能得到增强，同时还有一套抗重放的机制，可有效减少第三方恶意的重放攻击，其有效吞吐量较没有被攻击之前下降幅度不到 5%。

结束语　本文提出一种改进的 SCPS-SP，该协议在 SCPS-SP 的基础上新增两个功能：安全等级划分和抗重放功能。同时，在开源 SCPS 源代码的基础上修改、编译实现了所提的改进协议。最后通过仿真实验验证了本文所提改进安全协议的有效性。

参 考 文 献

[1] LIAO Y. Studies of space data communication transport protocol in unified information networks[D]. Chongqing: Chongqing University, 2014. (in Chinese)
廖勇. 统一信息网空间数据通信传输协议研究[D]. 重庆：重庆大学，2014.

[2] LI D R, SHEN X, GONG J Y, et al. On construction of China's space information network[J]. Geomatics and Information Science of Wuhan University, 2015, 40(6): 711-715, 716. (in Chinese)
李德仁，沈欣，龚建雅，等. 论我国空间信息网络的构建[J]. 武汉大学学报(信息科学版)，2015，40(6)：711-715，716.

[3] FEI X F. Research on the security of space communication protocols[D]. Zhengzhou: PLA Information Engineering University, 2008. (in Chinese)
费晓飞. 空间通信协议安全性研究[D]. 郑州：解放军信息工程大学，2008.

[4] CAUBET J, MUÑOZ J L, ALINS J, et al. Deploying Internet protocol security in satellite networks using transmission control protocol performance enhancing proxies[J]. International Journal of Satellite Communications & Networking, 2013, 31(2): 51-76.

[5] CCSDS[EB/OL]. [2016-03-31]. http://public.ccsds.org.

[6] CCSDS. Space communications protocol specification (SCPS)-security protocol: CCSDS 713.5-B-1, Blue Book[S]. 1999.

[7] LIU Y, DONG Y, LI Z H. Discussion of data security about space-earth all-in-one networking and analysis of CCSDS SCPS [J]. Chinese Space Science and Technology, 2004, 24(1): 31-36. (in Chinese)
刘泳，董勇，李泽慧. 空间通信协议分析与一体化网络安全问题

探讨[J]. 中国空间科学技术,2004,24(1):31-36.

[8] LI J Y. The design and implementation of SCPS-SP/IPSec protocol conversion[D]. Harbin: Heilongjiang University, 2013. (in Chinese)
李敬媛. SCPS-SP/IPSec 协议转换的方案设计与实现[D]. 哈尔滨:黑龙江大学,2013.

[9] YANG Y H. Research on the authenticated encryption technology in CCSDS[D]. Shenyang: Shenyang Aerospace University, 2011. (in Chinese)
杨亚辉. CCSDS 认证加密技术研究[D]. 沈阳:沈阳航空航天大学,2011.

[10] LI H X. Research on data encryption/decryption strategy of CCSDS space communication system[D]. Shenyang: Shenyang Ligong University, 2011. (in Chinese)
李海霞. CCSDS 空间通信系统中数据加密/解密策略研究[D]. 沈阳:沈阳理工大学,2011.

[11] LI H, FAN X X, MI J N, et al. Analysis of security technologies in integrated space-air-ground networks[J]. Journal of CAEIT, 2014,9(6):592-597. (in Chinese)
李华,范鑫鑫,秘建宁,等. 空天地一体化网络安全防护技术分析[J]. 中国电子科学研究院学报,2014,9(6):592-597.

[12] XU W, WANG T, LI L. The multi-level self-adaptive space communication security protocol[C]// Proceedings of the International Conference on Information Technology, Computer Engineering and Management Sciences. 2011:246-249.

[13] GONG C Q, YANG Y H. Research on the authenticated encryption technology in CCSDS[C]// Proceedings of the International Conference on Computational Intelligence and Industrial Application. 2010:321-329.

[14] AKYILDIZ I F, AKAN O B, CHEN C, et al. The state of the art in interplanetary Internet[J]. IEEE Communications Magazine, 2004,42(7):108-118.

[15] LIU J F, ZHOU M T. Research and taxonomy of replay attacks on security protocol[J]. Computer Application Research, 2007, 24(3):135-139. (in Chinese)
刘家芬,周明天. 对安全协议重放攻击的分类研究[J]. 计算机应用研究,2007,24(3):135-139.

[16] 廖勇,郭修琼. 一种 SCPS-SP 多安全等级及抗重放功能的设计方法:201510489336.3[P]. 2015-08-11

[17] SCPS Reference Implementation [EB/OL]. [2016-07-25]. http://www.openchannelfoundation.org.

[18] NS2[EB/OL]. [2016-07-25]. http://www.isi.edu/nsnam/ns.

[19] CCSDS. Space communications protocol specification(SCPS)-transport protocol: CCSDS 714.0-B-2, Blue Book[S]. 2006.

(上接第 138 页)

[7] CHALLITA N, BAKHACHE B. Enhancement of S-AES using chaos for the support of biomedical applications[C]// International Conference on Advances in Biomedical Engineering. IEEE, 2013:175-178.

[8] PRADHAN C, BISOI A K. Chaotic Variations of AES Algorithm[J]. International Journal of Chaos, Control, Modelling and Simulation, 2013, 2(2):19-25.

[9] DAEMEN J, RIJMEN V. AES Proposal: The Rijndael Block Cipher (V2)[EB/OL]. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf, 1999.

[10] ZHAO Y, LI X M. The Application of Compound Chaotic Encryption Algorithm in Power System Information Security[C]// The 26th Academic Annual Meeting of Chinese Colleges major in Power System Automation and Chinese Institute Of Electrical Engineering Power System Specialized Committee. 2010: 193-193. (in Chinese)
赵云,李晓明. 复合混沌加密算法在电力系统信息安全中的应用[C]//中国高等学校电力系统及其自动化专业第二十六届学术年会暨中国电机工程学会电力系统专业委员会 2010 年年会. 2010:193-193.

[11] CAI J, CHEN X, XIANG X D. Substitution-Permutation Network Structured Image Encryption Algorithm Based on Chaotic Map[J]. Computer Science, 2014, 41(9):158-164. (in Chinese)
蔡俊,陈昕,向旭东. 一种基于混沌的代换-置换结构图像加密算法[J]. 计算机科学,2014,41(9):158-164.

[12] AN Y M, HAO R F, ZHANG Z X, et al. The Generation and Analysis of Pseudo Chaotic Sequences Based on Tent Map[J]. Journal of Taiyuan University of Technology, 2008(S1):71-74. (in Chinese)
闫永梅,郝润芳,张朝霞,等. 基于 Tent 映射的伪混沌序列的产生和分析[J]. 太原理工大学学报,2008(S1):71-74.

[13] JIA K J, LIANG J, DU T H, et al. Chaotic Encryption Algorithm Based on Logistic Map Applied in Remote Monitoring of Transportation[J]. Control and Instruments in Chemical Industry, 2012, 39(12):96-100. (in Chinese)
贾科进,梁杰,杜太行,等. 运输远程监控中基于 Logistic 映射的混沌加密算法[J]. 化工自动化及仪表,2012,39(12):96-100.

[14] YU J F, YANG W G, LU W T, et al. Analysis of the Full Mapping Logistic Sequence's Generation and Performance[J]. Telecommunication Engineering, 2013(2):140-145. (in Chinese)
余金峰,杨文革,路伟涛,等. 满映射 Logistic 数字混沌序列的产生及性能分析[J]. 电讯技术,2013(2):140-145.

[15] STANDARDSTECHNOLOGY N I O. Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules[J/OL]. http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf, 2004.

[16] ELBADAWY A M, MOKHTAR A, EL-MASRY W A, et al. A new chaos Advanced Encryption Standard (AES) algorithm for data security[C]//2010 International Conference on Signals and Electronic Systems (ICSES). IEEE, 2010:405-408.

[17] MUHAYA F B, USAMA M, KHAN M K. Modified AES Using Chaotic Key Generator for Satellite Imagery Encryption[C]// International Conference on Emerging Intelligent Computing Technology and Applications. Springer-Verlag, 2009:6-23.

[18] YUAN K, HAN Z, LI Z. An Improved AES Algorithm Based on Chaos[C]// International Conference on Multimedia Information Networking and Security. IEEE, 2009:326-329.