卫星网络加密算法安全性分析与攻击建模

吴 杨,矫文成,潘艳辉,李 华
(军械工程学院 计算机工程系,河北 石家庄 050003)

摘 要:鉴于加密算法在卫星网络中的重要作用,评估加密算法在卫星网络中实际应用的安全性具有现实意义。针对加密算法面临的安全威胁,结合卫星网络的特点,对加密算法在卫星网络中的安全性进行了分析;建立了卫星网络加密算法差分故障攻击模型,并对模型的合理性及攻击实现过程进行了阐述。建立的卫星网络加密算法差分故障攻击模型对于在地面网络环境构建卫星网络加密算法攻击实验平台具有指导意义。同时,为加密算法在卫星网络中的安全应用提供了一定的思路。

关键词:卫星网络;加密算法;安全威胁;攻击模型
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)06-0140-05

Analysis of Cipher Security and Cipher Attack Modeling in Satellite Network

WU Yang, JIAO Wen-cheng, PAN Yan-hui, LI Hua
(Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: Whereas important functions of cipher in satellite network, research on cipher security in satellite network has realism sense of evaluating cipher security in satellite network. Aiming at security threats of cipher, analyze cipher security in satellite network according to characters of satellite network; Build up a differential fault attack model to cipher in satellite network and analyze rationality of the model and the attack process. The attack model presented has directive sense of building up experimental platform in terrestrial network. At the same time, it provides ideas to ensuring cipher application security in satellite network.

Key words: satellite network; cipher; security threats; attack model

0 引 言

在地面网络承载能力趋于饱和趋势下,卫星通信在通信领域的重要性也越来越明显。随着卫星通信系统的广泛应用,卫星通信的安全问题变得日益突出。卫星网络的安全通信,离不开密码学及认证技术的支撑,其安全性很大程度上依赖于现有的加密算法及认证技术。然而,现有的多数加密算法正面临着主动攻击及被动攻击的威胁。以主动攻击中的差分故障攻击为例,研究者利用差分故障攻击分别提出了对ECC[1]、3DES[2]、AES[3]、ARIA[4]、Camellia[5]、SMS4[6]、RC4[7]、Trivium[8]等算法的攻击手段。研究表明,任何加密算法攻击的实现,都离不开具体的加密环境。研究加密算法在卫星网络中的安全性,对评估加密算法在实际卫星网络应用环境中的安全性具有现实意义。同时,也为加密算法在卫星网络中的安全应用提供一定思路。

文中阐述了加密算法在卫星网络中的典型应用;介绍了现有加密算法面临的安全威胁;结合卫星网络自身特点及加密算法在卫星网络中的实际应用,对卫星网络中的加密算法安全性进行了分析;结合卫星网络特点及差分故障攻击技术,建立了卫星网络加密算法差分故障攻击模型,并对模型的合理性及攻击实现过程进行了分析。

1 加密算法在卫星网络中的典型应用

1.1 数据加解密

密码技术是实现网络信息安全的核心技术,是数据保护的重要工具之一。通过加密变换,将可读的文件变换成不可理解的编码,从而起到保护信息和数据的作用。加密算法则是上述机制的具体承担者。图1为形式化的数据加解密过程。

这里定义加密函数 $E(m,k_e)$ 和解密函数 $D(c,$

收稿日期:2010-11-16;**修回日期**:2011-03-05
基金项目:国家自然科学基金资助项目(60772082);河北省自然科学基金数学研究专项资助项目(08M010)
作者简介:吴 杨(1985-),男,硕士生,主要研究方向为网络安全与密码学;矫文成,副教授,硕士生导师,主要研究方向为信息安全与软件工程。

k_d),其中k_e和k_d分别为加密密钥和解密密钥。若$k_e = k_d$,则该加密算法为在加密和解密过程中使用相同密钥的对称加密算法;若$k_e \neq k_d$,则该密码算法为在数据的加密和解密过程中使用不同密钥的非对称加密算法。

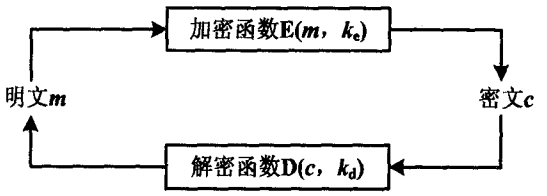

图1　密码系统加解密简化流程图

卫星通信采用广播方式,面临主动攻击及被动攻击的威胁[9]。在上下行链路以及星间链路上存在被动窃听的威胁,这种威胁不会对网络中的信息进行任何修改,更不会影响网络的操作与状态,一般不易察觉,但可能造成严重的信息泄密。针对卫星通信链路上的被动窃听威胁,最有效的方式是对卫星链路通信数据进行加密,即使攻击者获得了加密密文也无法获得原始通信数据内容。加密算法的安全性,将直接影响到卫星网络通信数据的安全。

1.2　认证实现

卫星通信采用广播方式,面临主动攻击及被动攻击的威胁[9]。在卫星网络主动攻击方式中,攻击者将试图截获卫星网络通信链路数据,并破坏数据的完整性,最典型的方式是篡改数据。主动攻击有重放攻击、拒绝服务攻击等方式。

卫星网络的开放性特点,使其面临着严重的主动攻击威胁,有效防御手段是引入认证机制,认证同样建立在密码学基础上。因此,卫星网络实体间认证的实现,同样离不开密码学的支撑。

本节介绍了加密算法在卫星网络通信中抵御被动攻击及主动攻击的重要作用。加密算法在卫星网络中的安全,直接关系到卫星网络通信的安全。下面将分析加密算法安全性,并对卫星网络环境下的加密算法安全性进行分析研究。

2　加密算法面临的安全威胁

加密算法攻击技术已成为密码学的研究热点,根据对计算过程的控制能力来分,可以将其分为两大类:主动攻击和被动攻击。主动攻击主要通过物理手段主动修改密码设备加解密实现中的内部状态,得到一些额外的输出信息,故障攻击最为常见。被动攻击主要采集密码设备加解密实现中内部状态泄露的物理效应信息,如:时间、功耗、电磁、频率、声音,并进行密钥分析,通常称为旁路攻击(Side Channel Attack:SCA)。下面将分别对加密算法的主动攻击和被动攻击进行阐述。

2.1　主动攻击

故障攻击是最为常见的主动攻击方式,攻击者可通过辐射、X光、微探测或切断线路等方法在防篡改芯片中引入故障,从而导致一些密钥信息从芯片中泄露。差分故障攻击方法结合了故障注入与差分分析方法可实现对分组密码及流密码的攻击,引言部分已对相关差分故障攻击成果进行了介绍。本节将介绍针对采用S盒的分组密码差分故障攻击思想及原理。

大多数分组密码为增强其抗线性和差分分析能力,在实现过程中采用了S盒。采用S盒的分组密码算法面临着差分故障攻击的严重威胁。对于攻击者而言,在加密过程中某轮导入随机故障f。一般,攻击者可以获得正确密文和出错密文,从而获得密文差分f',且满足[5]:

$$S[a] \oplus S[a+f] = f' \tag{1}$$

通过分析,攻击者可获得S盒输入索引a,而该值与扩展密钥紧密相关,此时攻击者结合密文信息可恢复相应的轮密钥。获得足够数量的轮密钥后,结合密钥扩展算法,即可恢复初始密钥值。针对S盒的分组密码差分故障攻击可概括为:故障导入、轮密钥推导、初始密钥推导。

2.2　被动攻击

(1) Cache攻击。

高速缓存Cache主要用于解决CPU与主存之间速度不匹配的问题。由Cache访问命中和失效会带来时间和能量消耗差异,而分组密码在加密过程中由于使用了S盒进行查表操作访问Cache,其Cache访问特征信息可通过时间或能量消耗特征信息泄露出来,可以说,Cache为密码加密提供了Cache访问信息泄露源。为提高算法非线性度和软件执行效率,现代分组密码大都使用S盒查表访问Cache。但是通过Cache攻击可采集到分组密码加解密过程中泄露的访问信息,而这些访问信息同查找S盒的索引、明文、密文、加密密钥有紧密关系。随着高精度和复杂精密测试计量仪器及技术的发展,通过Cache泄露的时间和能量消耗差异信息的精确采集已经具备实际可行性。加密设备中Cache的引入,为攻击者获得加密过程中的相关信息提供了隐通道,Cache攻击的威胁性越来越受到重视。

(2)功耗分析攻击。

功耗分析攻击主要利用密码设备在进行密码运算时产生的功耗信息,推导出运算中的秘密参量。根据功耗分析方法的不同[10],可以将其分为简单功耗分析(SPA)、差分功耗分析(DPA)和相关功耗分析(CPA)。

功耗分析攻击其信息来源于设备在加解密过程中寄存器中 0 和 1 的翻转所产生的电流功耗变化。攻击者利用功耗信息采集设备,在加密设备运行过程中,采集相关功耗信息,利用 SPA、DPA 及 CPA 方法,恢复完整密钥。

(3)电磁分析攻击。

电磁辐射泄漏可能是最早被关注的旁路攻击形式。在美国安全局最近解密的 TEMPEST 文档中,调查研究了不同辐射的威胁,其中电磁辐射是很重要的一类。电磁分析攻击主要通过测量密码芯片在运算期间发射的电磁信号,研究电磁场与内部处理数据之间的相关性而获取内部秘密参量。电磁泄漏攻击有简单电磁分析(SEMA)和差分电磁分析(DEMA)以及应用多旁路以提高攻击的效率。文献[11,12]分别在硬件平台上实现了对 ARIA 和 AES 电磁分析攻击。

综上所述,对加密算法的主动攻击成功与否很大程度上取决于能否通过物理手段主动修改加密设备加解密过程中的内部状态,得到攻击者期待的一些额外输出信息。对于被动攻击而言,在不影响加密算法执行的基础上,采集到加密设备运行过程中泄露的有用旁路信息,并结合相关统计分析方法,是实现被动攻击的前提。

3 卫星网络加密算法的安全性分析

卫星网络及其设备同传统的地面网络存在较大的差异。因此,加密算法在地面网络与卫星网络所面临的安全问题也存在很大差异。研究加密算法在卫星网络中的安全性之前,本节先对卫星网络的结构进行阐述。图 2 为空地一体的卫星网络组成图。所有的地面设备均可表示为地面端系统,空中卫星表示为卫星节点。

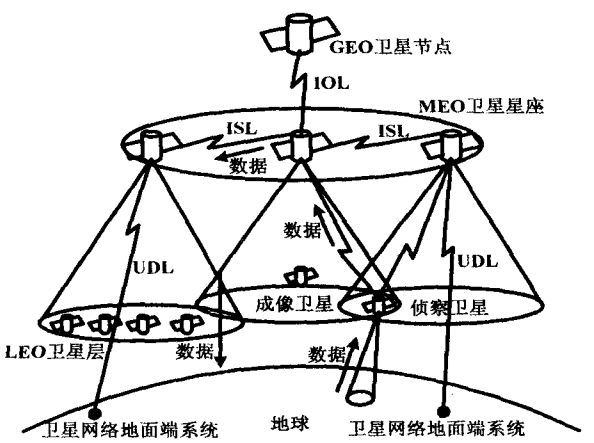

图 2 多层卫星网络组成图

由图 2 可知,卫星网络中加密算法执行设备主要集中于卫星节点及地面端系统。下面将分析研究第 3 节中加密算法常见攻击方法在卫星节点及地面端系统的有效性。

3.1 卫星节点的加密算法安全性分析

3.1.1 主动攻击有效性分析

现有针对加密算法的主动攻击主要以差分故障攻击为主,其攻击有效性在于满足:

(1)攻击者需近距离接触加密设备。

(2)在特定时刻向加密设备注入故障。

(3)在加密设备特定位置注入故障。

(4)故障注入宽度在可控范围内。

卫星节点的空间分布特性及动态性,使得差分故障攻击故障注入面临的问题有:

(1)卫星轨道高度较高,攻击者无法近距离接触卫星节点上的加密设备。

(2)星地链路长传输时延特性,使攻击者无法正确把握故障注入时刻。

(3)卫星节点的动态特性,使攻击者无法在卫星节点加密设备的特定位置实现故障的精确注入。

以上分析了地面攻击者对卫星节点加密设备实现成功故障注入所面临的问题。卫星节点的空间分布特性,为卫星节点上的加密算法抵抗来自于地面的差分故障攻击提供了天然的保护屏障。因此,在现有故障注入技术条件下,攻击者要实现针对卫星节点上的加密算法差分故障攻击是困难的。

3.1.2 被动攻击有效性分析

(1)Cache 攻击有效性分析。

第 3 节对 Cache 攻击原理进行了介绍,其攻击有效性关键在于满足:以时间或以能量为单位的信息的精确采集。然而,对未使用 Cache 的卫星节点,该方法将失效。即便卫星节点加密设备使用了 Cache,对于攻击者而言很难做到在卫星节点对采集到的信息进行分析,星地链路数据传输的高误码率,也对 Cache 攻击精确信息的采集提出了挑战。因此,在现有技术条件下,实现针对卫星节点加密算法的 Cache 攻击是困难的。

(2)功耗分析攻击有效性分析。

攻击者在对加密算法实施功耗分析攻击过程中,需要监测加密设备在运行过程中的功耗变化情况,一般通过监测加密设备运行过程中的电流变化,并通过相应的相关性分析方法,获得加密算法密钥。由于卫星节点的空间分布特性,攻击者很难实现对卫星节点加密设备功耗信息的获取。因此,卫星节点的空间分布特性,同样为卫星节点上的加密算法抵御功耗分析攻击提供了天然的保护屏障。

(3)电磁分析攻击有效性分析。

攻击者在对加密算法实施电磁分析攻击过程中,

需采集加密设备在运行过程中的电磁泄漏信息。通常通过采用高灵敏度探头,实现对有限电磁信息的采集。电磁分析攻击的成功率,与电磁信息采集的精度密切相关。

同样,卫星运行轨道较高,其星上加密设备运行释放的电磁强度有限,同时结合空间电磁环境的复杂性,要实现精确采集星上加密设备泄漏的电磁信息,其难度可想而知。

3.2　地面端系统的加密算法安全性分析

3.2.1　主动攻击有效性分析

地面端系统与卫星节点相比,其地理位置相对固定,攻击者可实现近距离接触地面端系统加密设备;利用现有的故障注入设备,攻击者能够实现在其加密设备运行的特定时刻、特定位置注入故障,并控制故障注入宽度。地面端系统与卫星节点的差异性,使得攻击者对地面端系统的加密算法进行差分故障攻击成为可能。

3.2.2　被动攻击有效性分析

对于被动攻击而言,多数情况下,一旦攻击者能够在有效的距离内接触加密设备,攻击者便能通过相应设备及技术获取加密设备运行过程中泄漏出的功耗、电磁等信息。在获得相关旁路信息基础上,通过统计分析方法,获取加密算法密钥。地面端系统,很大程度上为加密算法攻击者提供了便利的攻击条件。

4　卫星网络加密算法攻击建模

4.1　卫星网络加密算法差分故障攻击建模

结合加密算法面临的安全威胁及卫星网络特点,文中提出的卫星网络加密算法差分故障攻击模型如图3所示。

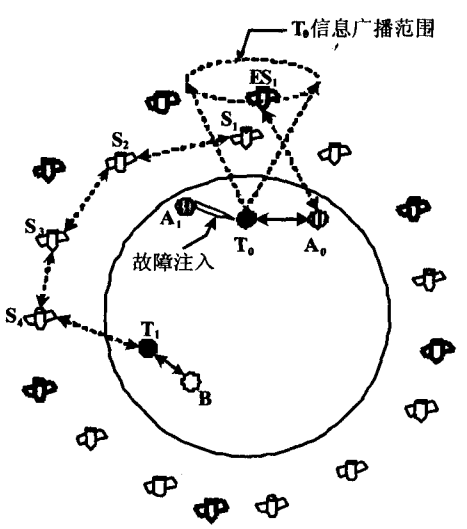

图3　卫星网络加密算法差分故障攻击模型图

图3为根据加密算法差分故障攻击原理及卫星网络数据通信特点构建的攻击模型图。地面合法用户之间可通过系统建立相互通信。系统建立会话通信信道后采用执行效率较高的对称加密算法加密会话信息。在会话密钥更新周期内,会话密钥保持不变。实际卫星网络中存在大量的间谍卫星节点,地面端系统和卫星节点均采用广播通信方式进行数据传输,处于广播范围内的间谍卫星节点能够获取广播的加密信息,并将其传递给攻击者。攻击者可利用收到的加密信息,结合加密算法攻击技术,获取加密算法密钥。

4.2　卫星网络加密算法差分故障攻击实现过程

(1) A_0、B 会话建立。

为降低卫星链路节点间会话密钥协商过程对卫星通信链路带宽占用率,确保实时通信质量,链路节点 T_0、S_1、S_2、S_3、S_4、T_1 间的会话密钥在会话密钥更新周期内保持不变。拥有合法身份的攻击者 A_0 向地面端系统 T_0 发起与地面用户 B 的通信申请。T_0 接受攻击者 A_0 的合法申请,通过卫星节点 S_1、S_2、S_3、S_4 和地面端系统 T_1 为用户 A_0 与 B 建立通信链路。T_0 与 S_1 间会话密钥为 K_{TS},A_0 与 T_0 间会话密钥为 K_{AT}。

(2) A_0 获取 T_0 广播的正确密文。

会话建立后,A_0 使用会话密钥 K_{AT} 加密明文 m,发送密文 C 到 T_0;T_0 由 C 和 K_{AT} 解密得到 m 后,使用会话密钥 K_{TS} 加密 m,以广播形式发送密文 C_1 到卫星节点 S_1,间谍卫星节点 ES_1 处于 T_0 信息广播范围内也将收到密文 C_1;ES_1 收到 C_1 后,发送 C_1 到 A_0。

(3) A_0 获取 T_0 广播的错误密文。

A_0 使用会话密钥 K_{AT} 加密相同明文 m,发送密文 C 到 T_0;T_0 由 C 和 K_{AT} 解密得到 m 后,将使用会话密钥 K_{TS} 加密 m,A_1 在 T_0 对 m 加密过程中的特定时刻特定位置导入随机故障 f,导致 T_0 产生错误密文 C^*;间谍卫星节点 ES_1 收到 T_0 广播的错误密文 C^* 后,将 C^* 发送给 A_0。

(4) A_0 分析获取 K_{TS}。

在相同明文条件下,重复执行(3)过程,A_0 将获得足够恢复密钥 K_{TS} 的错误密文集合。结合过程(2)中获取的正确密文 C,采用差分故障攻击方法,多数情况下 A_0 可获取密钥 K_{TS}。

4.3　攻击可行性分析

卫星网络采用广播方式进行数据传递,处于节点有效广播范围内的卫星节点和地面端系统能够获得广播的数据信息,这也为泄露卫星网络加密信息提供了通道。攻击者一旦在加密设备成功注入故障,便能通过间谍卫星节点获取错误密文信息。攻击者利用采集到的密文信息结合差分故障攻击方法,可对卫星网络加密算法安全构成严重威胁。提出的攻击模型的可行

性主要体现在以下几方面：

(1)在现有故障注入技术条件下，攻击者在地面端系统更易实现故障成功注入。

(2)卫星节点计算资源有限，在节点会话建立后，一般采用执行效率较高的对称加密算法进行会话信息加密。会话密钥在密钥更新周期内保持不变，攻击者可在会话密钥更新周期内完成攻击。

(3)在卫星网络开放环境下，攻击者利用间谍卫星节点能够获取加密过程中的密文信息，为加密算法的攻击提供了可靠的数据源。

(4)随着差分故障攻击技术的不断发展，攻击者利用较少的攻击样本即可实现对加密算法的攻击，攻击效率大大提高，确保在卫星节点会话密钥更新周期内完成攻击。

5 结束语

研究了现有加密算法的主要攻击手段，分析了加密算法在卫星网络中实现安全性。结合卫星网络自身特点和加密算法攻击技术，对卫星节点及地面端系统的加密算法抗攻击能力进行了分析研究。在此基础上，设计了针对卫星网络加密算法的差分故障攻击模型，并对模型的合理性进行了说明。文中提出的卫星网络加密算法攻击模型，为在地面网络环境中构建卫星网络加密算法攻击仿真平台提供了一定思路。

参考文献：

[1] Biehl I, Meyer B, Muller V. Differential fault analysis on elliptic curve cryptosystems[C]//CRYPTO 2000. [s. l.]: Springer, 2000: 131-146.

[2] Hemme L. A differential fault attack against early rounds of (Triple-) DES[C]//CHES 2004. [s. l.]: Springer, 2004: 254-267.

[3] Piret G, Quisquater J J. A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad[C]// CHES 2003. [s. l.]: Springer, 2003: 77-88.

[4] Li Wei, Gu Dawu, Li Juanru. Differential fault analysis on the ARIA algorithm [J]. Information Sciences, 2008, 178 (19): 3727-3737.

[5] Zhao Xinjie, Wang Tao. An Improved Differential Fault Attack on Camellia [EB/OL]. 2009. http://eprint.iacr.org/2009/585.

[6] Zhang Lei, Wu Wenling. Differential fault analysis on SMS4 [J]. Chinese Journal of Computers, 2006, 29(9): 2596-2602.

[7] Hoch J J, Shamir A. Fault analysis of stream ciphers[C]// CHES 2004. [s. l.]: Springer, 2004: 240-253.

[8] Hojsik M, Rudolf B. Floating fault analysis of Trivium[C]// INDOCRYPT 2008. [s. l.]: Springer, 2008: 239 - 250.

[9] 陈 浩，谢永春，安红章. 星座系统安全防护技术研究[C]//保密通信与信息安全现状研讨会论文集. 出版地不详：出版者不详，2007：124-129.

[10] Kocher P, Jaffe J, Jun B. Differential power analysis[C]// CRYPTO 99. [s. l.]: [s. n.], 1999: 388-397.

[11] Kim C, Schläffer M, Moon S. Differential Side Channel Analysis Attacks on FPGA Implementations of ARIA [J]. ETRI Journal, 2008, 30(2): 315-325.

[12] Carlier V, Chabanne H, Dottax E, et al. Electromagnetic side channels of an FPGA implementation of AES[EB/OL]. 2004. http://eprint.iacr.org/.

(上接第 121 页)

ment System for Running HLA-based Simulation over the Grid [C]//Proceedings of the Sixth IEEE International Symposium on Distributed Simulation and Real Time Applications. USA: IEEE Computer Society Press, 2002.

[4] Yuan Zijing, Cai W, Low M Y H. Federate Migration in HLA-based Distributed Simulation[C]//Proceeding of International Conference on Computational Science. Poland: LNCS, 2004.

[5] Martin E, Magnus S, Moradi F, et al. Peer-to-Peer-Based Resource Management in Support of HLA-Based Distributed Simulations[J]. Simulation: Transactions of the Society for Modeling and Simulation (S0037-5497), 2004, 80(4): 181-190.

[6] 刘晓建，钟海荣，金士尧. 大规模联邦仿真中实体迁移及其时间同步研究(一)——实体迁移协议与实现[J]. 计算机研究与发展，2005(4)：711-715.

[7] 李 文，王 壮，胡卫东. 基于 HLA 分布式仿真系统中的负载平衡问题[J]. 计算机仿真，2004(12)：124-127.

[8] 孟小锋，慕晓强，高洪奎. 分布式仿真中的负载平衡技术[J]. 现代计算机，2001(5)：14-17.

[9] 胡小梅，翟正军. 协同虚拟环境中的主动动态负载平衡算法[J]. 计算机工程，2007，33(20)：104-106.

[10] 蒋翠清，杨善林，黄梯云，等. 基于 Agent 的动态负载均衡技术及仿真实现[J]. 微电子学与计算机，2005(10)：47-50.

[11] Tan G, Perssion A, Ayani R. HLA federate migration[C]// Proceedings of the 38th Annual Simulation Symposium. [s. l.]: [s. n.], 2005.

[12] IEEE. IEEE Std 1516-2000, IEEE standard for modeling and simulation (M&S) high level architecture (HLA) frame-work and rules[S]. Washington, D. C., USA: IEEE, 2000.

[13] IEEE. IEEE Std 1516-2000, IEEE standard for modeling and simulation (M&S) high level architecture (HLA) federate interface specification[S]. Los Alamitos, Cal., USA: IEEE Computer Society, 2003.