一种基于量子密码的卫星网络窃听攻击检测方法

黄 静[1] 席 博[1] 李 鹏[1] 张 帆[2] 赵新杰[3]
(61541部队 北京 100094)[1] (浙江大学信息与电子工程学院 杭州 310027)[2]
(北方电子设备研究所 北京 100191)[3]

摘 要 鉴于窃听攻击是对卫星网络实施各类高级攻击行为的基础,结合量子密码在未来卫星网络的应用趋势,提出了一种基于量子密码的卫星网络窃听攻击检测方法。首先,基于卫星网络节点在空间分布上的分层特点,构建了层簇式的卫星网络窃听攻击检测模型。实际检测过程中,相邻卫星节点检测到窃听攻击威胁时,将相关预警信息经簇首节点融合后通过安全信道传送到地面控制中心,随后再根据地面控制中心反馈的安全链路构建方案构建节点间的安全通信链路。最后,对方案的安全性及有效性进行了分析。相关成果可为进一步深入开展卫星网络安全防护技术研究打下一定的基础。

关键词 卫星网络,量子密码,窃听攻击,分簇
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.7.028

Method for Detecting Wiretapping Attack in Satellite Network Based on Quantum Cryptography

HUANG Jing[1] XI Bo[1] LI Peng[1] ZHANG Fan[2] ZHAO Xin-jie[3]
(System Control Department of No. 61541 Unit, Beijing 100094, China)[1]
(College of Information Science & Electrical Engineering, Zhejiang University, Hangzhou 310027, China)[2]
(The Institute of North Electronic Equipment, Beijing 100191, China)[3]

Abstract The wiretapping attack is the foundation of many advanced attacks on satellite network. Since quantum cryptography will be widely used in satellite network, a method for detecting wiretapping attack in satellite network based on quantum cryptography was proposed. Based on the spatial distributions of the satellites, a layered and clustering wiretapping attack detection model was presented at first. During the process of wiretapping attack detection, when the neighboring satellites detect a wiretapping attack in their channel, the corresponding alarm messages will be first sent to the head node of their cluster through secure channels. At the same time, the corresponding alarm messages will be further fused and sent to the ground control center by the head node. The secure link of two satellites will be established according to the secure link establishing scheme from the ground control center. Eventually, the security and the effectiveness of the proposed method were analyzed. The proposed method can lay a foundation for further research on the techniques of satellite network protection.

Keywords Satellite network, Quantum cryptography, Wiretapping attack, Clustering

1 引言

与传统计算机网络相比,卫星网络具有不受地理条件约束、信号覆盖范围广等优点,其安全性自然也备受关注。由于卫星网络往往被部署在整个空间区域,卫星网络的广播特性使得传输数据极易遭受窃听攻击。非授权用户在检测和截获其信号后可进行数据恢复和分析,甚至破译密码。然而,窃听者通常采取搭线窃听的方式获取网络数据,并不会对正常卫星网络通信用户之间的数据传输造成影响。现有卫星网络尚缺乏有效的窃听攻击检测方法。与一般的信息安全保障机制相比,量子密码是量子信息学的一个重要分支,主要以量子态作为信息单元来实现信息的有效传送[1]。这种依靠基本粒子的量子力学性质的通信技术,是一种理论上可被证明的绝对安全的保密通信技术。通过量子密码获得的密钥在理论上可以达到无条件安全性,对保密通信的意义重大,引发了世界各国研究量子通信的热潮。近年来,无论在理论上还是在实验上,量子密码技术都在不断取得重要突破。随着单光子探测等技术的不断发展,量子密码通信技术在全光网络和卫星通信等领域的应用潜力将会不断得到挖掘并成为现实。我国的"量子科学实验卫星"也将于2016年发射升空,实现首次的星

到稿日期:2015-06-26 返修日期:2015-10-15 本文受国家自然科学基金(61272491,61309021,61472357,61571063)资助。
黄 静(1983-),女,硕士,助理工程师,主要研究方向为卫星网络与信息安全,E-mail:huangjing2013@tsinghua.org.cn;席 博(1983-),男,硕士,工程师,主要研究方向为卫星网络与信息安全;李 鹏(1984-),男,硕士,工程师,主要研究方向为卫星网络与信息安全;张 帆(1978-),男,博士,讲师,主要研究方向为信息安全与密码学,E-mail:fanzhang@zju.edu.cn(通信作者);赵新杰(1986-),男,博士,工程师,主要研究方向为网络安全和密码学。

地传输，并计划在2030年建成全球的量子通信卫星网络[2]。为检测卫星网络中存在的窃听攻击行为，本文将根据经典量子力学中的海森堡测不准原理和量子不可克隆原理，结合卫星网络多层分布特点，提出一种基于量子密码的卫星网络窃听攻击检测方法。

本文第2节在分析卫星网络特点及面临的安全问题的基础上，论述了量子密码的基本原理；第3节首先阐述了基于量子密码的卫星网络窃听攻击检测模型，并对具体检测方案进行了论述；第4节对方案的安全性及可行性进行了分析；最后对全文工作进行了总结。

2 卫星网络安全挑战及量子密码分析

2.1 卫星网络安全挑战分析

卫星网络是一种通过星间链路和星地链路把不同轨道上不同种类的卫星或星座系统以及相应地面设施相连接而成的网络系统，是一体化、多功能、动态立体的信息交换与信息处理网络。根据功能不同，卫星网络可被划分为卫星通信网络、卫星导航网络、卫星遥感网络和卫星测控网络。卫星通信网络的功能是实现“3W”(WHO, WHERE, WHEN)与“3W”的通信；卫星导航网络的功能是为航天器和地面目标提供高精度定位、测速和定时；卫星遥测网的功能是实现对目标的精确识别与动态监测、信号的截获与反侦察等；卫星测控网的功能是实现对目标航天器的测控。目前，针对卫星网络的研究多基于假设的理想安全环境，以提高数据传输效率和提升网络性能为目标，集中在卫星星座设计、路由与传输控制等方面；在应对恶意攻击的防御、检测等安全机制方面的研究相对较少，研究力度、深度不够。下面给出卫星网络的特点，并分析其在安全性方面存在的主要问题。

(1)动态的网络拓扑带来的安全挑战

卫星节点的高速运动导致节点间的邻居连接状态不断改变，动态节点的移动、加入或离开，无线发送功率的变化和无线信道的相互干扰等，都会引起网络拓扑结构的变化[3,4]。拓扑结构的时变性及卫星网络的开放特性使得网络节点中极易存在大量的非授权节点，从而受到节点假冒、信息篡改及窃听攻击威胁。

(2)链路传输距离远、时延长带来的安全挑战

卫星网络的无线链路距离较长，且会随着节点位置的改变而出现较大幅度的变化。当攻击者对网络实施通信干扰时，如消息重放、协议头地址篡改、散布虚假路由信息，或者向主要通信节点发送虚假信息等，极易造成系统阻塞甚至瘫痪。在这种条件下，如何实施可有效抵御上述攻击的安全机制，对确保卫星网络的正常运行至关重要。

(3)多跳性通信机制带来的安全挑战

卫星网络的多跳路由主要由卫星网络中普通网络节点而不是专用的路由设备来完成。当网络中存在不可信节点或伪装的内部恶意节点时，转发的信息容易被攻击者所截获。在开放的网络环境下，如何应对此类攻击，也是需要重点关注和解决的问题。

通过分析卫星网络攻击实现过程可知，不论是节点假冒攻击、信息篡改攻击还是路由攻击，它们均建立在窃听攻击的基础上。不难理解的是，上述攻击实施的前提是需要通过窃听手段对目标卫星网络进行有效的侦察，并分析其存在的潜在安全漏洞，进而发起攻击。因此，在制定有效的防御策略过程中，如果能够及早发现攻击者的窃听行为，则可将可能的攻击扼杀在原始状态，最大限度地确保卫星网络安全。本文将卫星网络窃听攻击行为检测作为研究的重点，旨在为后续的卫星网络安全防护技术研究提供支持。

2.2 量子密码分析

量子密码学的概念于20世纪60年代末由Wiesner提出，而第一个量子密码协议BB84协议则是由Bennett在1984年提出，其标志着量子密码学的诞生[5]。量子密码从提出至今已有半个多世纪的时间，但受限于技术的发展，其发展一直比较缓慢。自1990年开始，随着人们对信息安全认识的不断加深，量子密码越来越受到重视，其发展速度较快。量子密码研究领域的主要内容包括量子密钥管理[6]、量子认证、量子安全协议、量子加密、量子信息理论、量子协议安全性分析[7]等。上述研究内容中，量子密钥管理是目前研究较多的技术，发展也较为成熟。为便于理解量子密钥管理与传统密钥管理的区别，下面简要介绍量子密钥管理的优势。

与一般的密钥管理方案相比，量子密钥管理采用光子的量子态来表示不同的信息，常见的方式是采用光子的偏振态表征传统信息中的比特0和比特1。量子密钥管理的安全性主要是基于量子不可克隆定理，即不存在真实的物理系统可以精确地复制未知的量子态。这就使得窃听者无法通过复制光子的量子态来获得信息且不被合法用户发现。在量子密钥管理过程中，一旦合法用户间存在窃听用户，其窃听行为一定会被正常用户所发现。文献[8-10]等均对量子密钥管理的基本实现过程进行了详细描述，这里不再赘述其基本原理和实现过程。

3 卫星网络窃听攻击检测方法

3.1 检测模型

当前，卫星网络主要采用微波方式进行通信，对于网络中存在的窃听行为，尚缺乏有效的检测机制。如前所述，随着量子密码通信技术的不断发展及其在信息安全领域的巨大优势，其必将在未来卫星网络中得到广泛的应用。因此，本文立足于未来卫星网络安全通信技术发展的需求及趋势，开展基于量子密码的卫星网络窃听攻击检测技术研究，为进一步的卫星网络安全防护技术研究奠定基础。在基于量子密码的卫星网络窃听攻击威胁检测过程中，主要采用如图1所示的层簇式检测模型。检测网络模型主要由处于不同轨道高度的卫星节点构成。图1中处于较低轨道高度的卫星节点构成检测模型的第一层($Layer_1$)；处于中间轨道高度的卫星节点构成第二层($Layer_2$)；处于较高轨道高度的卫星节点构成第三层($Layer_3$)，通常可选择地球同步卫星节点作为第三层中的节点，且与地面控制中心保持通信。下面给出具体的检测方案。

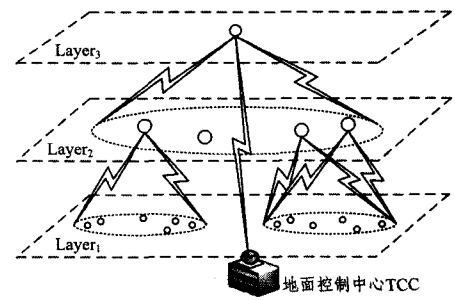

图1 卫星窃听攻击检测模型

3.2 检测方案的主要执行流程

基于图 1 所示的窃听攻击检测模型，提出的检测方法的主要执行流程如图 2 所示。

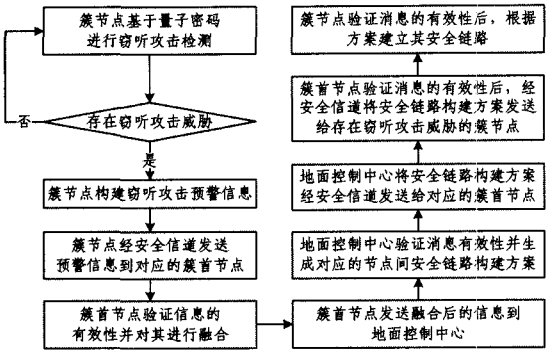

图 2 检测方案的主要执行流程

如图 2 所示，卫星网络中的簇节点通过量子密码通信机制检测到相邻节点间的信道存在窃听攻击威胁时，将构建对应的攻击预警，并将其发送到对应的簇首节点。窃听攻击预警信息得到簇首节点的验证后，将在 $Layer_2$ 或 $Layer_3$ 中的簇首节点进行融合，融合后的预警信息将通过安全信道发送给地面控制中心。地面控制中心收到并验证簇首节点发送消息的有效性后，结合卫星网络节点运动规律生成对应的卫星网络节点间的安全链路构建方案，并通过簇首节点将方案安全发送到对应的簇节点。簇节点间安全链路的构建将基于收到的安全链路构建方案。下面给出具体的检测方法。

3.3 具体检测方法

为便于对具体检测方案进行描述，首先给出与检测方法相关的定义。

定义 1 簇 $Cluster_{1i}$ 为由 $Layer_2$ 中的节点构成簇首、$Layer_1$ 中的节点构成一般簇成员的一级簇中的第 i 个簇。

定义 2 簇 $Cluster_{2i}$ 为由 $Layer_3$ 中的节点构成簇首、$Layer_2$ 中的节点构成一般簇成员的二级簇中的第 i 个簇。

定义 3 p_{kj}^1，p_{jk}^1 分别为一级簇 $Cluster_{1i}$ 中存在数据交互且相邻的两个普通簇成员节点 N_{1k} 与 N_{1j} 间量子通信的有效率。

$$\begin{cases} p_{kj}^1 = \dfrac{S_{kj}^1}{A_{kj}^1} \\ p_{jk}^1 = \dfrac{S_{jk}^1}{A_{jk}^1} \end{cases} \tag{1}$$

其中，S_{kj}^1 为节点 N_{1k} 统计的与节点 N_{1j} 间在一定时间内的通信过程中未遭窃听的通信次数，S_{jk}^1 为节点 N_{1j} 统计的与节点 N_{1k} 间在一定时间内的通信过程中未遭窃听的通信次数；A_{kj}^1 为节点 N_{1k} 统计的与节点 N_{1j} 间在一定时间内的通信总次数，A_{jk}^1 为节点 N_{1j} 统计的与节点 N_{1k} 间在一定时间内的通信总次数。

基于以上定义，提出的基于量子密码的卫星网络窃听攻击检测方法的主要步骤如下。

Step1 对于 $Layer_1$ 中彼此间存在数据交互的相邻节点 N_{1k}，N_{1j} 而言，当其通信次数 $A_{kj}^1 \geqslant M$ 且 $A_{jk}^1 \geqslant M$ 时，节点 N_{1k} 与 N_{1j} 分别统计其对应的通信有效率参数 p_{kj}^1，p_{jk}^1。

Step2 节点 N_{1k} 统计获得 p_{kj}^1 后，若 $p_{kj}^1 \geqslant \theta$，则构造预警消息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$，并借助与 $Layer_2$ 中对应的簇首节点 N_{2m} 间的安全信道将消息发送到 N_{2m}。其中，T_k 为节点 N_{1k} 发送消息到其簇首节点 N_{2m} 的时间戳。同理，若对于节点 N_{1j} 有 $p_{jk}^1 \geqslant \theta$ 成立，则节点 N_{1j} 构造预警消息 $\{N_{1k}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_j\}$，并借助安全信道将消息发送到 $Layer_2$ 中其对应的簇首节点 N_{2n}。若节点 N_{2m}，N_{2n} 为 $Layer_2$ 中的同一节点，则执行 Step3；若节点 N_{2m}，N_{2n} 为 $Layer_2$ 中的不同节点，则执行 Step4。

Step3 N_{2m} 首先验证消息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$、$\{N_{1k}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_j\}$ 的完整性及时效性，并进一步通过式(2)验证消息的有效性。若消息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$、$\{N_{1k}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_j\}$ 为有效消息，节点 N_{2m} 构造新的第一类消息 $\{N_{1k}, N_{1j}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_m\}$，并将其通过安全信道发送到 $Layer_3$ 中其对应的簇首节点 N_{3r}。

$$\begin{cases} p_{kj}^1 = p_{jk}^1 \\ S_{kj}^1 = S_{jk}^1 \\ A_{kj}^1 = A_{jk}^1 \end{cases} \tag{2}$$

Step4 节点 N_{2m}，N_{2n} 为 $Layer_2$ 层中不同节点时，以节点 N_{2m} 为例，其首先验证消息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$ 的完整性及是否超时。通过验证后，N_{2m} 构造新的第二类消息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_m'\}$，并将其发送到 $Layer_3$ 中的簇首节点 N_{3r}。节点 N_{2n} 按照相同的方式对消息 $\{N_{1k}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_j\}$ 进行验证及处理，并将新的第二类消息 $\{N_{1k}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_n'\}$ 发送到 $Layer_3$ 层中的节点 N_{3r}。由于 N_{1k} 与 N_{1j} 为邻节点关系，可认为其对应的 $Layer_2$ 中的簇首节点在 $Layer_3$ 中具有唯一的簇首节点 N_{3r} 与之对应。

Step5 若 $Layer_3$ 中的节点 N_{3r} 收到的消息为第一类消息 $\{N_{1k}, N_{1j}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_m\}$ 且消息通过验证，则节点 N_{3r} 进一步构造新的消息 $\{N_{2m}, N_{2m}, N_{1k}, N_{1j}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_r\}$ 并将其通过安全信道发送到地面控制中心 TCC。若节点 N_{3r} 收到的消息为第二类消息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_m'\}$、$\{N_{1k}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_n'\}$，则采用诸如 Step3 中的消息验证方式来验证消息的有效性。若第二类消息通过验证，则节点 N_{3r} 进一步构造新的消息 $\{N_{2m}, N_{2n}, N_{1k}, N_{1j}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_r'\}$ 并将其发送到地面控制中心 TCC。

Step6 TCC 收到并验证 N_{3r} 节点发送的系列消息 $\{N_{2m}, N_{2m}, N_{1k}, N_{1j}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_r\}$ 或 $\{N_{2m}, N_{2n}, N_{1k}, N_{1j}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_r'\}$ 后，汇总分析 $Layer_1$，$Layer_2$ 中各节点间通信过程的有效率参数，发现所在时段内卫星网络对应拓扑结构中存在窃听攻击威胁的链路，并根据卫星网络拓扑结构变化规律预测窃听节点下一阶段会影响的节点及链路。

Step7 如图 3 所示为 TCC 构建的相邻节点间安全链路构建示意图。

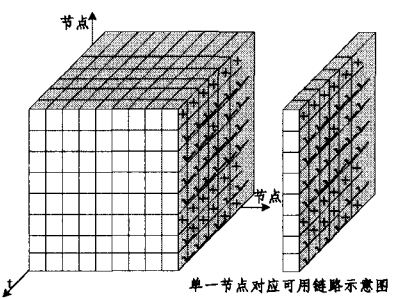

图 3 节点间安全链路构建方案引导图

图 3 主要用于说明随着时间的变化不同节点间是否存在窃听者并构建安全的链路。在图 3 所示网格状结构图中，“十”用于表示某时间段内对应网格代表的节点间存在窃听节点，“√”则用于表示不存在窃听节点。TCC 对图 3 的更新将根据网络中实时信息予以实现，不再赘述。

Step8 当网络中存在较为严重的窃听攻击威胁时，TCC

根据图 3 对所有节点面临窃听攻击威胁的程度进行评估。对存在较为严重的窃听攻击威胁的节点，通过安全信道发送该节点对应的安全链路构建方案到对应的节点。

Step9　对应节点收到其安全链路构建方案后，将验证其有效性。节点需要与其他节点建立通信链路时，将根据其安全链路构建方案判断是否与对应节点建立通信链路。

4　方案安全性及有效性分析

在给出具体检测方法的基础上，主要从理论角度对方案的安全性及有效性进行分析。

4.1　安全性分析

在检测方案的安全性分析过程中，主要从检测过程节点间传输数据的机密性、抗重放攻击能力、信息篡改攻击、发布虚假消息能力的角度进行论述。为便于描述，设定如图 4 所示的攻击想定场景。

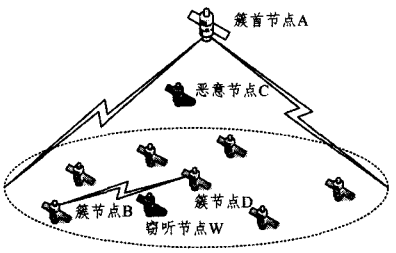

图 4　攻击想定场景

图 4 中节点 A 为簇首节点，存在多个下层的诸如节点 B、节点 D 的簇节点与之通信；而节点 C 为存在于节点 A 与下层簇节点间的恶意节点，具有窃听、重放及篡改信息的能力。提出的窃听攻击检测方案具有以下关键的信息处理步骤。

(1)预警信息的加密及传输：诸如 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$ 的预警信息通过节点间的安全信道 SC 进行加密传输。

(2)预警信息的验证：信息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$ 的验证内容包括可认证性、完整性及时效性等内容。

(3)预警信息的融合：信息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$、$\{N_{1k}, p_{jk}^1, S_{jk}^1, A_{jk}^1, T_j\}$ 通过验证后，将在对应的簇首节点进行融合，并进一步进行安全传输。

对于恶意节点 C 而言，其可以进行如下查询。

(1)预警信息查询：输入由安全信道加密的预警信息 $E\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$，挑战者把对应的预警信息 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$ 返回给恶意节点 C。

(2)信息替换查询：输入由安全信道加密的预警信息 $E\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$，挑战者对原始信息中的 $\{N_{1j}, p_{kj}^1, S_{kj}^1, A_{kj}^1, T_k\}$ 相关信息进行替换。

4.1.1　检测过程节点间数据传输的机密性分析

在恶意节点 C 的攻击下，检测过程节点 A 与节点 B 间数据传输的安全性通过游戏 1 予以定义。

(1)预警信息窃听阶段，挑战者 R 首先对节点 A 与节点 B 间的安全信道 SC 进行窃听，获得其传输的数据 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$。

(2)预警信息查询阶段，挑战者 R 对窃听到的信息 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$ 进行解密得 $\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}'$，并将其发送给节点 C。

(3)若 $\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}' = \{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$，则称节点 C 在游戏中获胜。

以上游戏执行过程中，簇内节点 B 与簇首节点 A 间的消息 $\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$ 均采用传统的基于微波的安全信道 SC 进行加密传输。消息 $\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$ 经安全信道 SC 加密后得秘密信息 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$。因此，挑战者 R 即使窃听到了秘密信息 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$，在未获得相关密码算法信息及密钥的情况下，也是无法对 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$ 进行解密的，即节点 C 在游戏中是无法获胜的，消息 $\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$ 的机密能够得到有效的保障。采用传统微波通信方式的目的在于当链路中存在窃听攻击者时，仍能够保障节点间正常的数据交互。若采用量子通信，一旦信息遭到窃听，则正常用户间的数据传输将必然遭到破坏，通信的成功率将显著降低。

4.1.2　检测方案抵御重放攻击能力分析

在恶意节点 C 的攻击下，检测过程抵御重放攻击的能力通过游戏 2 予以定义。

(1)预警信息窃听阶段，挑战者 R 首先对节点 A 与节点 B 间的安全信道 SC 进行窃听，获得节点 B 发送到节点 A 的数据 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$。

(2)预警信息重放阶段，挑战者 R 将窃听到的信息 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$ 重放给节点 A。

(3)若节点 A 判别 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$ 为有效信息，则称节点 C 在游戏中获胜。

通过上述游戏，攻击者能够恶意消耗目标网络的带宽及计算资源，影响用户对网络资源的使用。检测方案执行过程中，节点 A 与节点 B 间传输的信息均加入了时间戳 T_A。在采用安全信道对信息进行加密传输情况下，即使挑战者 R 截获了相关信息并重放到网络中，节点 A 或 B 在收到信息后，通过时间戳 T_A 也能够判断消息的新鲜性，只有处于有效时间段内的消息才能够获得进一步的处理。因此，攻击者并不能获胜，检测方法能够抵御恶意用户发起的重放攻击。

4.1.3　检测方案抵御信息篡改攻击能力分析

在恶意节点 C 的攻击下，检测过程抵御信息篡改攻击的能力通过游戏 3 予以定义。

(1)预警信息窃听阶段，挑战者 R 首先对节点 A 与节点 B 间的安全信道 SC 进行窃听，获得节点 B 传输到节点 A 的数据 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$。

(2)预警信息查询阶段，挑战者 R 对窃听到的信息 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}$ 进行解密得 $\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}'$。

(3)预警信息篡改阶段，挑战者 R 对 $\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}'$ 中的相关信息进行篡改得 $\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}''$，并对其进行加密 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}''$。

(4)预警信息重放阶段，挑战者 R 将篡改后的信息 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}''$ 重放给节点 A。

(5)若节点 A 判别 $E\{N_{1D}, p_{AD}^1, S_{AD}^1, A_{AD}^1, T_A\}''$ 为有效信息，则称节点 C 在游戏中获胜。

在该游戏中，由于节点 C 无法赢得游戏 1，因此节点 3 也无法赢得该游戏，其原因在于检测过程中，节点 A 与节点 B 间信息的传输主要依赖于安全信道，在安全信道中通过信息的完整性保障及验证机制，可检测并抵御恶意用户发起的信息篡改攻击。

4.1.4 检测方案抵御恶意用户发布虚假消息能力的分析

在恶意节点 C 的攻击下，检测过程抵御恶意用户发布虚假消息的能力通过游戏 4 予以定义。

(1)虚假预警信息构建阶段，挑战者 R 以节点 C 的身份构建节点 C 与节点 D 间的信道存在窃听攻击威胁的预警信息 $E\{N_{1D}, p^1_{CD}, S^1_{CD}, A^1_{CD}, T_C\}$。

(2)预警信息发送阶段，挑战者 R 将构建的虚假预警信息 $E\{N_{1D}, p^1_{CD}, S^1_{CD}, A^1_{CD}, T_C\}$ 发送给节点 A。

(3)若节点 A 判别 $E\{N_{1D}, p^1_{CD}, S^1_{CD}, A^1_{CD}, T_C\}$ 为有效信息，则称节点 C 在游戏中获胜。

在该游戏中，挑战者故意发布网络中存在窃听攻击的虚假消息 $E\{N_{1D}, p^1_{CD}, S^1_{CD}, A^1_{CD}, T_C\}$。由于检测方案在对挑战者发送的消息进行验证的过程中采用如式(2)所示的验证方法，挑战者无法赢得前面的游戏，在节点 D 未受到控制条件下，其无法以节点 D 的身份构造有效的信息 $E\{N_{1C}, p^1_{DC}, S^1_{DC}, A^1_{DC}, T_D\}$。因此，挑战者发送的虚假预警信息 $E\{N_{1D}, p^1_{CD}, S^1_{CD}, A^1_{CD}, T_C\}$ 将被节点 A 判定为无效消息，节点 C 无法赢得该游戏。此外，需进一步说明式(2)并不能有效检测节点 C 与节点 D 共同发起的同谋攻击。针对节点 C 与节点 D 间采用同谋攻击方式发布虚假消息的问题，可进一步采用基于信誉的卫星网络节点行为监控机制对卫星网络节点的行为进行监测。

4.2 有效性分析

4.2.1 检测窃听用户的有效性分析

由于检测方案主要通过提取卫星网络节点间量子通信过程的有效率作为判断对应的链路中是否存在窃听攻击的主要依据。以 BB84 协议为例，正常用户 A 与 B 采用 BB84 协议进行量子通信时，用户 A 每次发送的量子能够选择 4 种偏振态，针对 A 发送的每一个量子，窃听用户 C 随机选择与 A 发射量子偏振态完全相同的概率为 1/4。在 C 进行窃听时，针对单一量子，用户 A 与 B 无法检测出量子状态未发生改变的概率为 1/4。当 A 与 B 间发送的比特序列的长度为 n 时，窃听用户不被发现的概率可表示为 $(1/4)^n$。因此，随着用户 A 与用户 B 间传输信息量的增加，窃听用户 C 无法做到在不改变 A 与 B 间通信内容的情况下实现对 A 与 B 间通信内容的窃听，其窃听行为也一定能够被检测到。

4.2.2 检测过程信息传输的有效性分析

如图 1 所示，提出的检测方案主要根据卫星网络节点在空间上具有分层分布的特点，检测过程采用层簇式的信息传输机制。当 $Layer_1$ 中的节点需进行信息传输时，其信息将被首先传输到 $Layer_2$ 中其对应的簇首节点。$Layer_2$ 中其对应的簇首节点则将通过验证的信息进一步传输到 $Layer_3$ 中其对应的节点。$Layer_3$ 中其对应的节点则将收集到的信息通过安全信道传送到地面控制中心 TCC。地面控制中心 TCC 在收到相关信息并建立如图 3 所示的卫星网络节点间安全链路构建方案后，同样通过层簇式的卫星通信网络将相关信息安全地传送到对应的节点。综上所述，提出的检测方案充分利用卫星网络各节点在空间分布上具有的分层及分簇形态特征，采用层簇式的网络结构可提供高效的信息传输效率。

结束语 针对卫星网络窃听攻击检测问题，开展了基于量子密码的卫星网络窃听攻击检测方法研究。定义了基于层簇式的卫星网络窃听攻击检测模型，通过簇首节点的协作，在进行信息汇聚的基础上，可实现将相关节点的检测信息有效传递到地面控制中心。地面控制中心在收到相关信息后，综合分析当前卫星网络中相邻节点间的链路状况，并根据卫星节点的空间运动规律，对可能存在窃听攻击威胁的链路进行预测，并制定相应的节点安全链路构建方案，指导卫星网络中的节点构建安全的通信链路。本文主要从理论角度对所提方法进行了论述，如何在引入量子密码通信技术条件下，进一步深入研究地面控制中心对相关信息的处理、卫星网络节点间身份的认证、节点间信息的可靠传输，是下一步的研究方向。

参 考 文 献

[1] Chi Hao, Zhang Xian-min, Zhu Hua-fei, et al. Principles applications and state-of-the-arts of Quantum Cryptography[J]. Journal of Optoelectronics, LASER, 2001, 12(1): 105-108(in Chinese)
池灏，章献民，朱华飞，等. 量子密码的原理、应用和研究进展[J]. 光电子·激光，2001，12(1)：105-108

[2] Lu Bing-xu. Development of Quantum Cryptography [J]. Computer CD Software and Applications, 2014(24): 314-315(in Chinese)
路炳旭. 量子密码技术发展概述[J]. 计算机光盘软件与应用，2014(24)：314-315

[3] Wang J F, Li L, Zhou M T. Topological Dynamics characterization for LEO satellite networks [J]. Computer Networks, 2007, 51(1): 43-53

[4] Küçükate ş R, Ersoy C. Minimum flow maximum residual routing in LEO satellite networks routing set [J]. Journal of Wireless Networks, 2008, 14(4): 501-517

[5] Li Jia. Research on Quantum Cryptography System[J]. Science Mosaic, 2013(6): 221-226(in Chinese)
李佳. 量子密码体系研究[J]. 科技广场，2013(6)：221-226

[6] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography [J]. Reviews of Modern Physics, 2002, 74(1): 145-195

[7] Wen Qiao-yan, Qin Su-juan, Gao Fei. Cryptanalysis of Quantum Cryptographic Protocols[J]. Journal of Cryptologic Research, 2014, 1(2): 200-210(in Chinese)
温巧燕，秦素娟，高飞. 量子密码协议安全性分析[J]. 密码学报，2014，1(2)：200-210

[8] Su Jin-hai, Luan Xin, Guo Yi-xi, et al. A Group Key Agreement Scheme for QKD Networks[J]. Journal of Shanghai Jiaotong University, 2014, 48(10): 1498-1502(in Chinese)
苏锦海，栾欣，郭义喜，等. 一种适用于量子密钥分配网络的组密钥协商方案 [J]. 上海交通大学学报，2014，48(10)：1498-1502

[9] Luan Xin, Guo Yi-xi, Su Jin-hai, et al. Research of group key service initialization based on QKD[J]. Computer Science, 2013, 40(11A): 181-183(in Chinese)
栾欣，郭义喜，苏锦海，等. 基于 QKD 的组密钥服务初始化研究[J]. 计算机科学，2013，40(11A)：181-183

[10] Chen Yan-bin, Cheng Hu-lai, Gong Li-hua. Quantum key injection scheme [J]. Journal of Nanchang University (Natural Science), 2013, 37(6): 581-588(in Chinese)
陈燕彬，程虎来，龚黎华. 量子密钥注入方案 [J]. 南昌大学学报(理科版)，2013，37(6)：581-588