一种基于阈值更新的组播密钥管理应用方法

霍思羽[1] 杜 爽[1] 朱清倩[1] 陈海英[1]
HUO Siyu DU Shuang ZHU Qingqian CHEN Haiying

摘 要 卫星组播通信被广泛应用，组播通信的安全也得到广泛重视，传统组播密钥管理方案随着组播成员的变化不断更新，已不适用于卫星信道通信，基于此，文章采用基于阈值更新的子组组播密钥分发的方式，通过设定的最大成员变化数和密钥最大使用时间，触发组播密钥更新，既保证密钥的前向安全和后向安全，也降低对卫星信道资源的开销，并将组管理器权限开放给子组成员，成员间通过密钥协商方式保证密钥发送的机密性，采用线程池的并发处理方式，提高系统处理效率，保证密钥同步，从而保障卫星信道中组播通信的机密性。

关键词 组播密钥管理；阈值更新；线程池；密钥协商

doi：10.3969/j.issn.1672-9528.2025.08.022

0 引言

卫星通信具备覆盖范围广、传输距离远、通信容量大、传输质量高、可靠性高等特点，为充分利用卫星通信资源，提高传输效率，减轻通信负担，利用组播技术建立组播组成员间点对多点的网络连接的方式被广泛应用。但卫星通信因其开放性和高暴露性，通信信息更容易被窃取、篡改和攻击，因此，组播通信的安全得到了广泛的重视。

组播通信的安全常用保障方式通过在发送端采用加密算法和加密密钥，将需传输的明文转换为密文后再送入卫星信道进行传输，接收方使用相同的算法和对应的密钥，将密文恢复为明文，从而使通信信息获得安全保护。若非组播组内的成员，收到相应密文，但无对应的加密密钥，也不能正确解密出明文数据，因此在组播加密通信中，构建高效安全的组播密钥管理方案，是保障组播通信安全的基础。由于卫星通信网络存在通信延时大、资源受限、误码率高等不足，且存在通信节点多，动态变化大的特点，因此在工程应用中，密钥管理方案不仅需考虑密钥使用的安全性，也需保障密钥的高效同步，并降低对卫星信道资源的开销，基于安全性以最小化密钥更新的代价，保障组播通信的机密性和完整性需求[1]。

1 分散子组组播密钥管理方案

组播密钥管理方案常用的方式为集中式组密钥管理方案[2]，其结构清晰、便于管理，但组规模大或组内成员数量过多，不仅增加单节点的通信和计算压力，也容易出现单点失效等问题。

本文在集中式组播密钥管理的基础上，采用分散子组控制站的管理方案，如图 1 所示，通信系统内，可建立多个组播组，各用户站可加入多个组播组，某组播组内，可指定任意成员为组管理者，即组播主站，组管理者接收合法成员加入或退出的申请后，分别和各成员站建立加密通信链路，进行密钥分发和更新，并动态更新组内成员信息进行管理。成员站可根据应用场景和需求，申请加入多个组播组，每个组播组的组管理者，可掌握在不同或个别成员站中，降低单一的组管理者的计算压力，分担失控风险，同时每个成员或指定成员均具备成为组管理者的权限和能力，增加组播应用场景的灵活性和实用性[3]。

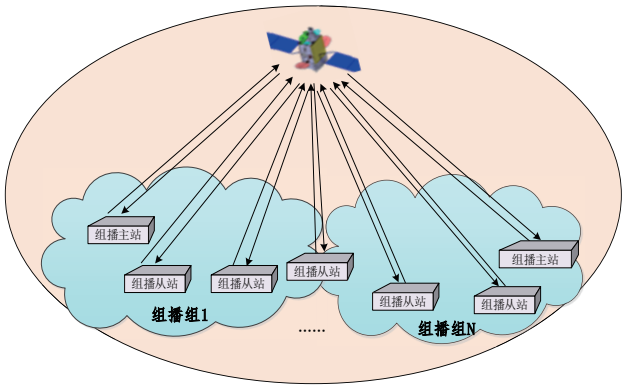

图 1 卫星组播通信图

组播通信中对组播密钥传输的安全性和对通信资源开销要求有着更高的要求，组播密钥管理的主要任务是实现组播密钥的分发、销毁与更新，保障当前组播组内的成员的安全通信，若任意组播组成员的加入或退出时均对所有成员站更新组播密钥，将大大增加通信开销负担，因此在卫星通信中，

1. 中国电子科技集团公司第三十研究所 四川成都 610041

组播密钥的分发与更新需在保证一定安全性的基础上，满足通信轻量化需求，降低对通信资源的开销 [1]。

组播密钥或管理信息在传输过程中，存在被窃听和篡改的可能，组播密钥若失控，组播通信业务将无法安全传输，因此组播密钥的管理方案也需解决如何安全地传输组播密钥问题，保证在卫星信道中传输的组播密钥和其他关键信息的机密性和完整性。

本文采用混合加解密体制建立组播主站与各成员站之间的加密通信通道 [4]，首先通过国密非对称算法 SM2 协商派生组播主站与对应成员站之间的端端会话密钥，通过国密分组算法 SM4 和协商出的端端会话密钥，对组播密钥和关键信息进行加解密处理，建立加密通信链路，实现传输链路的安全性。

2 基于阈值更新的组密钥管理方法

为平衡对卫星信道资源的占用情况和组播通信的通信安全，本文采用基于可配置调整的阈值更新方式对组播组内成员的组播密钥进行更新。为满足密钥使用安全和更新灵活性，本方案中组播密钥主动更新的触发条件主要分为 2 种情况：

（1）达到成员变化数阈值触发更新；

（2）达到密钥使用时间阈值触发更新。

情况 1：在某组播组内，主播主站设定时间阈值 T_{max}，使每组密钥最大使用时间不超过 T_{max}，记录密钥初始时间为 T_0，当时间 T> T_0+T_{max} 时，立即触发密钥更新，并更新密钥初始时间 T_0 为 T。

情况 2：设定成员变化阈值 $Memb_{max}$，使当前密钥在 T<T_0+T_{max} 内，当有成员变化时，成员累计变化数 $Memb_{chge}$< $Memb_{ma}$ 时，组内其他成员不进行密钥更新，若成员累计变化数 $Memb_{chge}$≥ $Memb_{ma}$，则立即更新密钥，并初始化 $Memb_{chge}$ 。

通过以上 2 种情况的触发更新， 在满足密钥的前向安全的同时，达到降低卫星信道资源占用的目的，可根据组播组的规模和应用场景等因素，不同组播组可设定不同的阈值，同一组播组，组播主站可动态调整 T_{max} 和 $Memb_{max}$ 数值。

3 组播密钥管理方案应用设计

3.1 组播密钥管理设计

组播组建立时，某成员站被指定为组播主站后，组播主站通过噪声源派生符合随机性要求的数据作为组播密钥，并指定该密钥的启用时间 T_0 和最大使用时间 T_{max}，组播主站实时监测密钥的使用有效期，并等待成员加入或退出。

根据应用规划需求，成员站向需加入的组播主站发起加入组播组的申请，主站接收成员站发起的加入申请后，判断其身份合法性，并发起端端密钥协商，获取端端的会话密钥，与单一成员站建立加密通信链路，用于组播密钥或管理指令的安全传输。各成员站正确接收组播密钥后，记录更新该密钥的启用时间 T_0 和最大使用时间 T_{max}，当各站检测到当前时间 T> T_0+T_{max} 时，对该密钥进行销毁并等待或更换使用新的密钥。

3.2 基于阈值的动态组播密钥更新流程

基于阈值的动态组播密钥管理流程如图 2 所示，组播主站根据组播组身份标识，实时检测正在使用的组播密钥的时间是否在时间阈值 T_{max} 范围内，若使用时间已超时，则立即派生新组播密钥 Key$^{'}$，并更新时间 T_0'，根据最新的组播成员列表进行批量更新，对于未完成更新的成员，启动定时更新机制，若超时未收到应答或超过发送次数，则移除成员列表。

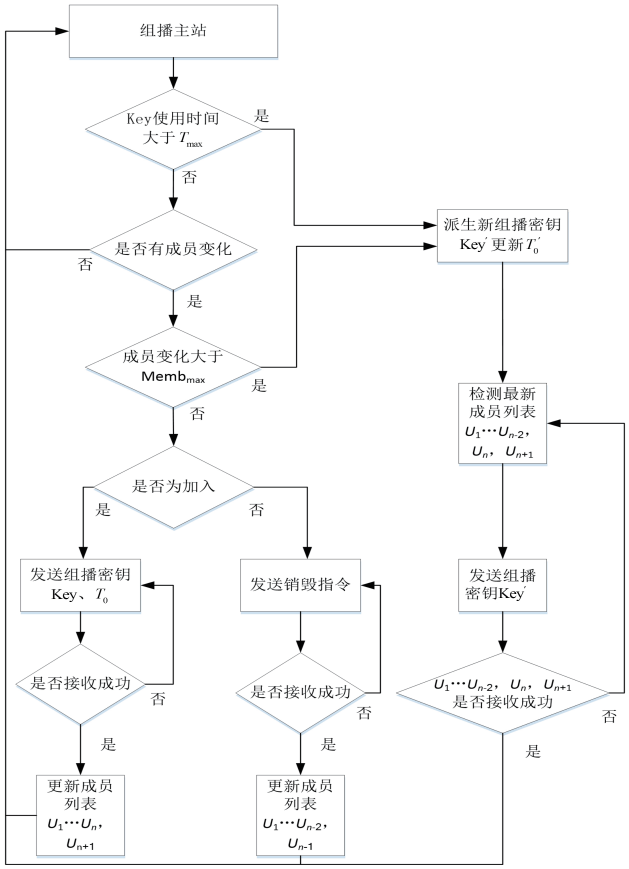

图 2 基于阈值的组播密钥管理流程

若组播密钥在时间阈值 T_{max} 内，有成员加入或退出，则判断成员累计变化数 $Memb_{chge}$ 是否已超过成员累计变化阈值 $Memb_{max}$，若已超过，则立即派生新组播密钥 KEY$^{'}$，更新时间 T_0'，并根据当前加入或退出的成员申请，实时刷新成员管理列表，若为成员加入，则对 N+1 个成员进行组播密钥和关键信息的更新，若为成员退出，则对 N-1 个成员进行组播密钥和关键信息的更新，同时发送密钥销毁指令至退出成员，保证密钥的前向安全。若成员累计变化数 $Memb_{chge}$ 未超过阈值，则仅对当前申请加入或退出的成员进行相应管控，动态

更新成员管理列表。

3.3 组播从站密钥超时管理设计

如图 3 所示，组播从站接收组播密钥和启用时间 T_0，启动密钥有效期判断管理，当组播密钥使用时间超过时间阈值 T_{max} 时，又未收到组播主站发送的新的组播密钥，且未收到管控设备要求的退出组播组的要求，先销毁本地已超时的组播密钥和关键信息，并再次向组播主站发起组播加入申请，若收到管控设备的退出组播组要求，但未收到组播主站的销毁指令，则向组播主站发起退出申请。若已收到新的组播密钥，则销毁旧密钥后，更新替换本地存储数据，并同步密钥的启用时间。

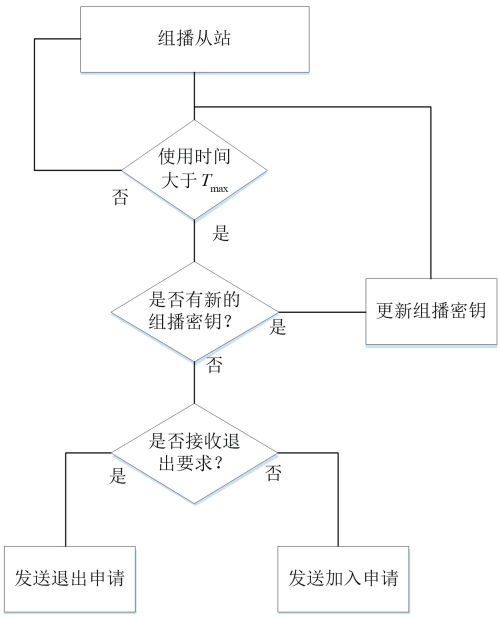

图 3 基于阈值的组播密钥管理流程图

4 基于密钥协商算法和分组算法的加密通信设计

为保证在卫星信道中组播密钥的传输安全，组播主站与组播成员站需建立安全的加密通信链路，预置密钥占用存储资源大且安全风险高，通过密钥分发管理设备分发灵活性差，且增加分发管理设备计算管理负担，本文采用混合加密体制建立组播主站与成员站之间的加密通信通道。

如图 4 流程所示，本方案采用轻量级的协商流程，降低对信道的占用率 [5]。

Step1：当组播从站 B 需加入或退出所在组播组时，首先向组播主站 A 发起加入或退出申请。

Step2：组播主站 A 首先检测从站 B 的合法性，检测是否与组播从站 B 之间存在有效的会话密钥，若存在有效会话密钥，则直接发送组播密钥或同意退出指令，若无有效会话密钥则发起协商流程。

Step3：主站 A 发起协商流程，主站 A 首先向从站 B 发送公钥 R_A 和可辨识标志 ID_A。

Step4：从站 B 接收公钥 R_A 和可辨识标志 ID，先验证公钥 R_A 和可辨识标志 ID_A 的合法性，若合法性不通过，则会话结束。从站 B 结合自身的公钥 R_B 和可辨识标志 ID_B，通过 SM2 算法进行计算，获取会话密钥，并将公钥 R_B 和可辨识标志 ID_B 发送至主站 A。

Step5：主站 A 通过 SM2 算法进行计算，获取会话密钥，并提取从站发送的关键信息验证会话密钥的正确性，验证失败，则会话结束，并启动定时协商机制，验证成功，则提取对应的组播密钥和关键信息，通过对称算法 SM4 和协商出的会话密钥进行加密处理后传输。

Step6：从站 B 通过 SM4 算法和会话密钥解密成功后获取组播密钥明文，并记录时间 T_0，并将处理结果反馈至组播主站 A。

为避免更新时大批量的协商，组播主站在组播存续期间，维护与各端站协商出的会话密钥，若更新或销毁时，未检测到有效的协商密钥，再重新发起协商。

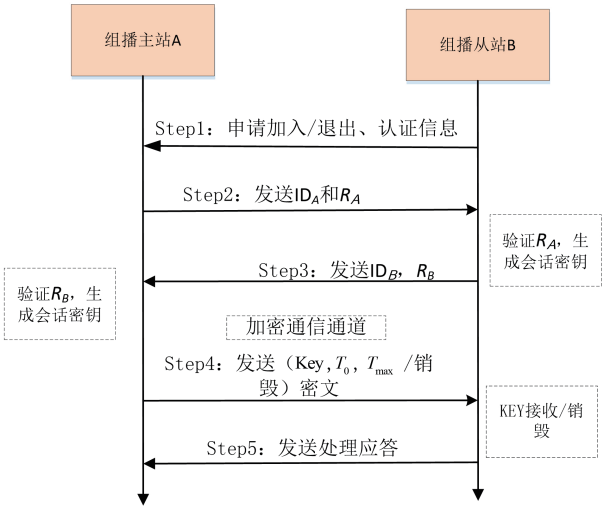

图 4 轻量级协商和通信流程

5 基于线程池的分发设计

组播密钥管理方案高效的关键，除采用高效的加解密算法之外，另一关键要素是高效处理和发送，以保证密钥切换时，组播通信所使用的密钥能够保持同步。当组播主站与组内各成员站在加密传输链路建立，或更新阈值触发进行集中密钥更新，若发送处理模块采用单线程方式轮流发送，会加大通信时延，特别是组规模较大，组内成员较多的情况下，可能会造成某成员站接收新的组播密钥不及时，导致密钥不同步，不能正确地进行加解密运算，无法正常进行通信，因此为提升发送效率，应采用多线程的加解密处理方式 [6] 进行协议处理。

组播主站与组内成员站间密钥协商、密钥分发和更新为

密集且耗时少的短任务，当任务集中出现时，采用传统的多线程方式频繁的线程创建和删除将消耗大量的时间，增大系统的资源损耗。针对周期性且具有一定规模的任务量，采用线程池方案，可节省线程创建和销毁的时间，加快任务的处理速度。

采用静态线程池方案[7]进行组播密钥管理协议处理，预先设定数量 M 的线程，当出现 N 个任务请求时，任务调度模块将任务投入任务队列中，任务队列中存在任务时，触发线程池从任务队列中获取任务，完成任务处理，实现并行处理要求，但组播组内的成员个数未知，若成员数过多，预设的线程数可能不满足高效处理的要求，若成员数较少，或造成系统资源的浪费。因此本方案采用动态线程池方案进行协议处理，增加任务监控线程，根据任务量实时对线程池进行动态调整[8]。

如图 5 所示。动态处理线程池预先设定数量 M' 的处理线程数，任务监控线程实时对任务量和线程使用率进行监控[9]，通过设定合理的线程数使用率，进行线程数量管控。任务监控线程实时轮询信号量，监控当前线程使用率，对处理线程池中的线程数量进行动态调整。若出现井喷式任务量时，线程使用数量过高或全占用，处理线程不能满足任务处理需求，任务监控线程将动态增加处理线程池中的线程数量，加快任务处理进度，提高处理效率，保证终端间的密钥协商和密钥发送速率，避免组播业务通信时，各用户站之间密钥不同步。若监控线程使用率较低时，则实时回收释放空闲线程，减少线程池中的线程数量，释放系统资源。

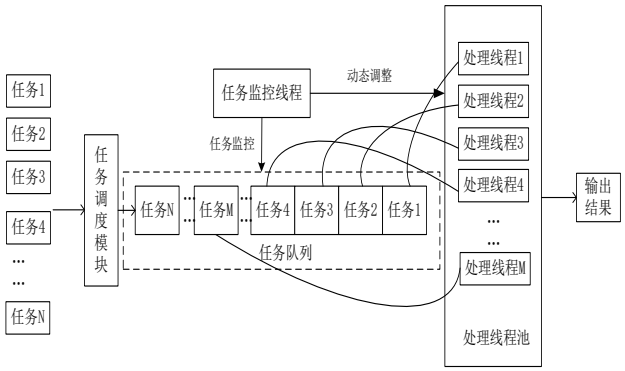

图 5 基于线程池的协议处理

通过动态线程池的设计，调整处理线程池中的线程数量，既降低创建销毁线程池的资源开销，降低超时发生率，保证任务的实时性，也避免空闲或任务量较小时造成系统资源浪费。

6 结语

上述组播密钥管理方案，通过分散组管理者的组播密钥管理方案，能灵活制定组管理者，降低单一节点的计算压力和失控风险，也更便于组播组管理；通过基于成员变化阈值和密钥使用时间阈值触发更新的组播密钥更新方式，降低密钥更新频率，降低通信资源占用率；当成员退出又未达到阈值触发更新时，组管理者将定时发送销毁指令，组播主站通过定时更新和即时销毁，从站通过密钥超时自动更新销毁机制，保障密钥的前向安全；为提高处理效率和系统资源使用率，采用动态线程池方案实现，通过任务量触发方式降低实现复杂度，通过动态调整线程池数量，满足大任务量时的高效处理能力，降低小任务量时对系统资源的占用，通过线程池的并发处理机制，提高处理能力，加快发送同步效率，满足定时大批量更新或销毁密钥的需求，为卫星通信的组播加密通信保驾护航。

参考文献：

[1] 陈启雅 . 面向安全组播通信场景的组密钥管理方案的研究 [D]. 合肥 : 中国科学技术大学 .2022.

[2] 边珊 . 空间信息网络中组播密钥管理方案研究 [D]. 成都 : 西华大学 ,2018.

[3] 刘淑影 , 许勇 , 杨帆 . 一种新的无线网络组播密钥管理方案 [J]. 计算机安全 ,2014(4):52-56.

[4] 夏涛 , 何俊 , 刘林 , 等 . 无人机轻量级认证密钥协商技术研究 : 第十届中国指挥控制大会论文集（下册）[C]. 武汉 : 国防科技大学信息通信学院 ,2022.

[5] 郑艳 , 江卫 . 宽带数字集群通信系统端端加密方案研究 [J]. 信息安全与通信保密 ,2014(9):147-150.

[6] 马占飞 , 李克见 , 史国振 . 基于多引擎并发的密码服务软件架构 [J]. 北京电子科技学院学报 ,2022,30(1):43-49.

[7] 王鑫 , 扈月 , 刘坤禹 , 等 .Linux 下多线程的方案实现与对比 [J]. 信息记录材料 ,2024,25(3):246-248.

[8] 刘新强 , 曾兵义 . 用线程池解决服务器并发请求的方案设计 [J]. 现代电子技术 ,2011,34(15):141-143.

[9] 黄鑫尧 , 周文辉 . 一种加解密设备模拟终端的设计方法 [J]. 微处理机 ,2024,45(5):46-49.

【作者简介】

霍思羽（1991—），女，四川蓬溪人，硕士研究生，工程师，研究方向：保密通信、嵌入式软件设计。

杜爽（1990—），女，四川广安人，硕士研究生，工程师，研究方向：信息安全与保密通信、嵌入式软件开发。

朱清倩（1991—），女，安徽舒城人，硕士研究生，工程师，研究方向：通信网络、嵌入式软件设计。

陈海英（1983—），女，黑龙江大庆人，硕士研究生，高级工程师，研究方向：信息安全、软件设计。

（收稿日期：2025-03-31 修回日期：2025-08-05）