

集群网络密钥管理方案研究综述

刘军, 袁霖, 冯志尚

(信息工程大学, 河南 郑州 450001)

摘要: 随着人工智能和通信网络技术快速发展, 集群智能越来越受到重视, 集群网络作为集群智能重要组成部分, 信息安全交互问题备受关注, 集群密钥管理成为该领域的研究热点。近年来, 研究者对集群密钥管理研究的不断深入, 提出了很多集群密钥管理方案, 为复杂的集群网络体系进行信息安全交互提供了有效解决思路, 但缺乏系统性的概括论述。对现有集群密钥管理方案进行了分析和总结, 并探讨了集群密钥管理未来研究方向和应用场景。介绍了包括控制层、簇头层、节点层的典型三层集群网络模型, 指出集群网络具有数量规模较大、动态拓扑变化、分层分簇异构的网络特性; 根据密钥管理策略和集群网络场景, 按照网络部署前和网络部署后归纳了集群密钥管理流程, 并从安全性、效率、灵活性3方面分析了密钥管理评价指标; 重点论述了预分配管理、愈合管理、动态管理3种密钥管理方案, 并分析了不同类型方案的基本思路和优缺点, 从技术基础、安全优势、灵活优势、效率优势4方面对不同方案性能进行了对比总结; 从跨域异构、集群认证、愈合机制、技术融合4方面对集群密钥管理相关的研究热点进行了展望, 并探讨了集群密钥管理在泛在物联、全域作战、智慧城市3个未来应用场景中的重要安全作用。

关键词: 集群网络; 密钥管理; 信息安全; 集群认证; 愈合机制

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022082

Survey of key management schemes for cluster networks

LIU Jun, YUAN Lin, FENG Zhishang

Information Engineering University, Zhengzhou 450001, China

Abstract: With the rapid development of artificial intelligence and communication network technology, increasing attention has been paid to cluster intelligence. Cluster network is an important part of cluster intelligence, the security of information interaction has attracted much attention, and cluster key management has become a research hotspot in network information security. In recent years, many cluster key management schemes have been proposed, which provide effective solutions for information security interaction of complex cluster network systems. The existing cluster key management schemes were analyzed and summarized, and the future research direction and application scenarios were discussed. The typical three-layer cluster network model was introduced, including the

收稿日期: 2022-04-06; 修回日期: 2022-11-06

通信作者: 袁霖, fkefss@126.com

基金项目: 国家自然科学基金(61902427)

Foundation Item: The National Natural Science Foundation of China (61902427)

引用格式: 刘军, 袁霖, 冯志尚. 集群网络密钥管理方案研究综述[J]. 网络与信息安全学报, 2022, 8(6): 52-69.

Citation Format: LIU J, YUAN L, FENG Z S. Survey of key management schemes for cluster networks[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 52-69.

control layer, cluster head layer and node layer. The characteristics of cluster network were summarized, such as large number and scale, dynamic topology change, and hierarchical cluster heterogeneity. According to the key management strategy and cluster networking scenarios, the cluster key management process before and after the network deployment was summarized. The key management evaluation index was analyzed from the aspects of security, efficiency, and flexibility. Then, three key management schemes including pre-distribution management, healing management and dynamic management were discussed. Their basic ideas, advantages and disadvantages were analyzed, and their performance from the aspects of techniques, security, flexibility, and efficiency was compared. Besides, the research hotspots related to cluster key management were prospected from cross-domain heterogeneity, cluster authentication, healing mechanism, and technology fusion. The security function of cluster key management in future application scenarios such as ubiquitous IoT, all-domain operation, and smart city was discussed.

Keywords: cluster network, key management, information security, cluster authentication, healing mechanism

0 引言

集群智能 (swarm intelligence) 是指简单个体通过相互协作表现出来集群智能行为, 最早源于法国生物学家 Grassé 对蚁群的出现、调节和控制机制的研究^[1], 蚁群个体通过相互合作完成复杂工作所表现的行为是集群智能雏形。集群智能系统通常指多个智能体 (agent) 组建集群网络、进行信息交互, 智能完成多样性的复杂任务, 具有自组织、无中心、高鲁棒性等特点^[2]。集群网络作为集群智能系统的神经中枢, 信息交互功能是确保集群协作的前提和基础, 集群网络通常采用无线方式进行信息传输, 具有与生俱来的广播 (组播) 通信特性, 极易受到攻击者的攻击, 信息安全与保密问题日益凸显。

“一切秘密寓于密钥”, 在网络安全管理中, 密钥是保护网络和信息安全的重要保证, 安全作用不言而喻, 一般来讲, 密钥管理指密钥产生到销毁全过程进行的管理, 是网络安全的关键技术, 包括在整个生命周期对密钥及其相关信息和活动实施有效影响的所有活动。广义来讲包括行政管理和技术管理, 狭义来讲主要指技术管理, 包括密钥生成、存储、分配、协商、使用、更新、备份和恢复、撤销和销毁等过程^[3]。本文主要从狭义上, 也就是技术角度分析密钥管理。一直以来, 国内外对密钥管理的技术研究比较重视, 在密钥管理方案的研究方面取得了大量成果, He 等^[4]、Barskar 等^[5]、Singh 等^[6]、Yousefpoor 等^[7]、Parthasarathi 等^[8]、Nithya 等^[9]对现有密钥管理方案成果进行了综述。近年来, 随着物联网、车联

网、无人机集群技术快速发展, 集群网络安全问题日益突出, 面向集群网络的密钥管理成为研究热点。本文梳理总结了有关集群网络密钥管理研究成果, 归纳集群网络模型和网络特性, 分析集群网络的密钥管理性能指标、步骤流程, 总结对比了不同集群网络密钥管理方案优缺点, 结合人工智能、区块链等新兴技术对集群网络密钥管理的应用前景和未来研究方向进行总结展望。

1 集群网络模型

1.1 典型网络

集群网络作为集群智能的重要组成部分, 网络模型通常是由一个或者多个静态 (或动态) 簇组组成的分层体系结构^[10]。分层的集群网络模型便于进行节点管理, 优化各级负载, 增强网络可扩展性, 有效减少通信开销^[11]。目前已广泛应用于卫星集群^[12]、无人机集群^[13]、车辆集群^[14]、传感器集群^[15]等应用场景。上述应用场景中典型的集群网络模型如图 1 所示。

1) 控制层 (control layer): 主要由基站 (BS, base station) 等控制节点组成, 是集群网络的顶层, 负责对集群网络内节点的控制管理, 接收节点传输的信息数据, 发送控制命令, 一般在密钥管理中担任密钥分发中心 (KDC, key distribution center) 角色, 地位处于最高级别。

2) 簇头层 (cluster head layer): 由集群网络中担任簇头 (CH, cluster head) 的节点组成, 负责中继信息数据和控制命令, 对成员节点进行控制管理, 接收成员节点数据并进行融合处理, 再传输给控制层, 减少通信开销, 密钥管理中往往

担任密钥组管理者 (GM, group manager), CH 节点性能、资源较好。

3) 节点层 (node layer): 由簇内的簇成员 (CM, cluster member) 节点组成, 集群网络中底层的应用节点作为网络基本单元, 负责执行具体任务, 通过节点之间信息交互达到数据共享, CM 节点资源和性能相对较差。

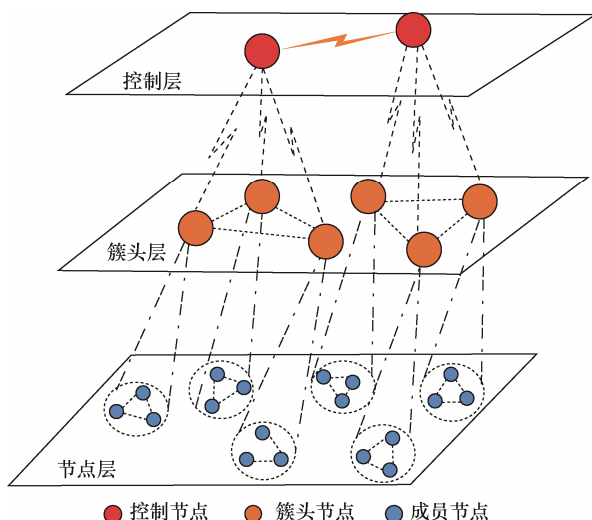


图 1 典型的集群网络模型
Figure 1 Typical cluster network model

1.2 网络特性分析

集群网络在网络结构上主要表现为数量规模较大、动态拓扑变化、分层分簇异构 3 个方面。

1) 数量规模较大。集群网络往往包含大量的节点, 其数量规模相对普通网络大很多。

2) 动态拓扑变化。集群网络通常采取无线方式进行通信, 拓扑易受到外部环境影响, 进而发生变化。

3) 分层分簇异构。具有较多异构节点, 中心节点性能有限, 往往需要采用分层分簇结构分化节点承担的各类负载和开销。

2 集群密钥管理步骤及评价指标

2.1 集群密钥管理流程分析

结合集群网络应用场景和密钥管理策略, 根据 Wang 等^[16]提出的密钥更新流程, 归纳了集群密钥管理流程, 如图 2 所示, 主要包括密钥预分配、密钥生成 (建立通信密钥)、密钥更新与分发、密钥愈合 (恢复)。

1) 密钥预分配: 主要在系统初始化阶段进行, 也就是网络部署前, KDC 从生成的密钥管理池中, 选取部分密钥分发至节点, 并为节点预置密钥材料用于生成密钥的过程。

2) 密钥生成: 建立通信密钥是密钥管理的基本问题。集群网络需要建立多种密钥进行通信, 包括 BS-CH、CH-CH、CH-CM、CM-CM 通信密钥, 需要考虑密钥随机性、强度和空间等问题, 确保密钥安全性。

3) 密钥更新: 会话超过设定周期或集群网络拓扑结构变化, 包括节点加入、节点退出、簇组合并、簇组分裂, 为避免密钥泄露, 需要进行密钥更新操作。

4) 密钥分发: 密钥生成 (更新) 到密钥使用的过程, KDC 通过安全通道对已经生成 (或更新) 的密钥进行分发管理, 通过广播或组播方式分发至 CH 节点和 CM 节点, 建立安全通信链路。

5) 密钥愈合 (恢复): 在部分动态无线网络中, 容易遭受压制攻击 (如电磁干扰) 导致通信中断, 丢失密钥更新数据包, 通信恢复后需要愈合恢复密钥, 确保后续建立安全通信, 增强网络鲁棒性。

2.2 密钥评价指标

密钥管理指通信各方之间建立、分发、更新和维护密钥的程序和技术, 评价指标包括安全性、效率和灵活性 3 个方面^[17]。

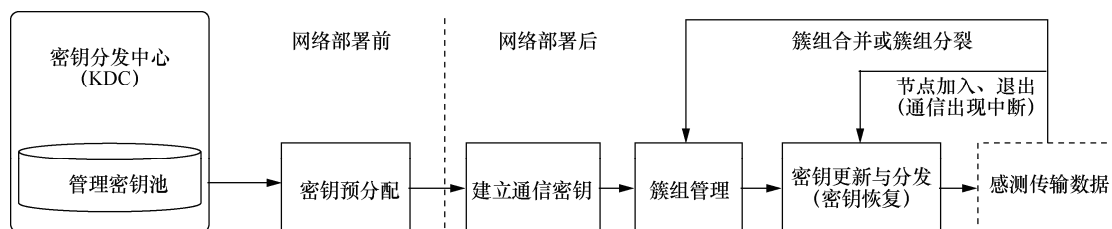


图 2 集群密钥管理流程
Figure 2 Cluster key management process

1) 安全性。包括抗毁性、抗共谋攻击、抗窃听攻击、前向和后向安全性、节点撤销能力等。抗毁性指抵御被捕获节点的攻击能力，防止攻击者利用捕获节点对密钥进行破解，有时也称抗捕获攻击能力；抗共谋攻击指阻止部分妥协节点通过共谋，利用自身存储的信息协作泄露密钥；抗窃听攻击指防止攻击者利用密钥管理过程中传输的信息破解密钥；前向安全性防止使用旧的密钥对新加密的消息进行解密，后向安全性防止使用新密钥对以前加密的消息进行解密^[4]。节点撤销能力指被撤销的节点不能计算当前时间段密钥。

2) 效率。包括密钥管理所需要的存储、通信、计算等各类开销指标。存储开销指存储密钥材料和密钥所需占用的内存空间；通信开销指密钥生成、分发、更新和维护过程中需要传输的信息大小和数量；计算开销指密钥管理过程中进行相关运算和操作的计算复杂度；能量消耗指密钥管理过程中，密钥管理消息发送、接收以及密钥计算过程中所消耗的能量。

3) 灵活性。包括密钥连通性、可拓展性和可伸缩性。连通性指任意需要通信的双方建立共享密钥的概率；可拓展性指密钥管理方案支持的最大网络规模数量；可伸缩性指在节点加入或离开时能够进行密钥更新的特性。

3 集群密钥管理方案

近年来，对集群网络密钥管理的研究不断深入，很多有关集群的密钥管理方案被提出，考虑集群网络结构特性，多数使用的是层次式的混合密钥管理方案，本文根据集群密钥管理流程，针对网络部署预分配降低计算和通信开销、网络部署后通信出现中断和通信拓扑变化 3 方面的问题，从大量文献归纳总结了 3 种密钥管理策略：预分配管理方案、愈合管理方案和动态管理方案。

3.1 预分配管理方案

密钥预分配主要指在部署网络时对密钥及相关参数进行预分配。Blom 等^[18]提出基于有限域上对称矩阵的密钥预分配方案，Blundo 等^[19]在 Blom 等基础上提出基于对称多项式的密钥预分配方案；Eschenauer 等^[20]提出了经典随机密钥预

分配 E-G 方案；Chan 等^[21]对 E-G 方案进行了改进，增强网络抗毁性，提出了 q-composite 的密钥预分配方案；Du 等^[22]结合 Blom 和 E-G 两种方案，提出了多密钥空间预分配方案（MKPS, multiple-space key pre-distribution scheme）；Liu 等^[23]提出了基于部署信息的密钥预分配管理方案；Zhu 等^[24]提出了经典的分层分组 LEAP+预分配密钥管理方案；经过学者不断研究和探索，近年来出现了较多与集群网络有关的密钥预分配方案。

张记等^[25]提出了基于可转化三元多项式的密钥预分配管理方案。① 基本思路。对网络结构进行层次化分簇为 BS、CH、CM，并引入密钥分发节点（KDN, key distribution node）。首先，BS 为任意节点随机生成可转化三元多项式 $f(x, y, z)$ ，将节点身份标志 ID_i 代入多项式计算出 $f(ID_i, y, z)$ ，并分发给节点，节点利用 BS 广播消息计算管理密钥 K ；令 $z=0$ ，利用 CH 的身份标志 ID_{CH_A} 和 ID_{CH_B} ，代入存储的多项式中，分别计算出 $K_{CH_A-CH_B} = f(ID_{CH_A}, ID_{CH_B}, 0)$ 和 $K_{CH_B-CH_A} = f(ID_{CH_B}, ID_{CH_A}, 0)$ ，根据对称性建立会话密钥 $K_{CH_A-CH_B} = K_{CH_B-CH_A}$ ，利用相同方法建立 KDN 之间会话密钥；CH-CM 通过 KDN 利用多项式计算出密钥，利用 Hash 函数进行单向处理后分发，建立 CH-CM 之间安全通信密钥。② 方案分析。方案提高了网络安全阈值和节点密钥破解难度，抗捕获攻击能力从 t 提高到 $2t+1$ ，降低了 CM 计算开销，但总体计算开销仍较大。

贺智明等^[26]针对 E-G 方案^[20]和 MKPS 方案^[22]存在的问题，提出了多密钥空间分层的密钥预分配管理方案。① 基本思路。将网络划分为多个正六边形网格的区域，节点分为不同簇组，给任意区域内 CH 分配密钥空间，如图 3 所示。采用 MKPS 方案生成预分配密钥空间 A_i （Blom 矩阵），在有限域上构造 $(\lambda+1) \times N$ 的公开矩阵 G （每列线性不相关），任意 CH_i 与 CH_j 可以根据密钥空间 A_c 计算出会话密钥 $K_{ij} = K_{ji} = A_c(i) \times G(j) = A_c(j) \times G(i)$ ，CH-CM 的通信会话密钥根据 CH 存储 Hash 函数和 CM 的 ID 计算。② 方案分析。保证在簇头层任意相邻 CH 或同一区域可以建立会话密钥，不存在 CH “孤点”，提高了

网络连通性和抗捕获能力, 将存储和计算开销主要集中在簇头层, 利用 CH 高性能优势, 降低 CM 性能需求, 效率开销较为合理。

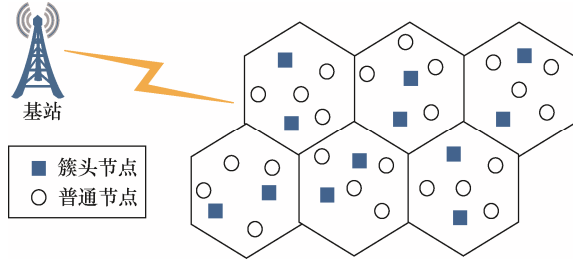


图 3 六边形分簇结构
Figure 3 Hexagonal cluster structure

赵然等^[27]针对 LU 矩阵方案^[28]计算、存储开销和基于多项式方案的安全阈值问题, 提出了基于对称多项式和 LU 矩阵的密钥预分配管理方案。① 基本思路。BS 从密钥池中选取对称多项式构造对称矩阵 $\mathbf{K}$ ($N \times N$ 阶), 分解为下三角 $\mathbf{L}$ 和上三角 $\mathbf{U}$ 矩阵, 并预分配给 CH 相应的行列信息; 任意 CH_i 与 CH_j 交换存储的矩阵行列向量 $(\mathbf{L}_{r(i)}, \mathbf{U}_{c(i)})$ 和 $(\mathbf{L}_{r(j)}, \mathbf{U}_{c(j)})$, 通过相乘计算 $K_{ij} = \mathbf{L}_{r(i)} \times \mathbf{U}_{c(j)}$ 和 $K_{ji} = \mathbf{L}_{r(j)} \times \mathbf{U}_{c(i)}$; 根据 K_{ij} 得到对称多项式 $f(x, y) = \sum_{m,n=0}^t a_{mn} x^m y^n$, CH_i 与 CH_j 计算会话密钥 $f(i, j) = f(j, i)$; BS 计算出通信密钥并预存到任意成员节点 CM_k 中; CH_p 根据成员节点预存的 CH_i 与 CH_j 的 ID 信息 (i, j) 计算出通信密钥 $K_{\text{CH}_p-\text{CM}_k} = f(k, i) \oplus f(k, j)$ 。② 方案分析。

CH 之间基于 LU 矩阵建立通信密钥, 连通率 100%, CM 可以与 BS 进行安全通信, 确保了 BS 对任意节点控制管理; CH-CH、CH-CM 建立唯一通信密钥, 即使捕获 CH 也不影响其他簇组; 同时任意节点的存储开销恒定, 支持节点加入和退出操作, 具有较好的可伸缩性, 但计算开销有待改善。

Chakavarika 等^[29]提出基于多项式的高效节能预分配密钥管理方案。① 基本思路。基于 Yi 等^[30]三层异构传感器网络模型, KDC 生成密钥池, 并从中随机选择 λ 个密钥, 其中 $2 < \lambda < m$ 且 $\lambda \bmod 2 = 1$, 存入相应的成员节点中; CH_i 与 CH_j 使用多项式和相应的 ID 进行计算

$f(\text{ID}_{\text{CH}_i}, \text{ID}_{\text{CH}_j}) = f(\text{ID}_{\text{CH}_j}, \text{ID}_{\text{CH}_i})$ 作为簇间会话密钥; CH-CM 的通信密钥通过异或运算 $K_{\text{CH-CM}} = (k1 \oplus k2 \oplus k3)(\lambda = 3)$ 生成; KDC 生成随机数 R 发送给所有合法节点, 更新密钥 $K'_{\text{CH-CM}} = (k1 \oplus k2 \oplus k3) \oplus R = k1' \oplus k2' \oplus k3'$, 随后丢弃 R , CH-CM 建立新的通信密钥。② 方案分析。降低了存储和能耗开销, 在多项式基础上使用 3 个异或运算计算密钥, 即使 CH 遭受到攻击后泄露, CM 存储的密钥也不会被泄露, 虽然在密钥更新过程提高了安全性, 但增加了成本开销。

Krishnappa 等^[31]提出了基于 LEACH (low-energy adaptive clustering hierarchy) 的随机密钥管预分配理方案。① 基本思路。方案使用 LEACH 算法将网络划分为多个簇, 并从每个簇中选择最佳 CH。BS 首先从大小为 K 的密钥池 (L 个密钥链) 中为任意节点随机选择预分配 k 个不同密钥, 存储为节点的密钥链 r_i , 节点通过存储的密钥链 r_i 计算随机密钥组合 $r_i(K/L)$; 相邻节点广播密钥标识符列表发现共享密钥, 或通过获取中继节点的共享密钥, 建立路径密钥进行安全通信; 密钥分配到各个节点后, 进入稳态阶段, 可以利用密钥加密传输数据, 未传输数据的节点保持休眠状态。② 方案分析。引入 LEACH 分簇算法降低了集群网络能耗, 提高了网络寿命周期, 方案提高了 CH-CM 建立共享密钥的概率, 增强了网络安全性, 但成本开销较大, 且易遭受共谋攻击。

Kumar 等^[32]提出了基于组合设计的密钥预分配管理方案。① 基本思路。BS 首先将网络分割成大小相等的单元区域, 每个区域有 3 个不同类型 CH, 采用差分法构造对称设计 $(k^2 + k + 1, k + 1, 1)$, 生成密钥集 ($k + 1$ 个密钥) 并随机分发给任意节点; 随后使用不同的密钥池为每类 CH 生成密钥集, 将密钥集分配给每类 CH 的 $3/4$, 确保区域之间至少有一条安全链路; CH-CM 采用 Bloom filter 发现共享密钥, 每个节点使用其密钥集来生成字符串, 并在区域内进行广播, 其他节点根据收到的广播, 使用存储密钥集和 Hash 函数获得共同密钥, 建立安全通信。② 方案分析。每个区域设定多个 CH, 区域间至少共享一个密钥, 保证区域连通性和网络弹性, 不

会因单个 CH 故障或妥协而影响安全链路，降低了 CH 存储开销，针对节点受损具有较好的恢复能力，同时使用 Bloom filter 能够较好地抵抗窃听攻击。

陈虹旭等^[33]提出了双变多项式密钥预分配管理的方案。① 基本思路。KDC 预分配密钥 K_{CM_i} 给任意节点，生成两个双变量多项式 $f(x, y)$ 分配给任意 CH， CH_i 与 CH_j 通过自身存储多项式 $f_1(x, y)$ 建立簇间会话密钥 $f_1(ID_{CH_i}, ID_{CH_j}) = f_1(ID_{CH_j}, ID_{CH_i})$ ；使用 $f_2(x, y)$ 建立 CH-CM 密钥，CH 根据 CM_i 发送的 3 个 ID 分别计算生成部分密钥 k_1, k_2, k_3 ，其中 $k_1 = f_{2a}(ID_{CH_a}, ID_{CM_i})$ ， $k_2 = f_{2b}(ID_{CH_b}, ID_{CM_i})$ ， $k_3 = f_{2c}(ID_{CH_c}, ID_{CM_i})$ ，通过异或运算计算 CH-CM 的密钥 $K_{MN_i} = k_1 \oplus k_2 \oplus k_3$ 。② 方案分析。CM 存储空间恒定，能够随网络规模增加进行有效拓展，具有一定抗捕获攻击能力，单节点密钥泄露不影响其他节点；但大于两个簇组后，整体存储空间呈指数增长。

Premamayudu 等^[34]提出了基于密钥池矩阵的密钥预分配管理方案。① 基本思路。BS 首先使用密钥池中的不同密钥生成 2 类矩阵

(MBH(MCH) 和 MC_i)，分别用于 BS-CH、CH-CM 生成密钥链；网络部署前将 MBH 矩阵密钥链加载到 BS 和 CH 上，MCH 矩阵密钥链加载到 CH 上， MC_i 矩阵密钥链加载到对应节点；需要节点间（或簇头间）通过消息交换密钥链，匹配相同密钥，进行异或运算创建密钥对，并进行编号标识，建立安全通信链路；节点生成所有密钥对，建立列表密钥环，并删除预加载的密钥链，防止恶意节点攻击。密钥更新与撤销需重新生成矩阵 MBH(MCH) 和 MC_i ，密钥链通过原来的密钥对加密分发。② 方案分析。具有较少通信和存储开销，连通率达到 100%，支持节点撤销机制，能够抵抗捕获攻击，密钥建立的计算开销主要是密钥链之间的搜索、比较和异或运算操作，但整个过程需要执行矩阵乘法、随机数生成和密钥链操作的创建，计算复杂度相对较高，不适用于需要高效更新密钥的应用场景。

综上所述，表 1 对本节论述的密钥预分配管理方案性能进行了总结比较。

3.2 愈合管理方案

目前无线网络不稳定，在实际应用中，通信受距离、地形、电磁环境等因素影响，容

表 1 密钥预分配管理方案性能比较
Table 1 Performance comparison of the key pre-distribution management scheme

文献	针对问题	技术基础	安全优势	灵活优势	效率优势
张记等 ^[25]	t-security	转化三元多项式 Hash 函数	抗毁性 抗共谋攻击	可拓展性	CM 计算开销↓ CM 存储开销↓
贺智明等 ^[26]	t-security 孤点现象	Blom 矩阵 Hash 函数	抗毁性 抗共谋攻击	连通性（100%）	CM 存储开销↓ CM 计算开销↓
赵然等 ^[27]	1-affect-n	对称多项式 LU 矩阵	抗毁性 抗共谋攻击	连通性（100%） 可拓展性	CM 存储开销恒定
Chakavarika 等 ^[29]	t-security 多项式系数存储空间	对称多项式 异或运算	抗毁性	可拓展性	CH 存储开销↓ CH 计算开销↓
Krishnappa 等 ^[31]	流量分析攻击 生命周期	LEACH 分簇 随机概率	抗毁性	连通性 可伸缩性	能耗开销↓
Kumar 等 ^[32]	节点资源有限	组合设计 Bloom filter	抗毁性 抗窃听攻击	连通性 可伸缩性	CH 存储开销↓
陈虹旭等 ^[33]	1-affect-n 计算复杂度	双变量多项式	抗毁性	可拓展性	计算开销↓ CM 存储开销恒定
Premamayudu 等 ^[34]	网络弹性 节点间密钥安全	密钥生成矩阵 异或运算	抗毁性	连通性（100%） 可伸缩性 可拓展性	存储开销↓ 通信开销↓ CM 计算开销↓

易出现通信中断情况, 密钥更新过程可能会出现数据包丢失, 致使密钥更新不及时影响后续通信, 因此, 在密钥管理过程中需要考虑到如何恢复密钥, 简单的办法可以通过请求重新传输数据, 但请求和重新传输均会造成较大的通信开销^[35], 因此, 在密钥管理中需要引入愈合策略, 通过自愈或互愈方式, 抵抗丢包影响, 减少网络流量, 防止流量分析攻击, 达到安全恢复密钥的目的。

愈合策略是在某个阶段数据包丢失, 无须向 KDC 或 GM 发送请求重传密钥更新消息, 有效降低通信负载, 提高密钥管理效率。基于 Shamir^[36]秘密共享思想, Staddon 等^[37]首次提出自愈机制, 为了解决通信网络不可靠的数据包丢失情况, 通过两个多项式构造会话密钥, 设计了具有撤销功能的非交互式自愈密钥管理方案, 解决了不可靠通信或有损网络中, 离线用户建立组密钥的问题, 但存储和计算开销较大; Liu 等^[38]提出了改进的密钥自愈方案, 对掩码公式进行优化, 进而降低了存储和通信开销, 但容易受到用户重新加入共谋攻击; 经过不断优化发展, 后续提出了多种自愈方案: 基于多项式^[39-41]、基于矢量空间^[42-43]、基于哈希链^[44-45]、基于双线性配对^[46]、基于指数^[47]等。但如果通信中断时间过长, 会导致丢失的广播消息数据较多, 超过滑动窗口大小时间, 无法通过自愈策略恢复密钥, 为保证密钥愈合的实时性, 需要对方案进行优化, 通过借助邻居节点来愈合密钥。Tian 等^[48]基于双线性对实现了互愈策略, 借助邻居节点愈合密钥, 但计算开销较大; Agrawal 等^[49]通过引入密钥确认和安全节点定位等功能降低了成本开销, 提高了安全性。近年来, 随着集群网络群组结构研究, 簇组内广泛应用愈合管理策略, 极大提高了网络的鲁棒性。

李德全等^[50]提出了基于有限域椭圆曲线的密钥自愈管理方案。① 基本思路。初始化过程中, KDC 生成系统参数 params 和主私钥 master_key , 通过安全通道为节点预置静态私钥 M , CH 利用 M 实现身份认证, 并使用签密方式将秘密信息和生成的动态私钥 D 发送给节点, 进而组成节点私钥 (M, D) ; 在一定时间周期后, CH 选择 k 时间段的秘密值 d_k , 生成节点动态私钥 D_k 和广播消息

$W_k(x)$, CM 可利用自身秘密消息和广播消息计算出秘密值 d_k , 进而更新私钥 (M, D_k) ; 若通信中断, 节点丢失时间段 $j(j_1 < j < j_2)$ 的广播消息, 在 j_2 接收到广播消息 $W_{j_2}(x)$ 后, 节点可以根据自身秘密消息和 $W_{j_2}(x)$, 通过 Hash 函数自愈恢复出 j 时间段动态私钥 D_j ; 新节点加入, CH 认证节点身份合法后, 分发身份标志和秘密信息, 并通过签密方式将当前动态私钥 D 分发至新节点; CH-CM、CM-CM 通过存储的私钥, 使用非交互的方式建立会话密钥, 进行安全通信。② 方案分析。既能够抵抗欺骗、重放、内部等主动攻击, 又能抵抗被动攻击, 具有较好的自愈能力和计算效率; 通过签密方式无须安全通道传输密钥, 节省网络带宽, 密钥协商使用非交互方式, 降低了通信开销; 但因 CH-CM 使用非交互方式建立会话密钥, 节点易遭到捕获攻击。

Agrawal 等^[51]提出了基于中国剩余定理 (CRT, Chinese remainder theorem) 的密钥愈合管理方案。① 基本思路。网络部署前, KDC 需要为任意节点预置密钥 s_i 和身份标志 ID_i , 并将对应的密钥和身份标志存储在所属的组管理器 (GM) 中, GM 随机选择密钥种子生成辅助哈希链集 HK 和滑动窗口 w ; 随后 GM 选择会话密钥 K_j , 从 HK 中选择辅助密钥 KA_j , 使用节点密钥 s_i 计算 PRF 值, 通过 Hash 函数和 CRT 构造一组广播消息 $z_j = (B_{j-w}, B_{j-w+1}, \dots, B_{j-1}, B_j)$; 节点接收到广播消息后, 使用自身密钥 s_i 计算 PRF' 值, 与接收到的 PRF 值对比验证真实性; 在真实性和新鲜性验证后, 利用广播消息计算出会话密钥 K_j ; 当节点丢失 j 会话阶段的数据包, 可以根据 w 周期内的未来广播消息计算出会话密钥 K_j ; 同时节点可以请求邻居节点获得丢失的广播消息来恢复密钥。② 方案分析。引入了自愈和互愈策略, 具有较好的前、后向安全性, 能够抵抗欺骗攻击、抗重放攻击、抗共谋攻击, 提供身份认证和密钥确认, 非法节点很难通过愈合机制计算出密钥, 与现有的互愈方案相比, 降低了计算、通信和存储等成本。

Guo 等^[52]提出了基于双链和多项式的密钥自愈管理方案。① 基本思路。GM 首先根据安全参

数生成 t 次秘密多项式 $S(x)$ ，并选择出每个节点的标志秘密信息 s_i 、第 j 阶段的随机数 ε_j ，通过安全通道分配给每个节点秘密信息 $S_i = \{s_i, \varepsilon_i \cdot S(s_i)\}$ ；随后 GM 根据合法节点的 s_i 和会话密钥 K_j ，利用双链构建广播消息 B_j ；在第 j 阶段会话过程中，合法节点根据 s_i 和 B_j ，通过模幂运算计算出会话密钥 K_j ，并恢复丢失的会话密钥；在 j 阶段有新节点加入时，GM 发送标志秘密信息给新节点，新节点计算出会话组密钥，但不能恢复第 j 阶段之前会话组密钥，进而保证后向安全性；在 j 阶段有旧节点退出时，GM 只需在下一阶段排除旧节点标志的秘密信息完成密钥更新，保证前向安全性。② 方案分析。能够抵抗多项式因子分解攻击，保证前向和后向安全性，具有节点撤销和抗共谋攻击能力，存储开销恒定，考虑到会话密钥更新的通信开销问题，设定周期对节点加入或退出进行密钥更新操作，减少了通信开销，但不适用于快速动态变化的网络。

Tsitaitse 等^[53]对智能电网提出了基于指数多项式的密钥自愈管理方案。① 基本思路。KDC 在初始化阶段选择一个 t 次秘密多项式 $h(x)$ 与远程终端单元 (RTU, remote terminal unit) 节点的身份标志 u_i ，生成秘密信息 $s_i = \{h(u_i)\}$ ，通过安全通道分发至各节点；KDC 通过撤销多项式 $v_j(x)$ 和秘密多项式 $h_j(x)$ 构造指数多项式 $Q_j(x)$ ，随后将密钥更新参数 δ_j 进行对称加密后生成 $E_{K_j}(\delta_j)$ ，并将其与指数多项式生成广播消息 B_j ，在一定滑动窗口周期 d 内，将 $\{B_{j-d} \parallel B_2 \parallel \dots \parallel B_j\}$ 发送至所有用户节点；用户节点根据接收到的 B_j 和自身 s_i 计算出会话密钥 K_j ，并解密出 δ_j ，进而更新秘密信息 $h_{j+1}(u_i) = h_j(u_i) + \delta_j$ ；若节点在滑动窗口周期内 $j_1 \sim j_2$ ($j-d \leq j_1 < j_2 < j$)，阶段通信中断，未收到广播消息，在 j 阶段收到广播消息，那么可以根据 B_{j_1} 恢复密钥 K_{j_1} ，更新秘密信息 $h_{j_1+1}(u_i) = h_{j_1}(u_i) + \delta_{j_1}$ ，进而可以恢复出会话密钥；新节点加入，KDC 验证身份后分发节点 $s_i = \{h(u_i)\}$ ，进入下一个阶段会话更新密钥，节点退出，KDC 将节点计入撤销集，并进入下一个阶段会话更新密钥。② 方案分析。保证前向和后向

安全性，具有节点撤销能力和抗共谋能力；同时存储开销恒定，引入了滑动窗口周期，降低了通信开销，延长网络寿命，不会因广播消息过大导致通信负载，有效提高了通信效率，但计算开销并不占有优势，而且对于滑动窗口的选择比较重要。

Li 等^[54]针对无人机网络不稳定提出了基于区块链的密钥自愈管理方案。① 基本思路。首先地面控制站 (GCS, ground control station) 构建一个私有区块链 UAV_BC，用于记录成员节点变化信息，分发和存储组密钥广播消息；随后，GCS 通过共识机制广播更新区块 Block_n ，节点收到更新区块 Block_n ，与本地存储最新的区块链对比验证合法性，验证通过后对本地区块链和组密钥进行更新，利用滑动窗口存储最新的区块；若节点出现通信中断，可以根据不同的攻击模型选择愈合机制：一是基于区块链存储数据信任的基本愈合协议；二是能够抵抗无人机被压制攻击（电磁干扰）的增强型密钥自愈协议。② 方案分析。动态管理成员身份，针对不同攻击模型，设计了基本型和增强型 2 种密钥自愈管理机制，在有限的计算和存储开销下，能够高效恢复丢失密钥，进而抵抗各类攻击。

Vadlamudi 等^[55]提出了一种基于向量空间最大距离可分离 (MDS) 码^[56]的自愈密钥管理方案。① 基本思路。GM 首先根据第 j 阶段簇组大小生成 MDS 码，并公开生成器矩阵 M_j ；随后，GM 随机选择组密钥 K_j ，与节点秘密信息 $H_j(x_{i_k})$ 和 M_j 构造码字 C_j ，将所有阶段的身份集 I_j 、 M_j 以及 C_j 相关参数用来构造广播消息 B_j 。当 CM 接收到第 j 阶段的 B_j ，通过转换 M_j 结构，与 B_j 进行重构码字，进而计算出组密钥 K_j ；即使在 j_1 阶段出现通信中断未接到 B_{j_1} ，在 j 阶段恢复通信接收到广播消息 B_j ，因为 B_j 包含未接收到会话阶段的参数，容易计算出中断会话阶段的组密钥。节点加入或退出，在密钥生成、广播和密钥恢复阶段进行更新生成器矩阵，完成密钥更新。② 方案分析。方案灵活性较高，方便任意节点间通信，撤销节点数量和设置不受限制，被撤销的节点可以在后续会话阶段重新加入，能够抵抗共谋攻击和内部攻击，具有较好前向和后向安全性，但每

次会话阶段需要传输新的生成器矩阵, 通信开销较大。

代紫梦等^[57]提出了一种基于指数算法的密钥自愈管理方案。① 基本思路。GM 首先从有限域中随机选择 t 次多项式 $f(x)$ 和随机数 ε_j 构造私钥 $S_i = \{s_i, \varepsilon_j \cdot f(s_i)\}$ 并分发给对应节点; 随后, GM 随机选择种子 S_1^{FB} 构造 Hash 链 $k_2 = k_1 \cdot H(S_1^{\text{FB}}), k_3 = k_2 \cdot S_2^{\text{FB}} = k_2 \cdot H^2(S_1^{\text{FB}}), \dots, k_j = k_{j-1} \cdot S_{j-1}^{\text{FB}} = k_{j-1} \cdot H^{j-1}(S_1^{\text{FB}})$; 结合身份标志使用拉格朗日插值法构造多项式 $A_j(x)$; 使用指数函数将 $A_j(x)$ 和 Hash 链构造广播消息 B_j , 合法节点收到 B_j 后, 利用自身私钥计算出 k_j , 进而解密出会话组密钥 K_j ; 若节点在 $j_2 (j_1 \leq j_2 \leq j < m)$ 会话阶段丢失数据包, 可以根据广播 B_j 和 Hash 链恢复会话组密钥; 最后一次会话阶段 m 丢失数据包, 可以请求邻居节点获得广播消息 B_m , 进而计算恢复 K_j 。② 方案分析。引入随机数隐藏节点私钥, 基于指数算法和 Hash 链构造广播消息, 具有较好的保密性, 能够抵抗共谋攻击, 保证前向和后向安全, 有效降低了存储和通信开销。

Chien 等^[58]提出了基于系统分组码^[59]的高效自愈密钥管理方案。① 基本思路。GM 首先生成特殊的系统分组码发生器矩阵 $M(n, k)$, Hash 函数 h_1 和 h_2 , 并选择密钥 k_i 分发给任意节点 U_i ; GM 在会话第 j 阶段随机选择组密钥 gk_j 和随机数 r_j , 根据节点在 j 阶段传输的消息数 s , 计算出身份认证令牌 $\text{seed}_{j,i}^s = h_2^s(h_1(k_i, r_j))$; 将组密钥、身份认证令牌集和生成器矩阵生成广播消息 BC_j , 在滑动窗口周期 p 内将广播消息 $\{\text{BC}_{j-p}, \dots, \text{BC}_j\}$ 分发至合法节点; 节点接收到 BC_j , 可以根据 BC_j 通过矩阵乘法恢复出组密钥 $\{gk_{j-p}, \dots, gk_j\}$ 和身份认证令牌, 进而使用身份认证令牌生成消息身份验证码 (MAC), 使用组密钥建立安全通信。② 方案分析。具有较好的前向和后向安全性, 节点加入或退出时较为灵活, 网络具有较好的鲁棒性, 通过发生器矩阵降低了计算和通信开销, 使用消息源身份认证, 有助于入侵检测和识别。但在每个会话阶段传输信息较多,

导致通信开销较大, 不能满足高速动态不稳定的网络需求。

综上所述, 表 2 对本节论述的密钥愈合管理方案的性能进行了总结比较。

3.3 动态管理方案

集群网络经常会出现节点加入、退出等频繁操作, 导致集群网络拓扑结构变化, 需要对密钥进行动态管理, 周期性或基于网络拓扑结构变化进行更新, 能够提高网络安全和延长网络生命周期^[7, 60]。Younis 等^[61]针对大规模集群网络提出了一种基于排他系统 (EBS) 的轻量级密钥管理方案 (SHELL 方案); Eltoweissy 等^[62]对 SHELL 方案进行改进提出了 LOCK 方案, 使用两层 EBS 对密钥进行动态管理, 减少集群密钥更新的时间时延和能量消耗; Divya 等^[63]提出一种基于汉明距离的密钥动态管理方案, 防止节点共谋攻击; Zhang 等^[64]、Guo 等^[65]和关志涛等^[66]提出了基于多项式的密钥动态管理方案, 在降低各类成本同时提高网络安全性能。下面重点论述近年来有关集群网络的密钥动态管理方案。

Chella 等^[67]提出了一种基于角度运动的高效节能密钥动态管理方案。① 基本思路。将集群网络分成若干簇组, 组内分为若干扇区, 每个 CH 存储一个数据列表, 负责控制和管理节点, 检查跟踪节点移动情况, 避免其他节点干扰。同时在网络部署前为所有节点预分发私钥, 与 CH 建立安全通信。节点从簇组 CG_i 向簇组 CG_j 移动时, 簇组 CG_i 内所有节点删除与移动节点的共享密钥, 移送节点向 CH_j 发送请求, CH_j 请求 CH_i 确认身份, CH_i 收到请求后, 将其添加到自身数据列表中, 符合要求后确认身份, CH_j 收到确认回复后分发新的私钥给移动节点, 移动节点删除原来私钥和相对 CH_i 的角值, 进而节点与 CH_j 使用新的密钥和余弦值进行定向加密通信。组内节点间通过自身存储的公/私钥对进行相互认证, 建立共享密钥, 在 CH 授予权限后可以建立安全通信。② 方案分析。允许网络节点位置的改变, CH 主动检测节点移动情况进行密钥更新, 引入角余弦值生成定向的安全密钥, 提高了安全性, 使用定向收发器降低了传输成本和传输能量, 但方案部

表2 密钥愈合管理方案性能比较
Table 2 Performance comparison of the key healing management scheme

文献	愈合机制	技术基础	安全优势		效率优势
李德全等 ^[50]	自愈	椭圆曲线	抗欺骗攻击	抗重放攻击	通信开销↓
		Hash 函数	抗被动攻击	节点撤销	计算开销↓
			前向安全性	后向安全性	
Agrawal 等 ^[51]	自愈+互愈	中国剩余定理	身份认证	抗欺骗攻击	存储开销↓
		Hash 函数	抗共谋攻击 (mt)	抗重放攻击	通信开销↓
		伪随机函数	前向安全性	后向安全性	计算开销↓
Guo 等 ^[52]	自愈	t 次多项式	多项式因子分解攻击	抗共谋攻击 (mt)	存储开销↓
		Hash 函数	前向安全性 (mt)	后向安全性	通信开销↓
Tsitaitsse 等 ^[53]	自愈	指数多项式	抗共谋攻击 (mt)	后向安全性 (mt)	存储开销↓
			前向安全性 (mt)		通信开销↓
Li 等 ^[54]	互愈	区块链	身份认证	抗毁性	计算开销↓
		Hash 函数	抗欺骗攻击	抗重放攻击	通信开销↓
			抗抑制攻击		时间开销↓
Vadlamudi 等 ^[55]	自愈	MDS 码	抗毁性	抗共谋攻击	计算开销↓
		Hash 函数	前向安全性	后向安全性 (mt)	
代紫梦等 ^[57]	自愈+互愈	指数多项式	抗共谋攻击 (mt)	后向安全性 (mt)	存储开销↓
		Hash 函数	前向安全性 (mt)		通信开销↓
		拉格朗日插值法			
Chien 等 ^[58]	自愈	系统分组码	身份认证	抗毁性	计算开销↓
		Hash 函数	抗共谋攻击	前向安全性	通信开销↓
			后向安全性		

署定向收发器一定程度增加了成本，而且建立节点间共享密钥需要较大通信开销。

Seo 等^[68]提出了一种无证书的有效动态密钥管理方案。① 基本思路。方案建立 4 类密钥，包括无证书公/私钥对、节点密钥、配对密钥和集群密钥。首先 BS 在节点 L_i 注册时生成系统参数 Ω 、无证书私钥 $sk_{L_i} = (d_{L_i}, x_{L_i})$ 和公钥 $pk_{L_i} = (P_{L_i}, R_{L_i})$ ，以及节点个人密钥 $K_{L_i}^0$ ，并将 $\{\Omega, sk_{L_i}, pk_{L_i}, K_{L_i}^0\}$ 存储在节点，相邻节点通过广播消息，利用无证书公/私钥对建立长期配对主密钥 K_{AB} ，然后利用 HMAC 对主密钥进行操作，生成短期配对加密密钥 k_{AB} ，对节点之间感知数据进行加密；CH _{j} 生成组密钥 GK_j ，并通过 CH-CM 的配对密钥加密后进行传输验证，验证通过可以利用组密钥建立组内安全通信；当出现节点在簇组之间移动以及节点加入或退出时，CH 按照生成规则重新更新组密钥。② 方案分析。方案的配对密钥可以在两

个节点之间有效共享，不需要复杂的配对操作和证书交换，降低了计算和证书管理开销；支持节点移动性操作，密钥更新操作较为简便，使用多种密钥提高了密钥管理的安全性；但管理过程中多个独立加解密操作和多级传输操作需要较多的计算开销和时间开销。

梁濛^[69]提出了一种基于多属性决策逼近理想解排序 (TOPSIS) 分簇算法的密钥动态管理方案。① 基本思路。KDC 首先基于椭圆曲线的公钥组合技术生成公钥 PK 和私钥 SK，BS 和 CH 通过公/私钥对进行身份认证后，建立会话密钥 $K_{CH,BS}$ ，CM 基于 Shamir 的门限秘密管理方案 (门限值为 τ)，任意 τ 个 CM 利用存储的子密钥分量 k_{Ni} ，通过共享多项式 $f(x)$ 进行重构，利用 Lagrange 插值公式计算簇内组密钥 K ；CH 选择采用 TOPSIS 分簇算法，降低了 CH 选择的能量开销，延长了集群网络生命周期；新节点加入需 CH 进行身份认证，BS 为新节点分配密钥并进行

广播公开其入网消息；节点退出时，若为成员节点，CH 重新计算分发子密钥分量 k'_{Ni} ，更新组密钥 K ，若为 CH 节点，簇内剩余节点基于 TOPSIS 算法重新选择新 CH，新 CH 重新计算分发子密钥分量 k'_{Ni} ，更新组密钥 K 。② 方案分析。通过预置公钥矩阵组合会话密钥，降低节点存储空间，采用非对称密钥体制进行节点认证，提高了密钥管理安全性；基于密钥共享机制进行密钥管理，增强了密钥管理灵活性；采用 TOPSIS 算法进行簇头重选，降低了网络能耗；支持节点加入、退出等操作，具有较强的可拓展性，但计算开销较大。

Athmani 等^[70]提出一种高效动态认证和密钥管理方案。① 基本思路。首先基于预存的信息数据生成动态矩阵密钥 DKM，并根据发送或接收的信息进行动态更新；给节点预先分配唯一的对称网络密钥 IK，并使用向量 VIK 进行简化表示；随后，数据发送方和接收方使用动态矩阵密钥 DKM 生成动态密钥 DK，对数据进行加解密传输，簇内建立 2 种密钥（线性动态对密钥 LDK 和正交动态组密钥 ODK），其中 CH-CM、CM-CM 的 LDK 建立，通过发送数据节点 $node_x$ 对应在密钥矩阵中数据进行串联形成 $LDK = DMK_{x,2} \parallel DMK_{x,3} \parallel \dots \parallel DMK_{x,33}$ ，CH-CH 的正交动态组密钥 ODK 生成，通过异或运算 $DMK_{i,j} \oplus VIK_{i \bmod 32} (i = 1, 2, \dots, n_{CH})$ 进行串联形成，其中 n_{CH} 为 CH 数量。BS-CH、CH-CH 使用更高安全级别的对角动态组密钥 DDK，基于对角线 $DMK_{p,p}$ 通过异或运算 $DMK_{p-2,p} \oplus VIK_{n \bmod 32}$ 串联形成。节点加入和节点退出时较为简单有效，对 DKM 进行更新或初始化，进而完成密钥动态更新。② 方案分析。基于本地预分配信息生成密钥，根据不同运算规则优化建立不同安全级别的密钥，使用异或运算串联，降低了计算和通信开销。引入身份认证可以抵抗恶意节点攻击、女巫攻击和重放攻击，而且密钥动态变化可以抵抗欺骗攻击和暴力攻击，增强了安全性。但密钥更新节点存储的 DKM 更新频繁，造成较多开销。

Wang 等^[71]提出了基于二次多项式和拉格朗日插值多项式的动态密钥管理方案。① 基本思路。首先，基于傅里叶级数生成不同阶段的

认证密钥 K_i ，生成广播认证消息 $L(i)$ 进行身份认证；接着，节点利用认证密钥进行加密广播密钥信息，任意两个相邻节点 a 和 m 收到对方广播的密钥信息，可以建立会话密钥 $K_{am} = h(CG) = h(GC) = K_{ma}$ ；CM 生成密钥信息使用会话密钥加密传输 $E_{K_{am}}(m(i))$ ：

CM $\rightarrow$ CH $\rightarrow$ BS，BS 根据密钥信息 $m(i)$ 生成拉格朗日插值多项式函数 $y(x)$ 和组密钥 K_{CH_j} ，组合形成 $y'(x)$ 并发送至节点 BS $\rightarrow$ CH $\rightarrow$ CM，节点获得 K_{CH_j} 建立组内安全通信，BS-CH 之间的网络密钥 K_N 与组密钥 K_{CH_j} 建立方案相同；私有密钥的生成和管理方案类似于组密钥，但其多项式函数系数只能由对应节点求得，因此，CH 不能获得私有密钥，而 BS 和对应节点可以获得，建立一对一私有安全通信。密钥更新过程往往需要更新共享函数 $f(x)_{new}$ 和私有函数 $g(x)_{new}$ ，再按照上述密钥管理方案依次对会话密钥、组密钥、网络密钥和私有密钥进行更新。② 方案分析。该方案使用 5 种密钥，相互补充且独立使用，引入正向、反向认证方法对网络节点身份的合法性进行认证，解决了会话密钥独立性和连通性问题，避免组密钥单点故障问题，但方案在密钥生成和更新过程中需要传输信息较多，导致计算和通信开销较大。

Yousefpoor 等^[72]提出了基于模糊逻辑^[73]的动态智能密钥管理方案。① 基本思路。方案使用了 4 种密钥：私钥、簇组密钥、成对密钥和路径密钥。BS 从密钥源中随机选择一个私钥，并分配至集群网络中每个节点，用于 BS 与任意节点的安全通信；CH 负责簇组密钥生成，通过私钥进行加密分发至 CM；相邻 CH 之间建立成对密钥进行安全通信；非相邻 CH 之间利用 Mamdani 模糊推理机制来建立路径密钥，进行安全通信。新节点加入时，BS 验证身份合法后为新节点分配私钥，获取各 CH 坐标信息和成员节点数量的信息，运用 Mamdani 模糊推理机制选择最佳 CH，并将新节点添加其中，CH 更新簇组密钥，节点退出时，将需要撤销的密码分析节点加入 R 列表中，并对网络中的密钥进行撤销和更新。节点移动或

CH-CM 之间出现长时间通信中断时,原 CH 更新簇组密钥,移动节点按照与新节点加入网络的管理过程,加入新的簇组。② 方案分析。通过删除密码分析节点执行密钥更新,提高网络安全性,增强对密码分析攻击的恢复能力和抵抗力,具有较好前后向安全性,在建立路径密钥和节点加入过程中使用模糊逻辑,提高决策选择的准确性和智能化,降低网络能耗,延长网络寿命,但在引入模糊逻辑同时,增加了网络反应时延和通信开销。

Kumar 等^[74]提出基于 Hash 链的高效密钥动态管理方案。① 基本思路。初始网络阶段,BS 选择 Hash 函数,并生成 Hash 链密钥池和收敛递归公式;网络部署前,为节点预分配 Hash 密钥链、序列的第一项、递归函数以及身份标志 S_i ; 随后节点广播其 S_i 和 Hash 链给相邻节点进行密钥链匹配,建立共享密钥,若无法匹配,则利用 S_i 和随机生成函数生成随机数 N_i 和共享密钥;节点之间所有对密钥建立后,进行递归 Hash 运算,并根据节点的最小距离和最远能量权重选择 CH,CH 生成组密钥并分发至 CM,建立簇内安全通信;节点加入后,可以按照共享密钥机制建立安全通信,并且 CH 为新节点分发组密钥;若网络结构拓扑发生变化或 CH 更改,BS 可以根据需要为特定节点或所有节点更新密钥。② 方案分析。基于序列生成和更新密钥,使用 Hash 密钥链进行配对建立共享密钥,具有较低的存储和能耗开销,支持可拓展性且能够抵抗重放、复制和捕获攻击,但安全性与密钥链长度成正比,提高安全性需要增加密钥链长度,增加计算开销。

Arumugam 等^[75]提出了基于位置信息的自适应多级动态密钥管理方案。① 基本思路。网络部署前,BS 分发给任意节点相应的节点密钥,用于加密命令消息,建立 BS 与任何节点安全通信,使用公/私钥对计算出节点的非对称密钥 (K_{s_i}, r_{s_i}) ; 部署后,区域内节点通过检索位置信息向邻居节点广播身份标志符和公钥,进行身份验证后,建立区域内密钥安全通信;CH 负责创建区域密钥并分发至区域内 CM,保证区域内建立安全共享密钥;节点退出时,CH 向 BS 报告节点退出消息,并更新区域密钥;新节点加入时,

CH 向 BS 验证节点合法性后,更新区域密钥。② 方案分析。方案使用多种密钥建立安全通信,提高了密钥破解难度,密钥更新过程进一步增强了安全性,既能抵抗欺骗、重放、捕获等主动攻击,还能抵抗窃听攻击,存储和能耗开销有了较大改善,但方案基于位置信息,容易被攻击者根据位置区分攻击,且整个方案通信开销并不乐观。

综上,表 3 对本节论述的密钥动态管理方案的性能进行了总结比较。

4 研究热点及应用前景

4.1 研究热点

相对传统密钥管理方案,集群网络技术快速发展对密钥管理提出了更高要求和更大挑战。随着集群网络大量应用到实践中,安全问题日益凸显,高效适用的密钥管理方案需求更为迫切,近年来,学术界结合各种前沿技术探讨在不同应用场景下的密钥管理方案。本文综述了预分配、愈合和动态 3 种策略的密钥管理方案研究进展,下面归纳集群密钥管理相关研究热点。

(1) 跨域异构

随着通信网络发展和完善,逐渐将陆地、海洋、空中和太空多维度连接成空天地一体化网络(SAGIN, space-air-ground integrated network),SAGIN 拥有大量异构网络节点,如卫星、无人机、高空平台和地面基站^[76]。卫星节点、空中节点、地面节点需要实现跨域进行信息交互,且空域、地域往往由不同的网络异构设备组成;节点的硬件配件、资源性能、通信带宽不同,导致计算、通信、存储性能不同^[77]。在跨域异构的天地一体化网络应用场景下,卫星节点资源性能受限、通信时延长,近空飞行节点网络不稳定、通信易中断,陆上节点易遭受物理攻击,被安装窃听设备以致信息泄露等因素,给密钥管理方案带来极大挑战^[78]。因此,跨域异构集群网络的密钥管理方案在保证基础安全性的前提下,还应满足以下要求:① 轻量级设计,通信和计算成本低;② 兼容异构网络节点;③ 不同域之间能快速融合和切换。

(2) 集群认证

在集群网络中,网络节点数量规模较大,而且节点之间通过自主动态组网与协同,快速完成

表3 密钥动态管理方案性能比较
Table 3 The key dynamic management scheme

文献	技术基础	安全优势		灵活优势	效率优势
Chella 等 ^[67]	余弦函数 角度运动	身份验证	节点撤销	连通性	通信开销↓
		抗毁性	前向安全性	可伸缩性	计算开销↓
		后向安全性			
Seo 等 ^[68]	椭圆曲线 Hash 函数	节点撤销	抗毁性	可伸缩性	通信开销↓
		抗欺骗攻击	前向安全性		计算开销↓
		后向安全性			
梁濛 ^[69]	椭圆曲线 Hash 函数 TOPSIS 算法	身份认证	抗毁性	连通性 (100%)	存储开销↓
		抗重放攻击	抗 DoS 攻击	可伸缩性	计算开销↓
		抗欺骗攻击	抗共谋攻击 (<i>mt</i>)		能耗开销↓
Athmani 等 ^[70]	动态矩阵密钥	身份验证	抗毁性	可伸缩性	存储开销↓
		抗欺骗攻击	抗重放攻击		计算开销↓
		前向安全性	后向安全性		能耗开销↓
Wang 等 ^[71]	二次多项式 拉格朗日插值多项式	节点撤销	抗共谋攻击	连通性 (100%)	存储开销↓
		抗毁性	前向安全性	可伸缩性	计算开销↓
		后向安全性			
Yousefpoor 等 ^[72]	Mamdani 模糊推理机制	节点撤销	抗毁性	可伸缩性	通信开销↓
		前向安全性	后向安全性		存储开销↓
					能耗开销↓
Kumar 等 ^[74]	收敛递归公式 Hash 密钥链	节点撤销	抗毁性	连通性 (100%)	存储开销↓
		抗重放攻击	抗复制攻击	可伸缩性	通信开销↓
				可扩展性	
Arumugam 等 ^[75]	公私钥对 Hash 函数	身份认证	抗毁性	连通性	存储开销↓
		抗重放攻击	抗欺骗攻击	可伸缩性	能耗开销↓
		抗窃听攻击	抗黑洞攻击		
		前向安全性	后向安全性		

组网, 具有动态变化的灵活性, 但攻击者往往会利用这种高程度的自主协同进行有效攻击, 窃取秘密信息, 实施内部攻击, 瘫痪整个集群网络体系, 因此需要对集群网络节点进行安全的身份认证, 提高密钥管理方案的安全性^[79]。集群网络认证难度较大, 需要对数量较多的网络节点实施批量动态认证, 在不可靠的无线通信网络环境下进行群组加入认证, 容易导致认证失败, 而研究集群身份认证对网络安全和密钥管理具有重要意义^[80]。

(3) 愈合机制

集群无线网络不可靠容易出现通信中断现象, 节点数量规模较大且具有高速移动特性, 部分节点可能会出现广播数据包丢失情况, 虽然自愈机制根据后续接收到的广播密钥更新消息能够

恢复密钥, 不需要向密钥分发中心 (KDC) 请求重发广播消息, 一定程度上降低了通信开销, 但广播消息需要包括以前阶段的密钥信息, 而且在当前会话阶段是无法恢复的, 只有在后续收到广播消息才能进行密钥恢复; 而自愈机制可以借助其他邻居共享丢失的广播消息进行恢复, 提高了实时响应性, 具有重要应用价值^[81]。因此, 适合不稳定无线网络的密钥愈合管理方案是未来的重要研究方向^[82]。

(4) 技术融合

随着前沿技术不断发展, 集群密钥管理不再局限于传统管理策略, 而是与相关技术融合进行密钥管理, 提升安全性和效率, 是未来密钥管理的研究重点方向。一是结合人工智能技术管理, 根据节点数量、前期密钥更新决策和当前网络

安全等级,通过强化学习算法,不断优化密钥更新频率和密钥长度,获得密钥最优更新策略,提高密钥管理的科学性和智能化^[83]。二是结合区块链技术管理,利用区块链去中心化、不易篡改和可追溯性等特征,设计密钥管理区块链,并使用智能合约进行密钥协商,无须第三方参与,自主分发和更新密钥,还可记录密钥更新过程,方便后续安全性检查,确保密钥管理机密性^[84-85]。三是结合动态分簇技术管理,引入动态分簇算法,对网络进行分层分簇,在节点加入、簇组合并或分裂等动态变化过程中,智能选出最佳簇头进行分发,便于动态更新密钥,延长网络密钥管理生命周期,增强密钥管理的灵活性。

4.2 应用前景

随着信息网络普遍应用,网络攻击手段不断演化升级,信息安全成为令人关注的话题,如何在复杂集群网络环境下维护网络安全,确保信息安全可靠传输,成为社会关注的重要安全问题,而密钥管理是信息安全的基石,具有广阔的应用前景。

(1) 泛在物联安全

随着5G、物联网技术的快速发展,泛在物联成为未来发展趋势,将现有的互联网拓展到物品,构建万物互联的网络,实现对物的智能化管理和信息收集。大量的异构节点信息连接和交互,形成了复杂的集群网络,容易遭受到各类网络安全攻击。而集群密钥管理给规模较大网络通信安全提供了解决方案,对网络节点进行分层分簇管理,可以完成对大量节点进行身份认证和数据加密,维护泛在物联网络的通信安全。

(2) 全域作战需求

未来作战不再是单一维度作战,而是高度融合陆、海、空、网、天、电等作战领域,协同多域作战力量,开展联合全域作战行动^[86]。完成全域作战需要强大的空天网络支撑和安全的指挥通信链路,进行跨域传输共享战斗数据。考虑到军事通信安全需求,在全域作战网络体系需要进行密钥管理,对所传输的数据进行加密操作,保证军事秘密安全传输,集群网络密钥管理为构建全

域安全通信链路提供了技术支撑。

(3) 智慧城市建设

智慧城市建设如火如荼,通过现代化信息技术,将社区、医疗、交通、政务、社会治理等业务组成复杂的城市系统,因其节点繁杂多样,对其安全攻击方法多样,危害性较大,而且正常运行需要对大量数据进行汇聚融合,数据安全成为突出问题。如何解决以“数据安全”为核心的智慧城市安全,成为重要研究难题,而密码技术作为信息安全的基础和核心技术,是智慧城市建设的安全基石,为智慧城市网络建立密码应用方案^[87],需要解决密码管理的核心技术密钥管理,因此,集群网络密钥管理对建设智慧城市具有重要的安全意义。

5 结束语

随着物联网、车联网、无人机集群技术快速发展,集群网络安全问题日益突出,集群密钥管理成为研究热点。本文介绍了集群网络的典型模型、特性,并分析了集群密钥管理的流程步骤和评价指标,根据网络部署前和部署后管理过程,总结分析了近年来有关的集群密钥管理方案研究进展情况,将其分为预分配管理、愈合管理、动态管理三类,最后展望了集群密钥管理的研究热点和应用前景。随着信息网络的飞速发展,网络结构将愈加复杂,传统单一模式的密钥管理不适用于未来复杂网络场景。集群密钥管理作为集群网络安全的技术基础和核心,为复杂网络体系的信息数据安全传输提供了有效的解决思路。目前,不存在完美的密钥管理方案,能满足所有安全性和成本效率,因此,实际应用中,需要把握适度原则,根据具体场景设计适合密钥管理方案,提高密钥管理的实践安全性,加快与区块链、人工智能、量子等技术融合,使得密钥管理更加智能化、科学化、高效化。

参考文献:

- [1] GRASSÉ P. La reconstruction du nid et les coordinations interindividuelles chez *Bellicositermes natalensis* et *Cubitermes* sp. la théorie de la stigmergie: Essai d'interprétation du comportement des termites constructeurs[J]. *Insectes Sociaux*, 1959, 6(1): 41-80.

- [2] 秦小林, 罗刚, 李文博, 等. 集群智能算法综述[J]. 无人系统技术, 2021, 4(3): 1-10.
QIN X L, LUO G, LI W B, et al. A review of swarm intelligence algorithms[J]. Unmanned Systems Technology, 2021, 4(3): 1-10.
- [3] 刘文婷, 杜春玲, 范修斌, 等. CFL 密钥管理研究[J]. 信息安全研究, 2016, 2(7): 628-638.
LIU W T, DU C L, FAN X B, et al. Study on the CFL's key management[J]. Journal of Information Security Research, 2016, 2(7): 628-638.
- [4] HE X, NIEDERMEIER M, DE MEER H. Dynamic key management in wireless sensor networks: a survey[J]. Journal of Network and Computer Applications, 2013, 36(2): 611-622.
- [5] BARSKAR R, CHAWLA M. A survey on efficient group key management schemes in wireless networks[J]. Indian Journal of Science and Technology, 2016, 9(14): 1-16.
- [6] SINGH P, GILL N S. A survey on key management schemes in wireless ad hoc networks[J]. International Journal of Applied Engineering Research, 2018, 13(1): 268-272.
- [7] YOUSEFPOOR M S, BARATI H. Dynamic key management algorithms in wireless sensor networks: a survey[J]. Computer Communications, 2019, 134: 52-69.
- [8] PARTHASARATHI P, SHANKAR S, NIVEDHA S. A survey on dynamic key management system in secure group communication[C]//2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS). 2020: 1440-1443.
- [9] NITHYA B. Cluster based key management schemes in wireless sensor networks: a survey[J]. Procedia Computer Science, 2020, 171: 2684-2693.
- [10] JAWAD H M, NORDIN R, GHARGHAN S K, et al. Energy-efficient wireless sensor networks for precision agriculture: a review[J]. Sensors, 2017, 17(8): 1781.
- [11] ANNAPURNA H S, SIDDAPPA M. A technique for multitier key distribution for securing group communication in WSN[M]//Emerging Research in Computing, Information, Communication and Applications. 2016: 87-94.
- [12] WANG W, WEI J, ZHAO S, et al. Energy efficiency resource allocation based on spectrum-power tradeoff in distributed satellite cluster network[J]. Wireless Networks, 2020, 26(6): 4389-4402.
- [13] ALI Z A, HAN Z, MASOOD R J. Collective motion and self-organization of a swarm of UAVs: a cluster-based architecture[J]. Sensors, 2021, 21(11): 3820.
- [14] SHIDDHARTHY R. A selective reliable communication to reduce broadcasting for cluster based VANET[J]. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021, 12(3): 4450-4457.
- [15] ACHROUFENE A, CHELIK M, BOUADEM N. Modified CSMA/CA protocol for real-time data fusion applications based on clustered WSN[J]. Computer Networks, 2021, 196: 108243.
- [16] WANG G, KIM S, KANG D, et al. Lightweight key renewals for clustered sensor networks[J]. Journal of Networks, 2010, 5(3): 300-312.
- [17] KUMAR V, MALIK N. Enhancing the connectivity and resiliency of random key pre-distribution schemes for wireless sensor network[J]. International Journal of System Assurance Engineering and Management, 2021: 1-8.
- [18] BLOM R. An optimal class of symmetric key generation systems[C]//Workshop on the Theory and Application of Cryptographic Techniques, 1984: 335-338.
- [19] BLUNDO C, DE SANTIS A, HERZBERG A, et al. Perfectly secure key distribution for dynamic conferences[J]. Information and Computation, 1998, 146(1): 1-23.
- [20] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. 2002: 41-47.
- [21] CHAN H, PERRIG A, SONG D. Random key pre-distribution schemes for sensor networks[C]//Proceedings of the 2003 Symposium on Security and Privacy. 2003: 197-213.
- [22] DU W, DENG J, HAN Y S, et al. A pairwise key pre-distribution scheme for wireless sensor networks[J]. ACM Transactions on Information and System Security (TISSEC), 2005, 8(2): 228-258.
- [23] LIU D, NING P. Location-based pairwise key establishments for static sensor networks[C]//Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. 2003: 72-82.
- [24] ZHU S, SETIA S, JAJODIA S. LEAP+ efficient security mechanisms for large-scale distributed sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2006, 2(4): 500-528.
- [25] 张记, 杜小妮, 李旭, 等. 安全的无线传感器网络密钥预分配方案[J]. 计算机应用, 2013, 33(7): 1851-1853.
ZHANG J, DU X N, LI X, et al. Secure key pre-distribution scheme for wireless sensor networks[J]. Journal of Computer Applications, 2013, 33(7): 1851-1853.
- [26] 贺智明, 曹谦. 传感器网络多密钥空间分层密钥预分配方案[J]. 计算机应用与软件, 2014, 31(11): 326-329.
HE Z M, CAO Q. A hierarchical key preallocation scheme for multiple key spaces in wireless sensor network[J]. Computer Applications and Software, 2014, 31(11): 326-329.
- [27] 赵然, 方承志. 分簇式无线传感器网络密钥预分配方案[J]. 计算机工程与设计, 2016, 37(2): 345-348.
ZHAO R, FANG C Z. Key pre-distribution scheme for clustered wireless sensor network[J]. Computer Engineering and Design, 2016, 37(2): 345-348.
- [28] DAI H, XU H. Key pre-distribution approach in wireless sensor networks using LU matrix[J]. IEEE Sensors Journal, 2010, 10(8): 1399-1409.
- [29] CHAKAVARIKA T T, GUPTA S K, CHAURASIA B K. Energy efficient key distribution and management scheme in wireless sensor networks[J]. Wireless Personal Communications, 2017, 97(1): 1059-1070.
- [30] YI C, AGRAWAL D P. An improved key distribution mechanism for

- large-scale hierarchical wireless sensor networks[J]. *Ad Hoc Networks*, 2007, 5(1): 35-48.
- [31] KRISHNAPPA V, NARAYANAGOWDA S. A novel technique for improving the security of WSN using random key pre-distribution scheme[J]. *International Journal of Intelligent Engineering and Systems*, 2019, 12(2): 33-41.
- [32] KUMAR A, BANSAL N, PAIS A R. New key pre-distribution scheme based on combinatorial design for wireless sensor networks[J]. *IET Communications*, 2019, 13(7): 892-897.
- [33] 陈虹旭, 李晓坤, 徐龙, 等. 泛在电力物联网的多项式密钥管理算法研究[J]. *智能计算机与应用*, 2020, 10(8): 140-143.
- CHEN H X, LI X K, XU L, et al. Research on polynomial key management algorithm ubiquitous in power internet of things[J]. *Intelligent Computer and Applications*, 2020, 10(8): 140-143.
- [34] PREMAMAYUDU B, RAO B T, RAO K V, et al. Key pre-distribution protocol for node to node for wireless sensor networks[J]. *Annals of the Romanian Society for Cell Biology*, 2021, 25(4): 16769-16779.
- [35] TIAN B, HAN S, PARVIN S, et al. Self-healing key distribution schemes for wireless networks: a survey[J]. *Computer Journal*, 2011, 54(4): 549-569.
- [36] SHAMIR A. How to share a secret[J]. *Communications of the ACM*, 1979, 22(11): 612-613.
- [37] STADDON J, MINER S, FRANKLIN M, et al. Self-healing key distribution with revocation[C]//*Proceedings 2002 IEEE Symposium on Security and Privacy*. 2002: 241-257.
- [38] LIU D, NING P, SUN K. Efficient self-healing group key distribution with revocation capability[C]//*Proceedings of the 10th ACM Conference on Computer and Communications Security*, 2003: 231-240.
- [39] SÁEZ G. On threshold self-healing key distribution schemes[C]//*IMA International Conference on Cryptography and Coding*. 2005: 340-354.
- [40] TIAN B M, HE M X. A self-healing key distribution scheme with novel properties[J]. *International Journal of Network Security*, 2008, 7(1): 114-119.
- [41] 曹帅, 张串绒, 宋程远. 具有抗合谋攻击能力的自治愈合群组密钥管理方案[J]. *计算机应用*, 2011, 31(10): 2692-2693.
- CAO S, ZHANG C R, SONG C Y. A self-healing group key management scheme with collusion resistance[J]. *Journal of Computer Applications*, 2011, 31(10): 2692-2693.
- [42] TIAN B, HAN S, DILLON T S, et al. A self-healing key distribution scheme based on vector space secret sharing and one way hash chains[C]//*2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks*. 2008: 1-6.
- [43] GU J, XUE Z. An efficient self-healing key distribution with resistance to the collusion attack for wireless sensor networks[C]//*2010 IEEE International Conference on Communications*. 2010: 1-5.
- [44] 李林春, 李建华, 潘军. 无线传感器网络中具有撤销功能的自愈组密钥管理方案[J]. *通信学报*, 2009, 30(12): 12-17.
- LI L C, LI J H, PAN J. Self-healing group key management scheme with revocation capability for wireless sensor networks[J]. *Journal on Communications*, 2009, 30(12): 12-17.
- [45] JIANG Y, LIN C, SHI M, et al. Self-healing group key distribution with time-limited node revocation for wireless sensor networks[J]. *Ad Hoc Networks*, 2007, 5(1): 14-23.
- [46] TIAN B, HAN S, DILLON T S. A self-healing and mutual-healing key distribution scheme using bilinear pairings for wireless networks[C]//*2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*. 2008: 208-215.
- [47] RAMS T, PACYNA P. Long-lived self-healing group key distribution scheme with backward secrecy[C]//*2013 Conference on Networked Systems*. 2013: 59-65.
- [48] TIAN B, HAN S, HU J, et al. A mutual-healing key distribution scheme in wireless sensor networks[J]. *Journal of Network and Computer Applications*, 2011, 34(1): 80-88.
- [49] AGRAWAL S, PATEL J, DAS M L. Pairing based mutual healing in wireless sensor networks[C]//*2016 8th International Conference on Communication Systems and Networks (COMSNETS)*. 2016: 1-8.
- [50] 李德全, 张习勇, 张婷婷, 等. 具有私钥自愈能力的DTN密钥管理方案[J]. *网络与信息安全学报*, 2017, 3(4): 26-31.
- LI D Q, ZHANG X Y, ZHANG T T, et al. Key management scheme with private key self-healing ability in DTN[J]. *Chinese Journal of Network and Information Security*, 2017, 3(4): 26-31.
- [51] AGRAWAL S, DAS M L. Mutual healing enabled group-key distribution protocol in wireless sensor networks[J]. *Computer Communications*, 2017, 112: 131-140.
- [52] GUO H, ZHENG Y, LI X, et al. Self-healing group key distribution protocol in wireless sensor networks for secure IoT communications[J]. *Future Generation Computer Systems*, 2018, 89: 713-721.
- [53] TSITAITSE T J, CAI Y, DITTA A. Secure self-healing group key distribution scheme with constant storage for SCADA systems in smart grid[J]. *Wireless Personal Communications*, 2018, 101(3): 1749-1763.
- [54] LI X, WANG Y, VIJAYAKUMAR P, et al. Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(11): 11309-11322.
- [55] VADLAMUDI C V, VADLAMUDI S P D. A novel self - healing key distribution scheme based on vector space access structure and MDS codes[J]. *International Journal of Communication Systems*, 2019, 32(16): 4088-4097.
- [56] TENTU A N, PAUL P, VENKAIAH V C. Computationally perfect compartmented secret sharing schemes based on MDS codes[J]. *International Journal of Trust Management in Computing and Communications*, 2014, 2(4): 353-378.

- [57] 代紫梦, 王方伟, 王长广. WSN 中基于指数算法的互愈组密钥分配方案[J]. 计算机与数字工程, 2019, 47(1): 180-185.
- DAI Z M, WANG F W, WANG C G. Exponential arithmetic based on mutual-healing group key distribution scheme for WSN[J]. Computer and Digital Engineering, 2019, 47(1): 180-185.
- [58] CHIEN H. Self-healing group key distribution facilitating source authentication using block codes[J]. Security and Communication Networks, 2021(6).
- [59] AYANOGLU E, CHIH-LIN I, GITLIN R D, et al. Diversity coding: Using error control for self-healing in communication networks[C]//IEEE INFOCOM'90: Ninth Annual Joint Conference of the IEEE Computer and Communications Societies, 1990: 95-104.
- [60] SINGH A, TENTU A N, VENKAIAH V C. A dynamic key management paradigm for secure wireless ad hoc network communications[J]. International Journal of Information and Computer Security, 2021, 14(3-4): 380-402.
- [61] YOUNIS M F, GHUMMAN K, ELTOWEISSY M. Location-aware combinatorial key management scheme for clustered sensor networks[J]. IEEE transactions on parallel and distributed systems, 2006, 17(8): 865-882.
- [62] ELTOWEISSY M, MOHARRUM M, MUKKAMALA R. Dynamic key management in sensor networks[J]. IEEE Communications magazine, 2006, 44(4): 122-130.
- [63] DIVYA R, THIRUMURUGAN T. A novel dynamic key management scheme based on hamming distance for wireless sensor networks[C]//2011 International Conference on Computer, Communication and Electrical Technology (ICCCET). 2011: 181-185.
- [64] ZHANG Y, SHEN Y, LEE S. A cluster-based group key management scheme for wireless sensor networks[C]//2010 12th International Asia-Pacific Web Conference. 2010: 386-388.
- [65] GUO S, QIAN Z. A compromise-resilient pair-wise rekeying protocol in hierarchical wireless sensor networks[J]. Computer Systems Science and Engineering, 2010, 25(6): 315-326.
- [66] 关志涛, 徐月, 伍军. 传感器网络中基于三元多项式的密钥管理方案[J]. 通信学报, 2013, 34(12): 71-78.
- GUAN Z T, XU Y, WU J. Ternary polynomial based key management scheme for wireless sensor network[J]. Journal on Communications, 2013, 34(12): 71-78.
- [67] CHELLA THEVAR G K, ROHINI G. Energy efficient geographical key management scheme for authentication in mobile wireless sensor networks[J]. Wireless Networks, 2017, 23(5): 1479-1489.
- [68] SEO S H, WON J, SULTANA S, et al. Effective key management in dynamic wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security, 2017, 10(2): 371-383.
- [69] 梁濛. 一种动态的分簇无线传感器网络密钥管理方案[D]. 西安: 西安理工大学, 2018.
- LIANG M. A dynamic clustering wireless sensor networks key management scheme[D]. Xi'an: Xi'an University of Technology, 2018.
- [70] ATHMANI S, BILAMI A, BOUBICHE D E. EDAK: an efficient dynamic authentication and key management mechanism for heterogeneous WSNs[J]. Future Generation Computer Systems, 2019, 92: 789-799.
- [71] WANG X, YANG Z, FENG Z, et al. A WSN layer-cluster key management scheme based on quadratic polynomial and lagrange interpolation Polynomial[J]. Sensors, 2020, 20(16): 4388.
- [72] YOUSEFPOOR M S, BARATI H. DSKMS: A dynamic smart key management system based on fuzzy logic in wireless sensor networks[J]. Wireless Networks. 2020, 26(4): 2515-2535.
- [73] DE SILVA C W. Intelligent control: fuzzy logic applications[M]. Boca Raton: CRC press, 2018.
- [74] KUMAR V, MALIK N, DHIMAN G, et al. Scalable and storage efficient dynamic key management scheme for wireless sensor network[J]. Wireless Communications and Mobile Computing, 2021: (7).
- [75] ARUMUGAM V, SESHASAYANAM A. An adaptive multilevel location based key management system for dynamic wireless sensor networks[J]. International Journal of Applied Science and Engineering. 2021, 18(1): 1-11.
- [76] GUO Y, LI Q, LI Y, et al. Service coordination in the Space-Air-Ground integrated network[J]. IEEE Network. 2021, 35(5): 168-173.
- [77] 刘梦如, 付玉龙, 曹进, 等. 基于区块链的天地一体化信息网络非交互式密钥交换方法[J]. 天地一体化信息网络, 2021, 2(3): 48-56.
- LIU M R, FU Y L, CAO J, et al. A non-interactive key exchange scheme for space-integrated-ground information network based on blockchain[J]. Space-Integrated-Ground Information Networks. 2021, 2(3): 48-56.
- [78] 张宏俊. 空天一体联合体系作战及其技术展望[J]. 上海航天, 2021, 38(3): 1-7.
- ZHANG H J. Combat and technology prospect of air and space integrated operation system[J]. Aerospace Shanghai, 2021, 38(3): 1-7.
- [79] 王云, 杨娟, 司书剑. 无人机集群组网认证技术研究[J]. 数据通信. 2020(5):10-14.
- WANG Y, YANG J, SI S J. Research on UAV cluster networking authentication technology[J]. Data Communication, 2020(5): 10-14.
- [80] XU G, LI X, JIAO L, et al. BAGKD: a batch authentication and group key distribution protocol for VANETS[J]. IEEE Communications Magazine. 2020, 58(7): 35-41.
- [81] PATEL N, KUMAR V. An efficient key distribution scheme for WSN with mutual healing capability[J]. Multimedia Tools and Applications, 2022, 81(25): 36735-36749.
- [82] FRIMPONG E, RABBANINEJAD R, MICHALAS A. Arrows in a quiver: A secure certificateless group key distribution protocol for drones[C]//Nordic Conference on Secure IT Systems. 2021: 31-48.
- [83] 徐堂炜, 张海璐, 刘楚环, 等. 基于强化学习的低时延车联网群密钥分配管理技术[J]. 网络与信息安全学报, 2020, 6(5): 119-125.
- XU T W, ZHANG H L, LIU C H, et al. Reinforcement learning

- based group key agreement scheme with reduced latency for VANET[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 119-125.
- [84] PANDA S S, JENA D, MOHANTA B K, et al. Authentication and key management in distributed IoT using blockchain technology[J]. IEEE Internet of Things Journal, 2021, 8(16): 12947-12954.
- [85] TAN Y, LIU J, KATO N. Blockchain-based key management for heterogeneous flying ad hoc network[J]. IEEE Transactions on Industrial Informatics, 2020, 17(11): 7629-7638.
- [86] 陈彩辉, 线珊珊. 美军“联合全域作战(JADO)”概念浅析[J]. 中国电子科学研究院学报, 2020, 15(10): 917-921.
- CHEN C H, XIAN S S. An analysis of U. S. armed forces “joint all-domain operation” concept[J]. Journal of China Academy of Electronics and Information Technology, 2020, 15(10): 917-921.
- [87] 董贵山, 张远云, 刘涛, 等. 智慧城市密码应用解决方案[J]. 信息安全与通信保密, 2020(1): 9-16.
- DONG G S, ZHANG Y Y, LIU T, et al. Smart city cryptography application solution[J]. Information Security And Communications Privacy, 2020(1): 9-16.

[作者简介]



刘军(1991-), 男, 湖南邵阳人, 信息工程大学硕士生, 主要研究方向为信息安全与密码管理。

袁霖(1981-), 男, 河南商丘人, 博士, 信息工程大学副教授, 主要研究方向为信息安全与密码管理。

冯志尚(1996-), 男, 河南郑州人, 信息工程大学硕士生, 主要研究方向为信息安全与密码管理。