数联网环境下基于秘密共享的移动数据终端切换认证方案

郭超[1,2]，于梦格[3]，张玲翠[2,4,5]，翟佳乐[2,4,5]，邓溶[3]
（1.北京电子科技学院电子与通信工程系，北京 100070；2.中国科学院信息工程研究所，北京 100085；
3.北京电子科技学院网络空间安全系，北京 100070；4.网络空间安全防御全国重点实验室，北京 100085；
5.中国科学院大学网络空间安全学院，北京 100049）

摘要：针对数联网环境中移动数据终端带来的认证时延与安全性问题，提出一种基于秘密共享的切换认证方案。引入互通域概念，结合马尔可夫过程预测节点信任状态，信任相近的节点动态聚合为可共享认证信息的逻辑子域，将全局认证简化为子域内的局部协作。针对高信任互通域，利用二元对称多项式的秘密共享特性，预先在子域内分发认证凭证，终端仅凭秘密份额即可实现切换认证，将传统的中心化认证转变为域内节点间的边缘认证，实现认证重心的下沉。通过Tamarin形式化验证方案安全性、评估计算与通信开销，结果表明，所提方案适用于数联网的高动态访问环境。

关键词：数联网；信任预测；秘密共享；切换认证
中图分类号：TN918.4
文献标志码：A
doi：10.11959/j.issn.1000–436x.TXXB250681

Handover authentication scheme for mobile data terminal based on secret sharing in the data Internet

Guo Chao[1,2], Yu Mengge[3], Zhang Lingcui[2,4,5], Zhai Jiale[2,4,5], Deng Rong[3]
1. Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China
2. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
3. Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
4. Key Laboratory of Cyberspace Security Defense, Beijing 100085, China
5. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: To address authentication delays and security issues caused by mobile data terminals in the data internet environment, a handover authentication scheme based on secret sharing was proposed. The concept of interoperability domains was introduced, and a Markov process was employed to predict node trust states. Nodes with similar trust levels were dynamically aggregated into logical subdomains sharing authentication information, reducing global authentication to local cooperation within subdomains. For high-trust interoperability domains, the secret-sharing property of bivariate symmetric polynomials was exploited to pre-distribute authentication credentials within each subdomain, enabling terminals to complete handover authentication using only their secret shares. Centralized authentication was thereby transformed into edge authentication among intra-domain nodes, pushing the authentication center down to the edge. The security of the scheme was formally verified using the Tamarin tool, and its computational and communication overheads were evaluated. Results show that the proposed scheme is suitable for highly dynamic access environments in the data Internet.

Key words: data Internet, confidence prediction, secret sharing, handover authentication

---

收稿日期：2026–01–04；**修回日期：**2026–03–28
通信作者：张玲翠，zhanglingcu@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2023YFB3106505）；国家自然科学基金资助项目（No.U24A20240, No.62441226, No.62476013）；中央高校基本科研业务费专项资金资助项目（No.3282024052）；北京电子科技学院一流学科建设项目（No.20250001Z0411）
Foundation Items： The National Key Research and Development Program of China (No. 2023YFB3106505), The National Natural Science Foundation of China (No.U24A20240, No.62441226, No.62476013), The Fundamental Research Funds for the Central Universities (No.3282024052), Beijing Electronic Science and Technology Institute First-class Discipline Construction Project (No.20250001Z0411)

0 引言

随着信息技术向数据技术时代的转化，移动互联网、物联网、云计算及大数据等前沿技术的快速发展推动数据成为驱动社会经济变革的重要生产要素[1]。在数据要素流通过程中，数据的跨域、多方、多轮交易特点决定了身份认证的复杂性与动态性[2]。在此背景下，数联网作为新型数据基础设施应运而生，旨在通过标准化协议和分布式架构实现跨域、多方、多轮的可信数据流通交易。

在数联网环境中，数据以数字对象的形式存在，通过 Handle 标识符系统进行全局唯一标识，借助数字对象接口协议（digital object interface protocol, DOIP）实现跨域访问与互操作。移动数据终端，包括边缘计算设备、移动工作站、物联网网关等，作为数据流通的前端节点，需要在不同组织、不同信任域的数联网接入节点（data Internet access node, DIAN）之间频繁切换，以实现对分布式数据对象的连续访问与实时交互。然而，现有的数据流通系统普遍面临认证模式多样、跨域信任缺失、身份确认困难等问题，导致数据主体身份难以确权、数据流通过程信任体系难以构建。特别是在移动访问场景下，跨域切换认证面临诸多挑战。

为增强认证中的安全与可信性，信任模型逐渐被引入。通过对节点行为历史、交互频率与服务质量等维度进行量化建模，信任模型为认证决策提供参考依据。Wu 等[3]提出了一种基于节点行为持久性的信任模型，通过持续评估节点的历史行为建立信任评分，并将其引入分布式估计过程中，以加权方式降低不可信节点对系统估计的影响。Chen 等[4]将信任评估嵌入区块链多分片架构，借助可信执行环境实现节点行为验证与隐私保护。Yi 等[5]提出多链信任协同模型，进一步提升了在跨域身份切换时的安全性与可扩展性。这些研究为在数联网环境中构建动态信任体系提供了理论基础。

信任模型本身也在不断演进。Soleymani 等[6]提出了一种基于证据理论的信任模型，用于评估工业物联网中智能设备采集数据的可信度。在边缘人工智能驱动的网络物理系统中，Xiang 等[7]设计的轻量级去中心化认证方案融合混沌映射与区块链技术，实现了低资源开销下的高强度身份验证，并通过真实或随机（real-or-random, RoR）安全模型验证其抗攻击能力，为资源受限的移动终端认证提供了新思路。

在数联网的高动态访问环境中，移动数据终端需要频繁接入不同的 DIAN，以实现数据对象的连续访问与实时上报。在此过程中，身份认证作为保障数据可信流通的关键环节，必须在短时间内完成，否则可能导致数据访问链路中断、业务流程受阻或严重安全风险。传统基于公钥体系的认证方法虽具备良好的安全性，但在频繁切换场景中常伴随计算复杂与响应迟缓等问题[8]，难以满足跨域数据访问、协同计算等对实时性要求极高的任务需求。

因此，在保障通信安全的前提下，实现低时延和高可靠的切换认证已成为当前数联网移动数据终端安全的重要问题[9]。认证方案应能适应高速移动带来的频繁连接变化，并在有限的通信窗口内完成身份确认与密钥协商，确保移动数据终端在跨越不同 DIAN 时通信不中断、控制信息及时传达。同时，面对动态的网络拓扑、异构通信协议及多样化的数据使用行为，这类认证过程还需具备一定的灵活性和环境适应能力，以应对不断变化的网络条件与安全威胁。

为提升切换过程中的认证效率并保障通信安全性，Chen 等[10]提出基于椭圆曲线密钥协商的切换认证协议，通过双向认证与高效密钥协商，有效减少通信成本。Wang 等[11]提出的基于椭圆曲线密码系统的无证书代理签名方案不需要证书管理，在提升认证效率的同时，具备对抗伪装攻击与中间人攻击的能力。张海波等[12]提出基于环的匿名高效批量认证与组密钥协商协议，通过少量双线性映射快速完成对大批车辆的批量认证。在提升群组认证效率方面，Nakkar 等[13]基于 Shamir 秘密共享和聚合消息认证码提出支持多次异步认证与会话密钥协商的轻量级群组认证方案，不需要重新分发密钥份额，适用于边缘计算和物联网环境。随后 Nakkar 等[14]又提出基于物理不可克隆函数的群组认证方案，动态生成密钥份额，利用秘密共享的同态特性支持多次认证、密钥更新及节点动态管理，具备良好的安全性与扩展性。

此外，预认证机制也成为优化认证时延的有效方法。通过在终端离开当前接入节点前提前完成部分认证流程，预认证机制可极大缓解切换带来的时延问题。Yang 等[15]基于中国剩余定理设计预认证协议，在数学结构上增强了认证信息的可组合性，

使终端在切换到目标基站后能快速完成身份验证。Li 等[16]提出了基于中继协助的组切换认证方案，借助移动中继节点在切换前完成认证传输，提高了协议在高速移动场景下的适用性。

尽管已有多种切换认证方案被提出，但在数联网的实际应用中，仍普遍存在认证过程复杂、容易出现单点故障，以及难以兼顾安全性与资源约束等问题。现有的预认证或分布式方案往往依赖固定的区域划分，在面对终端高频跨域移动时，难以兼顾安全判定的实时性与拓扑变化的自适应性。

为此，本文提出一种基于秘密共享的移动终端切换认证方案，面向数联网环境中移动数据终端跨 DIAN 访问的场景，在保证安全的基础上，提升数据要素流通中节点的切换效率。该方案通过信任预测与动态聚类协同构建互通域，以解决传统静态分域对动态环境适应性不足的问题，并利用二元对称多项式的秘密共享特性实现接入侧的边缘认证，减少了切换过程中对核心网管理层的信令依赖。本文的主要贡献具体如下。

（1）提出了一种基于三态马尔可夫过程的信任预测模型，通过细粒度的划分，将累积信任值建模为马尔可夫链，作为信任度量来预测节点的多种信任状态，更精细地划分节点的可信程度，为节点之间的高效认证提供支撑。

（2）提出了互通域的概念。互通域通过建立信任关系和安全机制来确保数据空间内的通信和数据处理的安全性，动态预测和调整节点的信任等级，确保信任关系的实时性和准确性，提高了系统的灵活性和适应性。互通域的划分使信任相近的 DIAN 能够共享认证信息，减少了跨域认证的复杂度，为分层、分级的认证策略提供了基础框架。

（3）提出了基于二元对称多项式秘密共享的移动终端切换认证方案，生成支持双边对称计算的密钥份额，实现身份绑定的快速认证，确保数据传输的完整性和保密性，在有限资源下实现高效认证。

1　基于信任模型的动态互通域构建

为实现移动数据终端在频繁切换环境下的高效认证控制，本文首先引入信任预测模型评估通信节点的行为可靠性。当下研究仅凭瞬时信任值进行评估难以应对行为状态的突发转变，且容易导致判别结果的滞后。引入三态马尔可夫过程预测信任状态，可以实现从基于事后评估的被动防御向基于预判准入的主动防御转变。通过建模信任等级的演化趋向，系统能够在切换发生前识别并剔除潜在恶意节点，确保认证逻辑具备先验安全性，从而为后续互通域的构建提供准确的安全依据。

1.1　结合状态转移的三态马尔可夫信任预测模型

基于三态马尔可夫过程的信任预测模型将累积信任值建模为马尔可夫链，节点的信任状态划分为高、中、低 3 种离散状态，分别用 h_1、h_2、h_3 表示。$P(h_1)$表示节点处于高信任状态的概率，$P(h_2)$表示节点处于中信任状态的概率，$P(h_3)$表示节点处于低信任状态的概率。通过随机过程建模信任演化，结合历史信任信息的影响，预测节点未来的信任状态。

稳态分布广泛应用于马尔可夫链。然而，在达到稳态之前，有限时间 t 内的瞬时分布也很重要，因为稳态结果不能准确表示有限时间内的信任值。基于稳态和非稳态，本文提出基于三态马尔可夫过程的信任预测模型。当 t 趋向于无穷大时，模型根据稳态分布预测节点信任状态。在有限时间 t 内，根据累积信任值与累计信任阈值的关系预测节点的信任状态。基于三态马尔可夫过程的信任预测模型如图 1 所示。

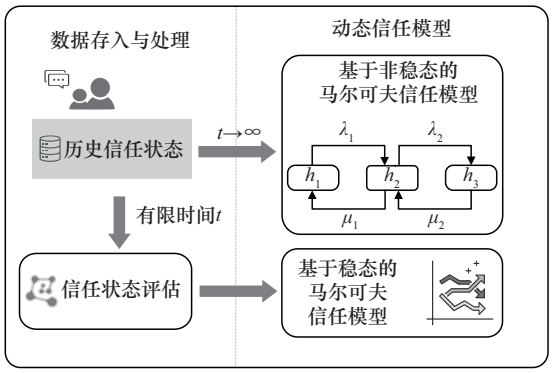

图 1　基于三态马尔可夫过程的信任预测模型

1.1.1　基于稳态的马尔可夫信任模型

由于认证行为会影响节点信任值，节点的信任值会发生变化，节点的信任状态也会随之发生变化。因此，每个发送认证请求节点的累积信任值 $A(t)$可以被认为是三态的马尔可夫链。

信任模型具有无记忆性，即当前的信任状态只依赖于上一个信任状态，信任状态 $h_i \in H$ 都可以从

其他任意信任状态$h_j \in H(j \neq i)$转换而来，因此，信任值模型还是不可约的，即：

$$\lim_{\to \infty} p_{ij}(t) = \pi_j \tag{1}$$

或者

$$\lim_{\to \infty} \pi_j(t) = \pi_j \tag{2}$$

在时间段$[0,f]$内，对于$\forall 0 \leqslant s \leqslant u < t$，有：

$$p_{ij}(s,t) = P(h_t = j | h_s = i) = \sum_{k \in S} p_{ik}(s,u)\, p_{kj}(u,t) \tag{3}$$

将式(1)和式(2)代入式(3)，可以得到：

$$\pi_j(t) = \sum_{i \in S} p_{ij}(s,t)\pi_i(s) \tag{4}$$

因此，状态概率向量$\boldsymbol{\pi} = [\pi_1,\pi_2,\pi_3]$，在时间段$[0,f]$内可以表示为：

$$\pi(t) = \pi(s)\boldsymbol{P}(s,t) \tag{5}$$

其中，$\boldsymbol{P}(s,t)$是任意一对信任状态i和j，在任意时间段(s,t)内的概率转移矩阵，稳态分布$\boldsymbol{\pi} = [\pi_1,\pi_2,\pi_3]$，$\sum_j \pi_j = 1$。

基于稳态的马尔可夫信任模型结合奖惩因子T_B和时间因子t计算概率转移矩阵，算法中涉及的主要参数符号定义如表1所示。

表1 算法中涉及的主要参数符号定义

参数	定义
h	历史信任状态
l	当前信任状态
$R=(R[1],R[2],\cdots,R[n])$	认证请求序列
E	节点信任状态评估，输出节点的当前信任状态
T_{B_i}	节点第i次请求认证的奖惩因子
t	时间因子
TM	状态转移矩阵，矩阵元素初始化为$\frac{1}{n}$，n是状态数
$\boldsymbol{P}$	概率转移矩阵

节点信任状态评估E使用Guo等[17]提出的基于Beta、通信字节波动与集中趋势度量的信任模型（beta-based trust model integrating communication byte fluctuation and concentrated trend measurement， BCCTM）信任状态的评估方法进行计算，T_{B_i}则为该模型中对应的奖惩因子。信任模型计算概率转移矩阵算法如算法1所示。

算法1 信任模型计算概率转移矩阵算法

输入 R，T_{B_i}，t

输出 **TM**，$\boldsymbol{P}$

1) for $i = 1$ to n do

2) $l = E[R(i)]$

3) $\mathbf{TM}[h][l] = t\mathbf{TM}[h][l] + T_{B_i}$

4) $h = l$

5) end for

6) return **TM**,$\boldsymbol{P}$

通过算法1计算得出基于稳态的马尔可夫信任模型中的概率转移矩阵$\boldsymbol{P}$，在模型达到稳态时，可以计算稳态分布，即状态概率向量$\boldsymbol{\pi} = [\pi_1,\pi_2,\pi_3]$，节点的预测信任概率为：

$$\boldsymbol{P}(v) = [P(h_1),P(h_2),P(h_3)] = [\pi_1,\pi_2,\pi_3] \tag{6}$$

其中，$i \in \{1,2,3\}$表示第i个信任状态，v表示节点。选择稳态分布中取得最大概率的信任状态作为节点的预测信任状态。

1.1.2 基于非稳态的马尔可夫信任模型

$A(t)$和$S(t)$分别用来表示在某一时间段$(0,t]$内信任值和信任阈值的累积量。累积信任值和累积信任阈值都可以被认为是随机过程。将节点的高、低信任阈值和信任值分别表示为S_1、S_2和A。

对于某个节点，在时间段$(s,t](0 \leqslant s \leqslant t)$内，如果累积信任值大于累积信任阈值$S_1$，即$S_1(s,t) - A(s,t) \leqslant 0$，表示为：

$$P(h_1) = P\{S_1(s,t) - A(s,t) \leqslant 0\} \tag{7}$$

如果累积信任值小于累积信任阈值S_2，即$S_2(s,t) - A(s,t) > 0$，表示为：

$$P(h_3) = P\{S_2(s,t) - A(s,t) > 0\} \tag{8}$$

则在任何时间段$(s,t](0 \leqslant s \leqslant t)$内，中等信任状态概率定义为：

$$\begin{aligned} P(h_2) &= 1 - P(h_1) - P(h_3) = \\ &1 - P\{A(s,t) - S_1(s,t) \geqslant 0\} - \\ &P\{S_2(s,t) - A(s,t) > 0\} \end{aligned} \tag{9}$$

通过计算$P(h_1)$的下界和$P(h_3)$的上界，可以判断节点的信任状态。如果某个节点具有累积信任值$A \sim {}_{tv}\langle f,\alpha \rangle$和累积信任阈值$S \sim {}_{tt}\langle g,\beta \rangle$，那么在

时间段$(s,t](0\leqslant s\leqslant t)$内，$P(h_i)$的上界为：

$$P(h_i)\leqslant f\otimes g\left(\alpha(t-s)-\beta_{i-1}(t-s)\right) \tag{10}$$

$P(h_{i-1})$的下界为：

$$P(h_{i-1})\leqslant \frac{1}{n-1}-f\otimes g\left(\alpha(t-s)-\beta_{i-1}(t-s)\right) \tag{11}$$

其中，$i(i-1\neq 0)$表示信任状态，n表示信任状态总数，在这里表示为3，β_{i-1}表示第$i-1$个信任阈值，$f\otimes g(t)$为最小加代数中函数f和g的最小加卷积，$f\otimes g(t)=\inf\limits_{0\leqslant s\leqslant t}\left[f(s)+g(t-s)\right]$。

信任状态在h_1、h_2和h_3之间交替，并且$A(t)$的变化率随时间变化。假设节点在时刻t处于某个状态，随着时间的推移，节点的信任度会根据系统的转移速率从当前状态转移到其他状态。如果节点的行为改善，它可能从h_2转移到h_1。如果节点的行为变差，则可能从h_2转移到h_3。

令h_1、h_2和h_3为3个信任状态的到达速率，假设每个状态的单位时间信任增长为：

$$\boldsymbol{H}=\mathrm{diag}(h_1,h_2,h_3) \tag{12}$$

则三态信任值过程具有信任曲线。

$$\alpha(t)=\rho(\theta)t \tag{13}$$

其中，$\rho(\theta)$为：

$$\rho(\theta)=\lambda_{\max}(\boldsymbol{Q}+\theta\cdot\boldsymbol{H}) \tag{14}$$

边界函数为：

$$f(x)=\mathrm{e}^{-\theta x},\forall\theta>0 \tag{15}$$

转移速率矩阵为：

$$\boldsymbol{Q}=\begin{bmatrix}-\lambda_1 & \lambda_1 & 0\\ \mu_1 & -(\mu_1+\lambda_2) & \lambda_2\\ 0 & \mu_2 & -\mu_2\end{bmatrix} \tag{16}$$

初始稳态分布为$\boldsymbol{\pi}=[\pi_1,\pi_2,\pi_3]$，满足$\boldsymbol{\pi}\cdot\boldsymbol{Q}=0$。根据实际应用中统计到的经验数据，可以得到信任值过程对应的转移概率，从而得到转移矩阵$\boldsymbol{Q}$。

通过矩母函数（moment generating function, MGF）[18]计算Chernoff（切尔诺夫）边界，定义偏移生成矩阵：

$$\boldsymbol{M}_A(\theta,t)=\mathrm{E}\left[\mathrm{e}^{\theta A(t)}\right]=\boldsymbol{\pi}\cdot\exp\left[(\boldsymbol{Q}+\theta\cdot\boldsymbol{H})t\right]\cdot\boldsymbol{1}\leqslant\|\exp\left[(\boldsymbol{Q}+\theta\cdot\boldsymbol{H})t\right]\|\leqslant\mathrm{e}^{\rho(\theta)t} \tag{17}$$

其中，$\boldsymbol{1}=[1,1,1]^{\mathrm{T}}$。通过马尔可夫不等式可得：

$$\Pr(A(t)\geqslant x)\leqslant\frac{\mathrm{E}\left[\mathrm{e}^{\theta A(t)}\right]}{\mathrm{e}^{\theta x}}=\mathrm{e}^{-\theta x}M_A(\theta,t) \tag{18}$$

引出边界：

$$\Pr(A(t)\geqslant x)\leqslant\mathrm{e}^{-\theta x+\rho(\theta)t} \tag{19}$$

式(19)对$\forall\theta>0$成立，上界最小时取得：

$$\theta_{\text{上}}^{*}=\arg\min_{\theta>0}\mathrm{e}^{-\theta(c-\rho_1(\theta))t}=\arg\min_{\theta>0}\left[-\theta(c-\rho_1(\theta))\right] \tag{20}$$

其中，$\rho_1(\theta)=\lambda_{\max}(\boldsymbol{Q}+\theta\cdot\boldsymbol{H})$，同理，下界最优值为：

$$\theta_{\text{下}}^{*}=\arg\min_{\theta>0}\mathrm{e}^{-\theta(\rho_2(\theta)-c)t}=\arg\min_{\theta>0}\left[-\theta(\rho_2(\theta)-c)\right] \tag{21}$$

其中，$\rho_2(\theta)=\lambda_{\max}(\boldsymbol{Q}-\theta\cdot\boldsymbol{H})$。

对于信任阈值模型，考虑最简单的情况，即不同信任状态的阈值是常数，假定为$c_{i-1}(i-1\neq 0)$，i对应不同的信任状态，那么累积信任阈值为：

$$\beta_{i-1}(t)=c_{i-1}t \tag{22}$$

其边界函数为：

$$g(x)=0 \tag{23}$$

根据上述结果，在任何时间间隔$(s,t](0\leqslant s\leqslant t)$中，$P(h_i)$的上界为：

$$P(h_i)\leqslant f\otimes g\left(\alpha(t-s)-\beta_{i-1}(t-s)\right) \tag{24}$$

且$P(h_{i-1})$的下界为：

$$P(h_{i-1})\leqslant\frac{1}{n-1}-f\otimes g\left(\alpha(t-s)-\beta_{i-1}(t-s)\right) \tag{25}$$

其中，$\alpha(t)=\rho(\theta)t$，$f(x)=\mathrm{e}^{-\theta x}$，$\beta_{i-1}(t)=c_{i-1}t$。

令累积平均信任值$\frac{A(t)}{t}$表示较短时间$[0,t]$内$A(t)$的变化率。给定两个恒定的信任值阈值c_1,c_2，在时间t范围内，节点不同信任状态的预测信任概率分别为：

$$P(h_1):\Pr\left(\frac{A(t)}{t}\geqslant c_1\right) \tag{26}$$

$$P(h_2):\Pr\left(c_2\leqslant\frac{A(t)}{t}<c_1\right) \tag{27}$$

$$P(h_3):\Pr\left(\frac{A(t)}{t}<c_2\right) \tag{28}$$

根据式(26)~式(28)，可以确定节点处于的信任

状态，节点的预测信任概率为：

$$\boldsymbol{P}(v)=\left[P\left(h_1\right),P\left(h_2\right),P\left(h_3\right)\right] \tag{29}$$

其中，$i\in\{1,2,3\}$表示第i个信任状态，v表示节点，选择其中取得最大概率的信任状态作为节点的预测信任状态。

由该模型可以较为全面地计算节点的预测信任概率，预测节点的下一信任状态。预测结果将以信任记录的形式存储在信任系统中，用于动态更新节点的信任状态。节点信任信息的访问权限受到严格控制，只有认证服务器在切换决策与认证过程中具备查询权限，以确保信任信息的独立性、可信性和防篡改性。

1.2 基于信任模型的有向动态互通域构建

为适应数联网环境中移动数据终端频繁切换的通信特点，本文提出互通域的概念。传统认证架构受限于固定的地理边界或物理拓扑分域，在处理终端跨域移动时，通常需触发涉及核心网实体的长路径信令重协商，由此产生的重认证时延难以满足高动态环境下的实时性需求。互通域用于划分信任状态相近且通信需求相似的一组网络节点，通过建立信任对等关系，支持彼此间的认证、授权与数据交付，遵循统一的安全策略与通信规范，从而减少了对身份验证、数据加密等措施的频繁需求。互通域根据信任状态的变化动态调整成员结构，允许高信任节点以更低认证成本完成切换与通信，优化流通路径与认证成本。在网络系统中，互通域的定义提升了信任度量的细粒度，在确保数据流通连续性的基础上简化了域内安全管理逻辑。针对静态划分方式难以感知节点行为特征变化且缺乏拓扑自适应性的缺陷，本文利用K-Means聚类算法根据节点信任状态的演化动态聚合逻辑子域，实现互通域的动态构建。

1.2.1 信任映射

结合BCCTM模型和基于状态转移的三态马尔可夫信任预测模型，各节点的信任值和预测信任概率作为节点的信任属性，推荐信任值映射到有向边权，综合信任值映射到节点权，实现互通域的有向图表示。其中，边的方向反映信任的传递关系，如低信任节点向高信任节点的单向访问受限。有向边的权重代表信任传递的强度，权重越高，该方向节点间信任关系越强。

（1）节点权重映射。考虑每个节点v_i的信任值和预测信任概率，定义权重向量为：

$$\boldsymbol{W}\left(v_i\right)=\left[T_{\mathrm{ID}_{U_i}},\boldsymbol{P}\left(v_i\right)\right] \tag{30}$$

其中，$\boldsymbol{P}\left(v_i\right)=\left[P_i\left(h_1\right),P_i\left(h_2\right),P_i\left(h_3\right)\right]$表示节点的预测信任概率向量，$T_{\mathrm{ID}_{U_i}}$表示节点$v_i$的信任值。

（2）边权重映射。对任意边$e_{ij}\in E$，综合考虑两节点之间有向推荐信任值和通信质量$Q_{ij}(t)$，定义有向边权重为：

$$\boldsymbol{W}\left(e_{ij}\right)=\gamma\lambda_{ij}+\left(1-\gamma\right)Q_{ij}(t) \tag{31}$$

其中，$\gamma\in[0,1]$用于平衡信任值与通信质量的影响。

通信质量指标$Q_{ij}(t)$为认证信令传输提供了物理可靠性保障，防止单一信任评估导致的协议失效。$Q_{ij}(t)$通过信噪比、丢包率、时延、吞吐量和误码率等多个参数综合评价。在实际应用中，可以利用实时采集的通信数据，通过加权计算得到综合通信质量指标。对于两个节点i和j，可定义$Q_{ij}(t)$为：

$$\begin{aligned}Q_{ij}(t)=&\ \xi_1\mathrm{SNR}_{ij}(t)+\\&\xi_2\left(1-\mathrm{PLR}_{ij}(t)\right)+\xi_3\frac{1}{\mathrm{Delay}_{ij}(t)}\end{aligned} \tag{32}$$

其中，$\mathrm{SNR}_{ij}(t)$表示在时刻t节点i与j之间的信噪比，$\mathrm{PLR}_{ij}(t)$表示丢包，$\mathrm{Delay}_{ij}(t)$表示传输时延，ξ_1、ξ_2和ξ_3是权重系数，满足$\xi_1+\xi_2+\xi_3=1$。该指标通过式(31)参与边权重$\boldsymbol{W}(e_{ij})$的映射计算，直接干预聚类分域的结果。若两节点间信道环境恶化，如丢包率$\mathrm{PLR}_{ij}(t)$异常或时延$\mathrm{Delay}_{ij}(t)$增大，即便其信任评分较高，加权后的综合权重仍会显著下调，从而过滤不稳定节点，规避认证超时风险。

此外，通信质量也为认证策略的动态调节提供了决策参考。针对数联网跨域访问对实时性的核心需求，具体设置时通常采取侧重时延参数ξ_3的非均衡加权方式[18]，比如$\xi_3>\xi_1,\xi_2$，使终端优先选择物理链路更稳定的接入节点。这种结合安全可信与传输可靠的双重约束逻辑，确保了互通域结构能根据异构通信环境灵活调整，使分域逻辑在物理层面具备更强的稳定性与可解释性。

为体现信任传递的方向性，采用有向图表示互通域。边e_{ij}的方向设为$i\rightarrow j$，其边权重为$\boldsymbol{W}\left(e_{ij}\right)$，由节点$v_i$对节点$v_j$的推荐信任度和节点$v_i$到节点$v_j$

的通信质量 $Q_{ij}(t)$ 决定。反之，边 e_{ji} 的方向则为 $j \to i$，其边权重为 $\boldsymbol{W}\left(e_{ji}\right)$，由节点 v_j 对节点 v_i 的推荐信任值 T_{D} 和节点 v_j 到节点 v_i 的通信质量 $Q_{ji}(t)$ 决定。两个节点间相互认证时，高信任度的节点对低信任节点需更严格认证。

1.2.2　*动态互通域划分*

通过设定动态阈值，筛选高信任度节点，划分互通域。采用 K-Means 聚类算法，根据信任值和拓扑结构进行分组，使互通域具备自治性和层级性。

（1）动态信任阈值筛选。设定一个动态信任阈值 T_{th} 和一个动态信任概率阈值 P_{th}，筛选出当前信任值较高且未来仍有较高概率保持高信任度的节点，这些节点表示为：

$$V_{\mathrm{high}} = \{\, v_i \in V \,|\, T_i(t) \geqslant T_{\mathrm{th}} \cap P_i\left(h_1\right) \geqslant P_{\mathrm{th}} \} \tag{33}$$

动态信任阈值 T_{th} 通常通过对当前网络中所有节点信任值的统计分析和历史行为反馈来确定，设在时刻 t 时，网络中共有 N 个节点，每个节点的信任值为 $T_i(t)$，其中 $i = 1,2,\cdots,N$。首先，对所有节点的信任值进行统计分析，计算其均值和标准差。

$$\mu_{\mathrm{T}}(t) = \frac{1}{N}\sum_{i=1}^{N} T_i(t) \tag{34}$$

$$\sigma_{\mathrm{T}}(t) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(T_i(t) - \mu_{\mathrm{T}}(t)\right)^2} \tag{35}$$

为了兼顾当前网络状态和历史行为反馈，将动态信任阈值 T_{th} 定义为均值与标准差的线性组合，同时引入历史均值变化作为反馈补偿项。

$$T_{\mathrm{th}}(t) = \mu_{\mathrm{T}}(t) + k\sigma_{\mathrm{T}}(t) + \lambda\Delta\mu_{\mathrm{T}}(t) \tag{36}$$

其中，k 为控制标准差贡献的系数，决定了对信任波动的敏感度；$\Delta\mu_{\mathrm{T}}(t) = \mu_{\mathrm{T}}(t) - \mu_{\mathrm{T}}(t-1)$ 表示均值的变化，用以反映历史行为反馈；λ 为反馈调节系数，用于平滑阈值变化，适应网络长期趋势。k 的初始值可设置为 1~2[19]，表示标准差在阈值中的适中贡献。λ 的初始值可设为 0.1~0.3，以较低比例调整均值变化对阈值的影响。

动态信任概率阈值 P_{th} 将综合考虑节点在未来保持高信任状态、中信任状态和低信任状态的概率。单个节点的预测信任水平表示节点 i 在未来处于不同信任状态的预测信任概率的加权平均值，计算式为：

$$\mu_{P_i} = w_1 P_i\left(h_1\right) + w_2 P_i\left(h_2\right) + w_3 P_i\left(h_3\right) \tag{37}$$

其中，w_1,w_2,w_3 分别表示高信任、中信任和低信任状态的权重系数，且 $w_1 + w_2 + w_3 = 1$，可以根据需求调整，确保系统更加关注未来某个信任状态的节点，或者适当平衡 3 个信任状态的影响。

每个节点 i 在时刻 t 对应的预测信任水平为 $P_i(t) = \mu_{\mathrm{P}_i}(t)$，计算所有节点的预测信任概率均值和标准差。

$$\mu_{\mathrm{P}}(t) = \frac{1}{N}\sum_{i=1}^{N}\mu_{\mathrm{P}_i}(t) \tag{38}$$

$$\sigma_{\mathrm{P}}(t) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(\mu_{\mathrm{P}_i}(t) - \mu_{\mathrm{P}}(t)\right)^2} \tag{39}$$

动态信任概率阈值 P_{th} 定义同 T_{th} 类似。

$$P_{\mathrm{th}}(t) = \mu_{\mathrm{P}}(t) + k\sigma_{\mathrm{P}}(t) + \lambda\Delta\mu_{\mathrm{P}}(t) \tag{40}$$

其中，$\Delta\mu_{\mathrm{P}}(t) = \mu_{\mathrm{P}}(t) - \mu_{\mathrm{P}}(t-1)$ 表示均值的变化。

（2）聚类分组。对于每个节点 i，构造包含信任值的多维特征向量 $\boldsymbol{x}_i = \left[T_i,P_i,Q_i,\cdots\right]$，$T_i$ 为节点 i 的实时信任值，$P_i = \mu_{P_i}$ 为节点 i 的预测信任水平，Q_i 为节点 i 的通信质量指标。其他维度可根据具体应用需求添加，如节点位置、历史认证成功率等。信任值作为第一维特征，可以通过归一化处理，使各维数据具有相同的量纲，确保信任值在聚类过程中具有适当的影响力。

将所有节点 $X = \left\{x_1,x_2,\cdots,x_N\right\}$ 聚类为 K 个互通域，每个簇 C_k 内节点具有相似的信任水平和通信特性，具体步骤如下。

步骤 1　初始化。随机从 X 中选择 K 个节点作为初始簇中心 $\mu_1,\mu_2,\cdots,\mu_K$。

步骤 2　分配。对于每个节点 x_i，计算其与每个簇中心的欧氏距离，即：

$$d\left(x_i,\mu_k\right) = \sqrt{\sum_{j=1}^{d}\left(x_{ij} - \mu_{kj}\right)^2} \tag{41}$$

其中，第一个维度 $x_{i1} = T_i$ 表示信任值，第二个维度 $x_{i2} = P_i$ 表示预测信任水平。可以通过设置权重 ω_1 和 ω_2 来增强信任值和预测信任水平的影响，表示为：

$$d\left(x_i,\mu_k\right) = \sqrt{\omega_1\left(T_i - \mu_{k1}\right)^2 + \omega_2\left(P_i - \mu_{k2}\right)^2 + \sum_{j=3}^{d}\omega_j\left(x_{ij} - \mu_{kj}\right)^2} \tag{42}$$

将节点 x_i 分配给距离最近的簇，即：

$$c_i = \arg\min_{1 \leqslant k \leqslant K} d\left(x_i,\mu_k\right) \tag{43}$$

步骤 3 更新。对于每个簇 C_k，更新簇中心为该簇内所有节点特征的均值，表示为：

$$\mu_k = \frac{1}{\left|C_k\right|}\sum_{x_i \in C_k} x_i \tag{44}$$

其中，更新后的第一维 μ_{k1} 即簇内所有节点信任值的均值，μ_{k2} 为簇内所有节点预测信任水平的均值。

步骤 4 收敛判断。重复分配和更新步骤，直到簇中心的变化小于预设阈值 ε，即

$$\max_k \left\| \mu_k^{(\text{new})} - \mu_k^{(\text{old})} \right\| < \varepsilon \tag{45}$$

划分高信任互通域的 K-Means 聚类算法伪代码如算法 2 所示。

算法 2 K-Means 聚类算法

输入 节点特征集 $X = \left\{x_1,x_2,\cdots,x_N\right\}$，其中 $x_i = \left[T_i,P_i,Q_i,\cdots\right]$，聚类数 K，权重向量 $\boldsymbol{\omega} = \left[\omega_1,\omega_2,\cdots,\omega_d\right]$，收敛阈值 ε

输出 簇集合 $C = \left\{C_1,C_2,\cdots,C_K\right\}$，簇中心 $\left\{\mu_1,\mu_2,\cdots,\mu_K\right\}$

1) 随机选择 K 个节点作为初始簇中心 $\left\{\mu_1,\mu_2,\cdots,\mu_K\right\}$

2) repeat

3) 对每个节点 $x_i \in X$

4) 对 $k = 1,2,\cdots,K$ 计算距离

5) $d(x_i,\mu_k) = \text{sqrt}\,(\omega_1(T_i - \mu_{k1})^2 + \omega_2(P_i - \mu_{k2})^2 + \sum[\,j = 3 \text{ to } d\,]\omega_j(x_{ij} - \mu_{kj})^2)$

6) 令 $c_i = \arg\min_{1 \leqslant k \leqslant K} d\left(x_i,\mu_k\right)$

7) 对每个簇 $C_k\left(k = 1,2,\cdots,K\right)$

8) 更新簇中心

$$\mu_k = \frac{1}{|C_k|}\sum[\,x_i \in C_k]x_i$$

9) 计算 $\Delta = \max_k \left|\left|\mu_k^{(\text{new})} - \mu_k^{(\text{old})}\right|\right|$

10) until $\Delta < \varepsilon$

11) 返回簇集合 $\left\{C_1,C_2,\cdots,C_K\right\}$ 及簇中心 $\{\mu_1,\mu_2,\cdots,\mu_K\}$

对于当前信任值中等且不会有较高概率转移到低信任度的节点和信任值较高但未来有较高概率转移到中等信任状态的节点，有：

$$V_{\text{medium}} = \{\, v_i \in V \left| \left(T_{\text{low}} \leqslant T_i(t) < T_{\text{th}} \cap P_i\left(h_1\right) \geqslant P_{\text{th}}\right) \cup \left(T_{\text{low}} \leqslant T_i(t) < T_{\text{th}} \cap P_i\left(h_2\right) \geqslant P_{\text{th}}\right) \cup \left(T_i(t) \geqslant T_{\text{th}} \cap P_i\left(h_2\right) \geqslant P_{\text{th}}\right)\right. \} \tag{46}$$

信任值较低的节点和未来有较高概率保持或转移到低信任状态的节点，有：

$$V_{\text{low}} = \{\, v_i \in V | T_i(t) < T_{\text{low}} \cup P_i\left(h_3\right) \geqslant P_{\text{th}}\} \tag{47}$$

其中，T_{low} 表示提前设定的最低信任值。这些节点采用同样的 K-Means 聚类算法，根据信任值和拓扑结构进行分组，构建出逻辑上互通的中等信任域和低信任域。

（3）互通域表示。在将聚类结果映射回拓扑图时，将每个聚类 C_k 视为一个动态互通域 D_k。

步骤 1 子图构造。对于全局拓扑图 $G = (V,E)$，经过 K-means 聚类后得到节点分组 $\left\{C_1,C_2,\cdots,C_K\right\}$。对于每个聚类 C_k，对应的子图为 $D_k = \left(V_k,E_k\right)$，其中 $V_k = C_k$，$E_k = \{\, e_{ij} \in E \left| i,j \in C_k\right.\}$。

步骤 2 节点与边权重映射。每个节点 $v_i \in V$ 已经具备实时信任值 T_i 和预测信任概率向量 $\boldsymbol{P}\left(v_i\right)$，根据节点和边权重映射，确定节点权重和边权重。

步骤 3 映射回全局拓扑。全局动态互通域表示为：

$$G = \bigcup_{k=1}^{K} D_k \tag{48}$$

其中，每个 D_k 都是基于信任度量构建的逻辑域，可作为跨域认证的基本单元。

通过式(46)~式(48)和构建方法，每个聚类 C_k 被映射为一个动态互通域 D_k，其节点和边均带有实时更新的信任属性。动态互通域不仅体现了物理连接，还显示了节点间的信任传递强度，从而为认证策略选择提供了可靠的数据基础和决策依据。系统可以根据互通域的信任程度选择适合的认证方案。在高信任互通域内节点采用轻量级认证方案，提高通信效率。互通域间及低信任互通域内节点采用增强认证方案，以防范潜在风险。

2 基于秘密共享的移动终端切换认证方案

本节针对数联网环境中对可移动终端身份认证的高安全性与高效率需求，提出一种基于秘密共享的移动终端切换认证方案。在该方案中，移动终端作为数据交互实体，以数据使用方接入系统，发起

数据访问与授权请求。传统的集中式密钥管理或基于中心化授权实体的认证机制，在处理终端大规模、高频次的切换请求时，极易造成核心网认证服务器的信令瓶颈，该方案设计基于前文构建的互通域所提供的拓扑支撑，结合二元对称多项式的秘密共享特性，预先在高信任互通域内的节点间分发秘密份额，终端身份与密钥份额绑定，移动终端仅凭本地预存的秘密份额即可完成双向身份认证，实现快速切换，提升认证的安全性与效率。通过将认证任务由数联网核心管理层向边缘接入层下沉，有效缓解了终端频繁切换过程中的信令交互压力，在保障认证安全性的同时显著提升了系统切换性能。

2.1　系统模型与安全模型

2.1.1　系统模型

基于秘密共享的移动终端切换认证方案的系统模型由3个部分组成。系统模型如图2所示。

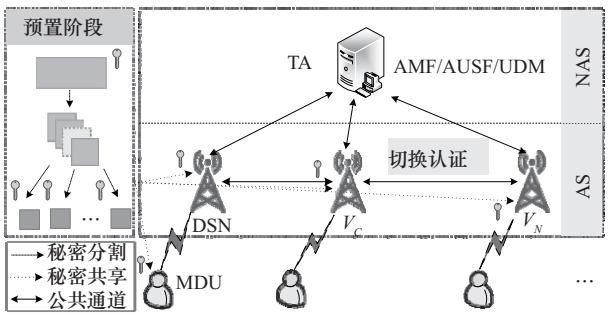

图2　系统模型

（1）移动数据终端（mobile data user, MDU）。MDU指具备通信能力并能参与数联网接入与数据交互的移动节点设备，以边缘计算终端、移动工作站、物联网网关等形式存在，承担着发起接入、完成身份认证、维持通信会话等关键任务。MDU集合表示为$U=\{u_1,u_2,\cdots,u_n\}$。

（2）数联网接入节点（data internet access node, DIAN）。DIAN是部署在数联网边缘的数据接入与管理节点，基于数字对象架构提供数据对象的注册、解析、访问控制等核心服务。DIAN视为接入节点（access node, AN），表示为$V=\{v_1,v_2,\cdots,v_n\}$，将目前终端连接的接入节点称为当前接入节点，用V_C表示。终端将移动到的下一个接入节点称为下一接入节点，用V_N表示。

（3）可信授权中心（trusted authority, TA）。TA是数联网的中央安全管理实体，承担设备身份注册、密钥生成、证书签发和统一认证等核心职能。TA集成5G核心网功能模块，包括接入与移动管理功能（access and mobility management function, AMF）、认证服务器功能（authentication server function, AUSF）、统一数据管理（unified data management, UDM）等，处理MDU的认证请求、管理认证策略与密钥状态。TA集合表示为$S=\{s_1,s_2,\cdots,s_n\}$。

2.1.2　安全模型

为明确方案适用的安全边界，本节对敌手能力与系统信任假设进行形式化定义。

（1）敌手模型

本文假设敌手为多项式时间攻击者，并遵循Dolev-Yao攻击模型。敌手可以完全控制公开通信信道，包括对消息的窃听、篡改、重放、插入与时延；同时，敌手可能渗透部分数联网接入节点，但被攻破的节点数量不超过秘密共享门限$t-1$。敌手还可能发起合谋攻击，其规模同样不超过$t-1$，并尝试伪造身份标识或篡改信任记录。

在计算能力方面，敌手无法在多项式时间内破解安全哈希函数的单向性，也无法求解有限域$\mathrm{GF}(p)$上的离散对数问题。

（2）信任假设

在上述模型的假设下，作如下信任前提约定。S作为可信授权实体，在系统运行期间不会主动泄露主密钥或伪造注册信息；当被攻破的DIAN数量少于门限t时，基于二元对称多项式构造的秘密份额验证机制能够保证份额及信任记录的完整性。

2.2　方案设计

2.2.1　初始化阶段

系统初始化阶段由S完成，选择大素数p，生成椭圆曲线$E(F_p)$，在$E(F_p)$上选择q阶子群G，然后选择G的任意生成元P。S选择一个随机数$x\in Z_p^*$作为主密钥，计算出对应的系统公钥$P_{\mathrm{pub}}=xP$，确定2个安全哈希函数H_1和H_2，其中$H_1:\{0,1\}^*\to\{0,1\}^n$，$H_2:\{0,1\}^*\to Z_q^*$，其中，$n$表示字符串的长度，且$n\geqslant 1$，$G$表示有限域中的群，$Z_q^*$表示所有与$q$互素的元素的等价类构成的乘法群。$S$发布$Pa=\{p,q,E(F_p),G,P,P_{\mathrm{pub}},H_1,H_2\}$作为系统参数，密钥$x$保密。

2.2.2　注册阶段

移动数据终端U_i随机选取秘密值$y_{U_i} \in Z_q^*$，计算公开参数$Y_{U_i} = y_{U_i}P$，将含有自己身份标识的注册请求$\{\mathrm{ID}_{U_i}, Y_{U_i}\}$通过安全通道发送给$S$。$S$收到消息后，选择一个随机数$r_{U_i} \in Z_q^*$，计算$R_{U_i} = r_{U_i}P$，$d_{U_i} = r_{U_i} + x\mathrm{TID}_{U_i}$，生成$U_i$的临时身份$\mathrm{TID}_{U_i} = H_1(r_{U_i}P_{\mathrm{pub}}) \oplus \mathrm{ID}_{U_i}$，之后，$S$将包含用户临时身份的注册响应消息$\{\mathrm{TID}_{U_i}, R_{U_i}, d_{U_i}\}$发送给用户。用户$U_i$收到消息后，验证$d_{U_i}P = R_{U_i} + P_{\mathrm{pub}}\mathrm{TID}_{U_i}$是否成立，判断密钥的合法性。若验证不通过，则重新向S申请密钥；否则，密钥生成成功。U_i的公钥为$\mathrm{PK}_{U_i} = (Y_{U_i}, R_{U_i})$，私钥为$\mathrm{SK}_{U_i} = (y_{U_i}, d_{U_i})$。移动数据终端注册交互时序如图3所示。

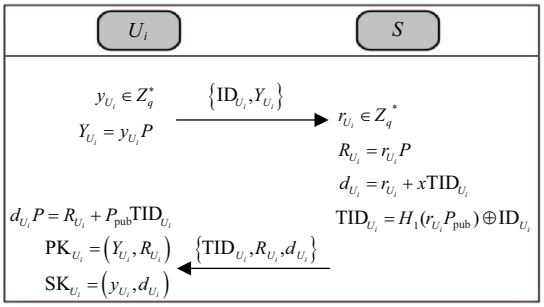

图3　移动数据终端注册交互时序

2.2.3　预置阶段

本阶段由S执行，完成秘密份额的生成与分发。为明确预置阶段中各变量的逻辑关联，表2汇总了该阶段涉及的核心参数及其物理意义。为进一步阐明秘密份额在系统预置及认证阶段的逻辑关联，图4展示了秘密份额生成、分发、验证与重构的生命周期管理流程。

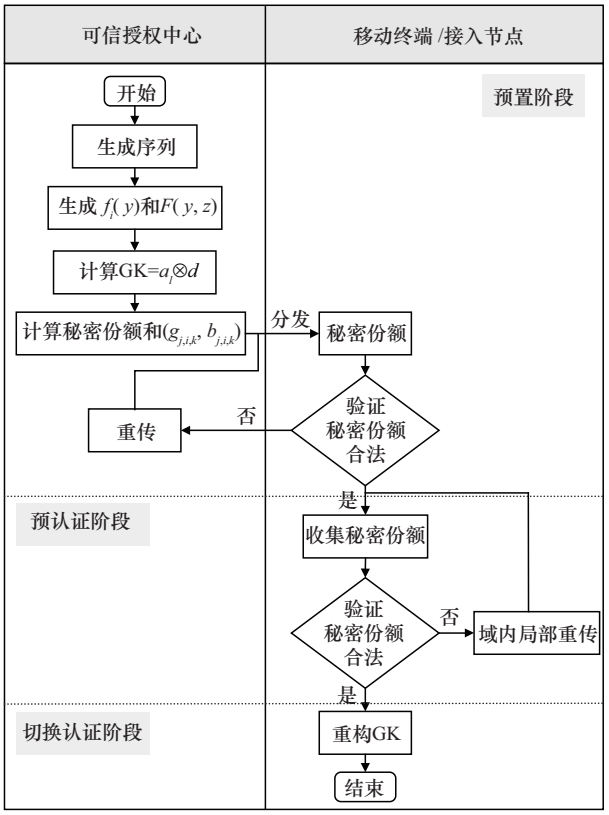

图4　秘密份额生命周期管理流程

S选择秘密GK，大素数p，$\mathrm{GF}(p)$是p阶有限域，GK保证在有限域$\mathrm{GF}(p)$上进行选择，同一互通域内的移动数据终端、DIAN作为参与者集合，门限值为t，安全参数为v，按照下面的步骤进行预置。

（1）选择随机整数$l(1 \leqslant l \leqslant v)$，并生成序列$a_1 > a_2 > \cdots > a_{l-1} > a_l < a_{l+1} \cdots < a_v$。

（2）对于$i = 1, \cdots, v(i \neq 1)$，随机生成单变量多项式$f_i(y) = a_{i,0} + a_{i,1}y + \cdots a_{i,t-1}y^{t-1} \bmod q$，其中，$a_{i,0} = a_i$，$y$为该方程式的变量，$a_{i,j} \in \mathrm{GF}(p)$表

表2　预置阶段涉及的核心参数及其物理意义

参数符号	物理意义	计算规则
GK	系统预置秘密	由服务器S随机选择，并满足关系式$\mathrm{GK} = a_i \oplus d$
t	秘密共享门限值	预先设定的安全参数，代表重构秘密所需的最小合法份额数
v	安全序列长度	对应多项式系数的防御深度
$F(y,z)$	二元对称多项式	$t-1$次多项式，系数满足$c_{i,j} = c_{j,i}$，用于生成节点间对称密钥份额。
$f_i(y)$	单变量多项式	$t-1$次多项式，用于互通域内非对称路径的秘密分片计算
$\boldsymbol{s}_i$	秘密份额向量	包含v个维度的向量$(s_{i,1}, s_{i,2}, \cdots, s_{i,v})$

示变量y^j的系数，其取值为随机生成的一组序列中的第t个值。对于序列的l位置，生成$t-1$次二元对称多项式。

$$F(y,z)=a_l+c_{1,0}y+c_{0,1}z+c_{1,1}yz+\cdots+c_{t-1,t-1}y^{t-1}z^{t-1} \bmod q$$

其中，$c_{i,j}=c_{j,i},\forall i,j\in[0,t-1]$，$F(0,0)=a_l$，$z$为二元对称多项式的另一个变量，$c_{i,j}\in \mathrm{GF}(p)$表示变量的系数。

（3）计算d满足$\mathrm{GK}=a_l\oplus d$。

（4）计算秘密份额$\boldsymbol{s}_i=(\boldsymbol{s}_{i,1},\boldsymbol{s}_{i,2},\cdots,\boldsymbol{s}_{i,v})$，通过安全通道分发$\boldsymbol{s}_i$和$d$给互通域内的参与者$P_i(1<i<n)$。其中，$\boldsymbol{s}_i$中的每个元素$\boldsymbol{s}_{i,k}\equiv(s_{i,k,0},s_{i,k,1},\cdots,s_{i,k,t-1})$为$t$维向量，$s_{i,k,0},s_{i,k,1},\cdots,s_{i,k,t-1}(1\leqslant i\leqslant n,1\leqslant k\leqslant v)$是$\mathrm{GF}(q)$上随机选取的元素，当$k=l$时，$\boldsymbol{s}_{i,l}=(s_{i,l,0}=F(\mathrm{ID}_i,0),\cdots,s_{i,l,t-1})$，当$k\neq l$时，$\boldsymbol{s}_{i,k}=(s_{i,k,0}=f_i(\mathrm{ID}_i),\cdots,s_{i,k,t-1})$。其中，$\mathrm{ID}_i$表示第$i$个参与者的身份信息。

（5）随机在有限域$\mathrm{GF}(p)$上选取非空值$g_{j,i,k}(1\leqslant i\leqslant n,1\leqslant j\leqslant n,1\leqslant k\leqslant v,i\neq j)$，计算$b_{j,i,k}=g_{j,i,k}s_{i,k,0}+\mathrm{ID}_i s_{i,k,1}+\cdots+\mathrm{ID}_j^{t-1}s_{i,k,t-1}$，通过安全通道向每个$P_j$分发$(g_{j,i,k},b_{j,i,k})$，其中，$1\leqslant i\leqslant n,i\neq j$，$\mathrm{ID}_j$表示第$j$个参与者的身份信息，$g_{j,i,k}$表示在$\mathrm{GF}(p)$中随机选择的非空元素。

2.2.4　预认证阶段

预认证阶段执行切换前预处理。为简单起见，假设U与当前接入节点V_C之间的共享密钥为K_{UC}，当前接入节点V_C和S之间的共享密钥为K_{CS}，当前接入节点V_C和下一接入节点V_N之间的共享密钥为K_{CN}。

步骤 1　用户U_i向接入节点V_C发送预切换请求。U_i计算得到$\mathrm{MAC}_{U_i}^1=H_2(K_{\mathrm{UC}}\|\mathrm{TID}_{U_i}\|\mathrm{TID}_{V_C}\|\mathrm{ts}_1)$，$\mathrm{ts}_1$是用来抵抗重放攻击的时间戳。$U_i$生成预切换信息$H_{\mathrm{req1}}=\{\mathrm{TID}_{U_i},\mathrm{TID}_{V_C},\mathrm{ts}_1,\mathrm{MAC}_{U_i}^1\}$发送给当前接入节点$V_C$，其中$\mathrm{TID}_{V_C}$表示接入节点$V_C$的临时身份信息。

步骤 2　V_C验证U_i发送的信息，向S移交预请求消息。当前接入节点V_C接收到请求消息后，首先与当前时间进行比较，检查时间戳ts_1是否在允许的时间范围内。若ts_1正确，V_C利用K_{UC}检查$\mathrm{MAC}_{U_i}^1$的正确性，如果不正确，V_C拒绝预切换请求；否则，认为收到的$\mathrm{MAC}_{U_i}^1$来自合法用户。V_C计算$\mathrm{MAC}_{V_C}^1=H_2(K_{\mathrm{CS}}\|\mathrm{TID}_{V_C}\|\mathrm{TID}_{U_i}\|\mathrm{ts}_2)$，其中$\mathrm{ts}_2$表示$V_C$选择的时间戳。$V_C$将消息$H_{\mathrm{req2}}=\{\mathrm{TID}_{V_C},\mathrm{TID}_{U_i},\mathrm{ts}_2,\mathrm{MAC}_{V_C}^1\}$发送给$S$。

步骤 3　S为U_i选择下一接入节点V_N，将U_i当前预测信任状态和可用安全策略返回给V_C。S接收到信息H_{req2}后，首先检查时间戳ts_2是否正确，并利用K_{CS}检查$\mathrm{MAC}_{V_C}^1$的正确性。S选择下一接入节点V_N，并向信任系统查询U_i的当前预测信任状态和对应的安全策略，计算$H_{\mathrm{res1}}=\mathrm{Enc}_{K_{\mathrm{CS}}}(\mathrm{TID}_{U_i},\mathrm{TID}_{V_C},\mathrm{TID}_{V_N},T_T,\mathrm{ts}_3,\mathrm{Trust\ Level},\mathrm{ID}_{\mathrm{enc}},\mathrm{ID}_{\mathrm{int}})$，其中，$T_T$为当前信任等级生成的时间，Trust Level为当前信任等级，ts_3为S选择的时间戳，用于保证消息的有效性，$\mathrm{ID}_{\mathrm{enc}}$是保密性算法标识符，$\mathrm{ID}_{\mathrm{int}}$是完整性算法标识符，$\mathrm{Enc}_{K_{\mathrm{CS}}}(\cdot)$表示将括号内的数据计算完后加密发送给$V_N$，Enc表示对称加密算法，表示$S$用对称密钥$K_{\mathrm{CS}}$对信息进行加密，$\mathrm{TID}_{V_N}$表示接入节点$V_N$的临时身份信息。$S$返回消息$H_{\mathrm{res1}}$给$V_C$。

步骤 4　V_C收集相邻接入节点的秘密份额，与U_i确认可用的安全策略。V_C接收到H_{res1}后，检查时间戳ts_3，解密得到密文消息后计算$H_{\mathrm{req3}}=\mathrm{Enc}_{K_{\mathrm{UC}}}(\mathrm{TID}_{V_C},\mathrm{TID}_{U_i},\mathrm{TID}_{V_N},\mathrm{ts}_4,\mathrm{ID}_{\mathrm{enc}},\mathrm{ID}_{\mathrm{int}})$，其中，$\mathrm{ts}_4$表示$V_C$选择的时间戳。$V_C$将可用安全策略请求$H_{\mathrm{req3}}$发送给$U_i$。$V_C$收集与自己相邻的$m(1\leqslant m<t)$个接入节点的秘密份额，将自己秘密份额$\boldsymbol{s}_C$分别用相邻接入节点各自的公钥加密发送给他们，相邻接入节点收到并进行解密后，首先利用各自的$(g_{j,i,k},b_{j,i,k})$对V_C秘密份额$\boldsymbol{s}_C$进行验证，验证公式$b_{j,i,k}=g_{j,i,k}s_{i,k,0}+\mathrm{ID}_i s_{i,k,1}+\cdots+\mathrm{ID}_j^{t-1}s_{i,k,t-1}$是否成立。若验证成功，则将各自的秘密份额用$V_C$的公钥加密发送给$V_C$。否则，进行互通域内的局部重传，重新获取秘密份额。V_C收到m个接入节点的秘密份额后以相同的方式进行验证，将验证成功的秘密份额与U_i和V_C的秘密份额共$a(a<t)$份，组成秘密份额集合$S_a=\{\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m,\boldsymbol{s}_u,\boldsymbol{s}_C\}$，验证失败的秘密份

额则丢弃，其中，$\boldsymbol{s}_i(1 \leqslant i \leqslant m)$表示第$i$个接入节点的秘密份额。

步骤5　U_i接收到H_{req3}后，确认需要用到的安全策略。U_i计算$H_{\text{res2}} = \text{Enc}_{K_{\text{UC}}}\left(\text{TID}_{U_i},\text{TID}_{V_C},\text{ts}_5\right)$，其中，$\text{ts}_5$表示$U_i$选择的时间戳。$U_i$返回确认安全策略消息$H_{\text{res2}}$给$V_C$。

步骤6　V_C通知下一接入节点V_N收集秘密份额并同步安全策略，V_N返回确认信息后，V_C向U_i发送预切换请求响应消息。V_C计算$H_{\text{req4}} = \text{Enc}_{K_{\text{CN}}}\left(\text{TID}_{V_C},\text{TID}_{V_N},\text{ts}_6,\text{ID}_{\text{enc}},\text{ID}_{\text{int}}\right)$，其中，$\text{ts}_6$表示$V_C$选择的时间戳。$V_C$将同步消息$H_{\text{req3}}$发送给$V_N$。$V_N$收到并解密安全策略同步消息后，存储安全策略，用与$V_C$相同的方式对相邻$p(1 \leqslant p < t)$个接入节点的秘密份额进行收集和验证。验证结束后，$V_N$会拥有包含自己秘密份额在内的共$b(a+b \geqslant t)$份，组成秘密份额集合$S_b = \left\{\boldsymbol{s}_1,\cdots,\boldsymbol{s}_p,\boldsymbol{s}_N\right\}$。随后$V_N$返回确认消息$H_{\text{res3}} = \text{Enc}_{K_{\text{CN}}}\left(\text{TID}_{V_N},\text{TID}_{V_N},\text{ts}_7\right)$，其中，$\text{ts}_7$是$V_N$选择的时间戳。

步骤7　V_C返回$H_{\text{res4}} = \text{Enc}_{K_{\text{UC}}}\left(\text{TID}_{V_C},\text{TID}_{U_i},\text{ts}_8\right)$给$U_i$，其中，$\text{ts}_8$表示$V_C$选择的时间戳。

2.2.5　切换认证阶段

假设当前接入节点V_C与下一接入节点V_N之间的共享密钥为K_{CN}。终端切换认证协议交互时序如图5所示，具体流程如下。

步骤1　U_i向当前服务的接入节点发送切换请求。U_i生成切换信息$H_{\text{req5}} = \text{Enc}_{K_{\text{UC}}}\left(\boldsymbol{s}_u,\text{ts}_9\right)$发送给$V_C$，$\text{ts}_9$是用来抵抗重放攻击的时间戳。

步骤2　V_C收到切换请求消息后，通知V_N移动数据终端U_i正在执行切换认证。V_C收到切换请求消息H_{req5}后，首先与当前时间比较，检查时间戳ts_9是否在允许的时间范围内。若ts_9正确，则V_C利用K_{UC}检查$\text{MAC}_{U_i}^2$的正确性，如果不正确，V_C

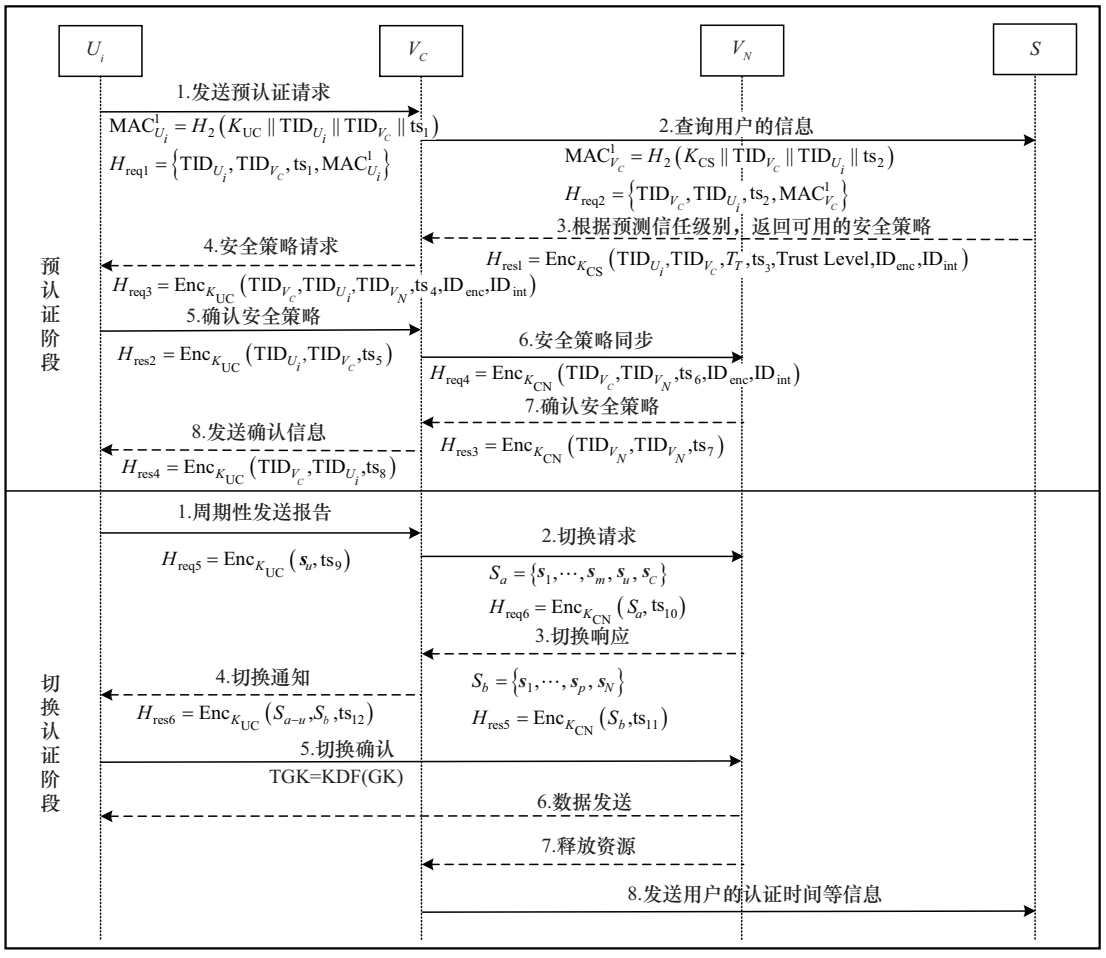

图5　终端切换认证协议交互时序

拒绝切换请求；否则，认为收到的$\mathrm{MAC}_{U_i}^2$来自合法用户。V_C根据收集的秘密份额集合$S_a=\{\boldsymbol{s}_1,\cdots,\boldsymbol{s}_m,\boldsymbol{s}_u,\boldsymbol{s}_C\}$，计算$H_{\mathrm{req6}}=\mathrm{Enc}_{K_{\mathrm{CN}}}(S_a,\mathrm{ts}_{10})$，其中，$\mathrm{ts}_{10}$表示$V_C$选择的时间戳。$V_C$将切换请求$H_{\mathrm{req6}}$发送给$V_N$。

步骤 3　V_N响应切换请求，重构秘密GK，计算与U_i的会话密钥TGK。V_N收到H_{req6}后，若处于空闲状态，则利用共享密钥K_{CN}解密收到的H_{req6}，检查时间戳ts_{10}是否在允许的时间范围内。若ts_{10}不在允许的时间范围内，V_N拒绝切换请求；否则，通过拉格朗日插值法计算出多项式在$k=l$位置的常数项a_l，利用S_a和S_b并根据等式$\mathrm{GK}=a_l\oplus d$，重构秘密GK，并计算与U_i的会话密钥$\mathrm{TGK}=\mathrm{KDF}(\mathrm{GK})$，其中KDF表示一个密钥派生函数，它是一个单向函数。V_N将自己的份额和验证过的秘密份额集合$S_b=\{\boldsymbol{s}_1,\cdots,\boldsymbol{s}_p,\boldsymbol{s}_N\}$作为响应信息的一部分，然后计算$H_{\mathrm{res5}}=\mathrm{Enc}_{K_{\mathrm{CN}}}(S_b,\mathrm{ts}_{11})$，其中，$\mathrm{ts}_{11}$表示$V_N$选择的时间戳。之后，$V_N$将含有秘密份额的响应信息$H_{\mathrm{res5}}$发送给$V_C$。

步骤 4　V_C收到相应信息后，利用共享密钥K_{CN}解密收到的响应信息H_{res5}，检查时间戳ts_{11}是否在允许的时间范围内。若ts_{11}不在允许的时间范围内，V_C拒绝切换转发；否则，V_C计算$H_{\mathrm{res6}}=\mathrm{Enc}_{K_{\mathrm{UC}}}(S_{a-u},S_b,\mathrm{ts}_{12})$，其中，$R_{C5}$表示$V_C$的随机数，$S_{a-u}$代表$S_a$中除去$\boldsymbol{s}_u$外秘密份额集合，$\mathrm{ts}_{12}$表示$V_C$选择的时间戳，之后再将响应消息$H_{\mathrm{res6}}$发送给$U_i$。

步骤 5　移动数据终端收到H_{res6}后，与当前时间比较，检查时间戳ts_{12}是否在允许的时间范围内，验证收到的s_C和s_N，如果验证成功，移动数据终端利用自己的秘密份额和收到的秘密份额S_{a-u}和S_b，重构出秘密GK，计算与V_N相同的会话密钥$\mathrm{TGK}=\mathrm{KDF}(\mathrm{GK})$，并用会话密钥加密切换确认消息，发送给$V_N$。

步骤 6　V_N收到切换确认消息后，切换完成，U_i与V_N进行数据的互相传输。

步骤 7　V_N通知V_C释放资源，则V_C不再向移动数据终端发送资源数据，以达到节约接入节点有限资源的目的。

步骤 8　V_C向S发送U_i的认证时间等信息，信任系统根据新的认证行为更新U_i的信任状态。

3　仿真分析

3.1　模型实验结果及分析

（1）马尔可夫链的性能边界

基于$A(t)$的边界推导预测概率的边界，选择最优θ^*在理论上可以确保边界收缩至最小。为验证Chernoff边界在累积信任过程中的紧致性及其对信任演化机制的敏感性，构建了多组具有不同信任演化特性的三态速率矩阵$\boldsymbol{Q}$，计算并绘制了不同$\boldsymbol{Q}$下$\rho(\theta)$与chernoff边界随θ变化的曲线，实验中对每条曲线均求解最优θ^*。结果显示，$\rho(\theta)$在各参数下表现为准线性增长，不同的$\boldsymbol{Q}$显著影响最优θ^*的取值与上界收敛速度，表明信任行为的动态演化机制直接决定边界收紧程度。

不同转移速率矩阵$\boldsymbol{Q}$对应的$\rho(\theta)$曲线变化如图6所示。从图6可以看出，当θ增大时，$\rho(\theta)$呈现单调递增趋势，且不同参数组合下曲线斜率存在显著差异。该实验验证了累积信任建模中$\rho(\theta)$对系统稳定性及概率界收敛速度的敏感性，为后续最优θ^*的选择提供了参考依据。Chernoff界与最优θ^*变化如图7所示，上界函数与下界函数在不同参数组合下展现出显著的非对称性，其中下界在$\theta\to 0$附近即达最优，而上界则存在偏移的最优截断点，说明参数选择将影响信任累积过程的尾概率控制能力。

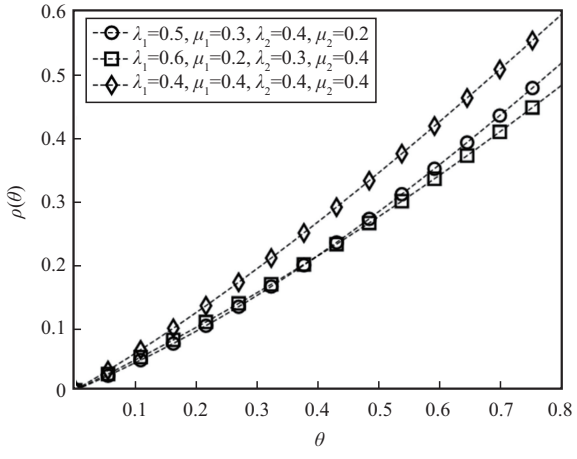

图6　不同转移速率矩阵$\boldsymbol{Q}$对应的$\rho(\theta)$曲线变化

（2）预测准确率

为验证基于三态马尔可夫过程的信任预测模型的有效性，设计了基于模拟节点行为的实验，采用

连续信任演化与预测相结合的方式进行评估。实验首先基于BCCTM模型模拟了正常节点的行为状态演化过程，节点初始处于中信任状态。

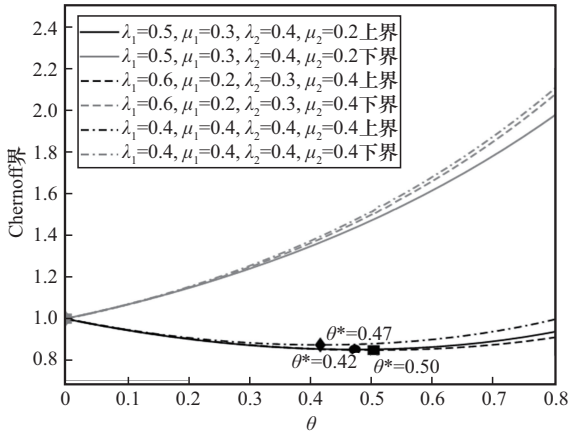

图7　Chernoff界与最优θ^*变化

信任预测模型在T_0步前基于推导的概率边界进行状态预测，以解决冷启动下的数据稀疏问题，当时间步达到切换点T_0后，模型切换为基于状态转移概率的三态马尔可夫模型，使用前T_0步的真实状态对转移矩阵进行学习和更新，从而实现长期稳定的信任状态预测。实验将T_0设置为20，兼顾早期预测的适应性与后期模型的稳定性。整个预测流程通过准确率进行评估，并结合信任值变化曲线与预测–真实状态对比图进行可视化分析。

基于三态马尔可夫过程的信任预测模型预测准确率评估如图8所示，模型在切换点T_0后能够快速准确地预测出节点真实的信任状态，整体预测准确率达到93.33%。该结果验证了本文模型在动态行为环境下的稳定性与鲁棒性。

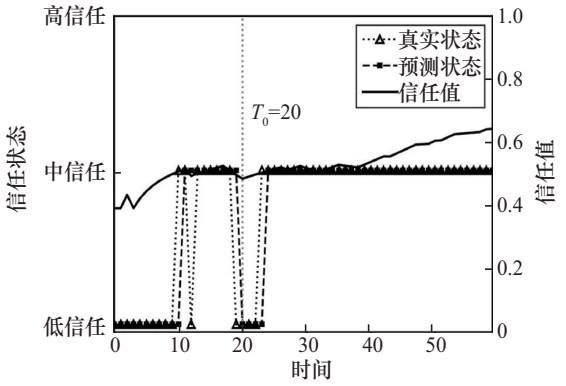

图8　基于三态马尔可夫过程的信任预测模型预测准确率评估

（3）模型对比

将本文模型与文献[20]提出的前馈神经网络（feedforward neural network, FNN）信任预测模型、文献[21]提出的支持向量机（support vector machine, SVM）信任预测模型作对比，实验结果如图9所示。其中，每个矩阵通过对比真实状态和预测状态展示模型的准确性，矩阵中的对角线数字表示正确预测，非对角线数字表示错误预测，颜色深浅表示对应分类的样本数量。本文模型整体表现最为稳定，在低、中两类信任状态的预测中具有较高的准确率，误判数量较少。FNN模型虽然对中信任状态具有一定的识别能力，但存在部分中类被误判为低类的情况。SVM模型在中等信任状态类别上的预测几乎完全正确，但在低类别上误判率相对较高。整体来看，本文模型在多类别信任状态识别中表现出更好的分类均衡性和泛化能力。

3.2　安全评估

3.2.1　理论安全性分析

在2.1.2节定义的敌手模型与信任假设下，本

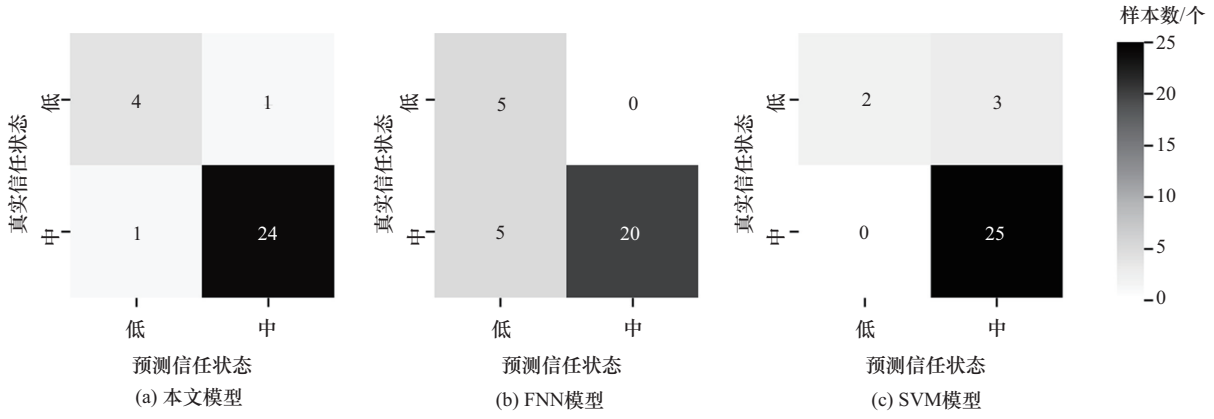

图9　不同模型信任等级分类混淆矩阵对比

节对协议的安全性进行理论论证。该模型假设敌手具备完全控制公开信道的能力，并可渗透部分DIAN节点，但受限于门限值t的约束。

（1）双向认证。本文认证方案能实现双向身份认证。在预置阶段，TA预先计算并分发秘密份额$\boldsymbol{s}_i=\left(\boldsymbol{s}_{i,1},\boldsymbol{s}_{i,2},\cdots,\boldsymbol{s}_{i,v}\right)$，通过安全信道将$\boldsymbol{s}_i$分发至同一互通域内的合法参与者，并向每个参与者发送$\left(g_{j,i,k},b_{j,i,k}\right)$。在切换时，认证方仅需出示自身的秘密份额，验证方便可通过$\left(g_{j,i,k},b_{j,i,k}\right)$验证等式$b_{j,i,k}=g_{j,i,k}s_{i,k,0}+\mathrm{ID}_j s_{i,k,1}+\cdots+\mathrm{ID}_j^{t-1}s_{i,k,t-1}$是否成立，实现高效可靠的切换阶段双向认证。基于敌手模型中的假设，敌手无法通过控制少数节点伪造合法的份额证明，从而确保了双向认证在敌手合谋上限内的可靠性。

（2）前向/后向安全性。在每次会话中使用一次性随机变量$a_i,c_{i,j}\in \mathrm{GF}(p)$，且$\mathrm{GK}=a_i\oplus d$，攻击者无法获取$a_i$，即使某次会话密钥被泄露，之前和未来的会话秘密也无法被推出。

（3）匿名性。本文认证方案中引入临时身份标识，所有身份相关交互均通过一次性标识TID_{U_i}进行，真实身份信息不在通信过程中直接暴露。攻击者必须破解哈希函数的单向性获取ID_{U_i}，这在计算上几乎不可行，从而实现认证过程中的参与者匿名性。

（4）防重放攻击。预置阶段使用随机变量$a_i,c_{i,j}$生成不可预测的共享份额，切换认证阶段，在认证信息中均使用时间戳字段，接收方在处理请求前首先验证时间戳的时效性，有效抵抗重放攻击行为。

（5）避免单点故障问题。方案使用无证书公钥密码体制，TA不需要持有终端或接入节点的完整私钥，仅参与部分密钥的初始化与分发，可以抵抗针对服务器的恶意攻击，避免单点故障问题。根据2.1.2节的信任假设，若TA暂时失效，合法参与者仍可利用本地存储的参数完成秘密重构，维持系统的可用性边界。

（6）抗冒充攻击。使用参与者身份信息ID_{U_i}作为多项式输入变量，计算生成的秘密份额$\boldsymbol{s}_i$与ID_{U_i}相关，冒充者无法合成合法份额$\boldsymbol{s}_i$，否则计算结果不一致，验证失败。

（7）抗中间人攻击。方案采用预共享GK、d以及密钥映射函数，且不在公开信道传输原始秘密参数，攻击者即使中间截获信息也无法恢复或篡改。

（8）抵抗恶意参与者篡改份额。秘密份额$\boldsymbol{s}_i$通过二元多项式$F(y,z)$构造，公开参数和身份变量绑定，同时，$\boldsymbol{s}_i$包含多个冗余值$\boldsymbol{s}_{i,k}$，支持一致性验证。在敌手模型的合谋规模限制内，份额$\boldsymbol{s}_i$与身份变量绑定，且支持一致性验证。若合谋数超过上限，安全性将发生退化。

进一步分析表明，本文方案在节点受损时具有良好的安全韧性与退化处理能力。当敌手能力表现为节点渗透时，即部分DIAN被攻破，攻击者仅能获得该节点的私有份额。由于本文方案采用分布式存储，根据本文定义的敌手模型，只要被攻破节点数未达到门限t，单一节点的失效就不会导致全局密钥GK泄露。若检测到某互通域内异常节点数增加，系统可动态调高门限值t，通过牺牲部分认证效率来提升攻击者的合谋代价，确保系统在高压力敌手环境下仍具韧性。

3.2.2　形式化验证

本节使用形式化验证工具Tamarin，基于2.1.2节定义的安全模型构建敌手模型，对本文方案进行了形式化安全性分析和验证。首先，针对方案的安全目标，给出以下形式化定义。

（1）存活性：定义引理Aliveness（存活性）。若实体A完成与B的协议交互，则B在此前必然已经启动过，确保了通信双方的真实存在性，可以有效抵御身份欺骗攻击。

（2）消息源认证：定义引理U_auth_RSU1、RSU2_auth_U等。若实体A接收到来自B的消息并完成认证，则B必然在此前发送过该消息。

（3）机密性：定义引理SecrecyMessage（消息机密性）和SecrecyKey（密钥机密性）。若消息n被定义为秘密，则在整个执行过程中，在未发生长期密钥泄露的前提下，攻击者无法推导该消息。

（4）可执行性：定义引理ExecutableRequest（可执行请求）和ExecutableConfirm（可执行确认）。通过exists-trace（存在性轨迹）验证是否存在至少一条有效路径，使实体间能够正确完成请求与响应的交互。

预认证阶段的验证结果如图10所示。所有与

认证相关的引理均在未发生长期密钥泄露的前提下通过自动证明，未发现攻击轨迹。这表明在攻击模型下，攻击者即使完全控制通信信道，也无法伪造关键认证消息或破坏协议的认证语义。具体而言，引理Aliveness确保了通信对端的真实存在性，引理U_auth_RSU1和RSU1_auth_S确保了消息源认证的有效性。同时，引理SecrecyMessage和SecrecyKey通过验证，说明被标记为秘密的通信数据不会进入攻击者知识集合。引理ExecutableRequest和ExecutableConfirm的成立表明协议规则集闭合且不存在死锁路径。

```
==============================================================================
summary of summaries:

analyzed: pre.spthy

  Aliveness (all-traces): verified (2 steps)
  U_auth_RSU1 (all-traces): verified (71 steps)
  RSU1_auth_S (all-traces): verified (14 steps)
  S_auth_RSU1 (all-traces): verified (71 steps)
  RSU1_auth_U (all-traces): verified (14 steps)
  SecrecyMessage (all-traces): verified (6916 steps)
  ExecutableRequest (exists-trace): verified (8 steps)
  ExecutableConfirm (exists-trace): verified (8 steps)
  SecrecyKey (exists-trace): verified (3 steps)

==============================================================================
```

图10　预认证阶段的验证结果

切换认证阶段的验证结果如图11所示。消息源认证相关引理如U_auth_RSU2和RSU2_auth_U均通过验证，说明在协议切换过程中，终端与目标DIAN间的关键认证消息无法被伪造或重放。引理SecrecyMessage和SecrecyKey通过证明，表明会话相关敏感信息在攻击者控制信道条件下仍保持保密。引理FunctionalCorrectness验证协议规则的逻辑一致性与可执行性，表明在建模假设下协议不存在内部冲突或未定义行为。

```
==============================================================================
summary of summaries:

analyzed: handover.spthy

  FunctionalCorrectness (exists-trace): verified (3 steps)
  U_auth_RSU2 (all-traces): verified (197 steps)
  RSU2_auth_U (all-traces): verified (3 steps)
  SecrecyMessage (all-traces): verified (17919 steps)
  ExecutableRequest (exists-trace): verified (7 steps)
  ExecutableConfirm1 (exists-trace): verified (4 steps)

==============================================================================
```

图11　切换认证阶段的验证结果

3.3　性能分析

本节从计算和通信开销两个方面，对本文方案与以下5种代表性方案进行性能对比：文献[22]提出的高效群组切换认证协议（efficient group-based handover authentication protocols，EGHR），文献[23]提出的固定轨迹群组预切换认证协议（fixed-trajectory group pre-handover authentication，FTGPHA）中的FTGPHA1与FTGPHA2，文献[15]提出的快速切换认证协议（fast handover authentication protocol，FHAP），以及文献[24]提出的基于区块链与Secgear（华为开源可信执行环境开发框架）的改进型LTE-R（铁路专用长期演进技术）接入认证方案（improved LTE-R access authentication scheme based on blockchain and Secgear，BSHAP）。

3.3.1　计算开销

本节评估了本文方案的计算开销，并与其他方案的计算开销进行了对比。为了方便统计，考虑部分操作的计算成本，级联操作和异或操作的计算开销太小，可以忽略。根据文献[15]的结果可以得到不同操作的计算时间如表3所示。

表3　单个运算操作执行时间

运算操作	定义	执行时间/μs
T_{M}	椭圆曲线点乘运算	1.00×10^{3}
T_{D}	椭圆曲线点乘运算	2.53
T_{H}	散列运算	2.39
T_{KDF}	密钥生成运算	2.42
T_{SIGN}	数字签名运算	1.20×10^{3}
T_{VER}	数字签名验证运算	0.81×10^{3}
T_{DEC}	非对称解密运算	0.08
T_{S}	对称加密或解密运算	2.26

不同方案的计算开销如表4所示。FTGPHA2因包含大量密钥协商操作而导致极高的计算负载，不利于资源受限终端使用；EGHR则因多次签名操作带来了较大的计算时延。相较之下，FHAP和BSHAP主要依赖于轻量级哈希及对称加密操作，整体计算开销显著较小，适合终端计算能力受限的应用场景。本文方案在计算开销方面表现最优，仅涉及1次哈希、2次密钥派生及4次简单加密操作，计算资源消耗极低，能够有效减轻计算负担。

表 4　　计算开销对比

方案	UE	Access node	Server	合计
EGHR[22]	$9T_{KDF} + 2T_S$	—	$11T_{KDF} + 2T_{SIGN} + 2T_{VER}$	$20T_{KDF} + 2T_{SIGN} + 2T_{VER} + 2T_S$
FTGPHA1[23]	$2T_H + 3T_{KDF} + T_S$	T_{KDF}	$T_H + 3T_{KDF} + T_S$	$3T_H + 7T_{KDF} + 2T_S$
FTGPHA2[23]	$3T_M + 3T_H + 2T_D + T_S$	$2T_S$	$4T_M + 5T_H + 3T_D + T_S$	$7T_M + 8T_H + 5T_D + 4T_S$
FHAP[15]	$3T_H + 4T_{KDF}$	$T_{DEC} + 2T_H + T_{KDF}$	—	$T_{DEC} + 5T_H + 5T_{KDF}$
BSHAP[24]	$T_H + 2T_S$	$3T_H + 2T_S$	—	$4T_H + 4T_S$
本文方案	$T_H + T_{KDF} + T_S$	$T_{KDF} + 3T_S$	—	$T_H + 2T_{KDF} + 4T_S$

3.3.2　通信开销

为评估各认证方案在带宽资源占用方面的性能差异，通信开销统计基于统一的密码学参数设定进行对比。其中，门限值 t 是平衡方案安全性、稳健性与资源开销的核心要素。在安全防御层面，只有当合谋节点数达到 t 时才能重构秘密 GK，因此高风险环境下应提高 t 值以增加破解代价。从性能均衡角度看，由于通信负载随 t 线性增长，在实时性要求极高的场景下选取较小的 t 值，如选取 $t = 3$，能显著降低认证时延。此外，在动态适应层面，若 t 选取过大可能导致因活跃节点不足而重构失败，故系统需遵循需求导向原则，根据信任预测及通信质量灵活配置 t 及其多项式阶数，确保认证流程的高可用性。其他具体参数设定如表 5 所示。

表 5　　参数设定

参数	取值/bit
身份标识	128
p, q	1 024, 160
安全参数 v	2
门限值 t	3
ECC 密钥	256
密钥生成函数的输出长度	256
哈希函数的输出长度	128
随机数	128
时间戳	32
其他信息	128

通信开销和信令开销对比结果如表 6 所示。由表 6 可知，本文方案在切换认证阶段的通信开销为 728 bit，支持双向认证与密钥协商；EGHR 通信开销为 6 979 bit，在 6 种方案中处于较高水平；FHAP、BSHAP 的通信开销虽低，但其切换认证阶段仅完成了认证，未包含密钥协商等后续过程的通信开销；本文方案虽在通信开销方面高于 FTGPHA1，但在计算开销和安全性方面优于该方案，仍具有一定优势。本文方案在保证认证协商能力的前提下控制了通信资源消耗，引入门限秘密共享与多向量验证机制增强安全性与抗攻击能力，在功能完整性、安全鲁棒性与资源可控性之间实现了较优平衡。

表 6　　通信开销和信令开销对比结果

方案	通信开销/bit	信令开销/次
EGHR[22]	6 979	19
FTGPHA1[23]	432	14
FTGPHA2[23]	928	14
FHAP[15]	182	6
BSHAP[24]	704	2
本文方案	728	2

3.3.3　信令开销

信令开销作为通信代价的动态衡量标准，由协议交互轮次、处理等待及时延表现共同决定。从表 6 可以看出，本文方案在核心切换阶段仅需 2 次信令交互即可完成切换认证。相比之下，对比方案呈现出明显的开销梯度，EGHR、FTGPHA1 与 FTGPHA2 在切换时分别需要 19 次、14 次与 14 次的高频信令交互。在参数敏感性上，门限参数 t 的增加虽然会使预置阶段的通信比特数上升，但由于本文

方案采用二元多项式重构，关键验证等待环节仅涉及简单的多项式求值，不需要复杂的双线性对运算。因此，重构时延随t的增长仍保持在较低水平。在鲁棒性代价上，当出现份额不足或验证失败等异常情况时，系统触发互通域内的局部重传机制。终端通过当前接入节点向邻居节点请求缺失分量，该过程不需要回溯至远程服务器。这种局部化的异常处理路径避免了长距离信令往返带来的高额损耗，在保障系统鲁棒性的同时，极大地降低了极端情况下的总体信令代价。

4 结束语

本文提出一种基于秘密共享的移动数据终端切换认证方案，该方案引入互通域概念，利用基于三态马尔可夫的信任预测模型动态调整节点信任等级，通过二元对称多项式秘密共享实现快速边缘切换认证，有效降低认证时延与冗余开销。互通域的局部聚合机制与边缘认证协同作用，使系统在大规模节点接入时仍能保持平稳的计算与通信开销。Tamarin形式化验证结果表明，本文方案安全可靠，适用于数联网环境中高动态、低时延及大规模接入场景。

参考文献：

[1] 李凤华, 李晖, 牛犇, 等. 数据要素流通与安全的研究范畴与未来发展趋势[J]. 通信学报, 2024, 45(5): 1-11.
Li F H, Li H, Niu B, et al. Research category and future development trend of data elements circulation and security[J]. Journal on Communications, 2024, 45(5): 1-11.

[2] 李恒, 李凤华, 史欣怡, 等. 面向数据跨域安全流通的访问控制研究综述[J]. 通信学报, 2025, 46(4): 238-254.
Li H, Li F H, Shi X Y, et al. Research on access control for secure cross-domain data circulation[J]. Journal on Communications, 2025, 46(4): 238-254.

[3] Wu H, Zhou B, Zhang C. Secure distributed estimation against data integrity attacks in Internet-of-things systems[J]. IEEE Transactions on Automation Science and Engineering, 2022, 19(3): 2552-2565.

[4] Chen X, Xue G L, Yu R Z, et al. A vehicular trust blockchain framework with scalable Byzantine consensus[J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 4440-4452.

[5] Yi W L, Xie Q L, Kuzmin S, et al. CCC-TM: Cross-Chain consensus committee method using a trust model[J]. Information Sciences, 2024, 677: 120930.

[6] Soleymani S A, Goudarzi S, Anisi M H, et al. TRUTH: trust and authentication scheme in 5G-IIoT[J]. IEEE Transactions on Industrial Informatics, 2023, 19(1): 880-889.

[7] Xiang X Y, Cao J, Fan W G. Secure authentication and trust management scheme for edge AI-enabled cyber-physical systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2025, 26(3): 3237-3249.

[8] Jamil M, Farhan M, Ullah F, et al. A lightweight zero trust framework for secure 5G VANET vehicular communication[J]. IEEE Wireless Communications, 2024, 31(6): 136-141.

[9] Dwivedi S K, Amin R, Vollala S, et al. B-HAS: blockchain-assisted efficient handover authentication and secure communication protocol in VANETs[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(6): 3491-3504.

[10] Chen Y, Liu W, Zhan Z. Safety certification for next generation high-speed railway heterogeneous network handover[J]. Journal of Cyber Security, 2022, 7(5): 79-90.

[11] Wang Y, Zhang W F, Wang X M, et al. Improving the security of LTE-R for high-speed railway: from the access authentication view[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(2): 1332-1346.

[12] 张海波, 兰凯, 陈舟, 等. 车联网中基于环的匿名高效批量认证与组密钥协商协议[J]. 通信学报, 2023, 44(6): 103-116.
Zhang H B, Lan K, Chen Z, et al. Ring-based efficient batch authentication and group key agreement protocol with anonymity in Internet of vehicles[J]. Journal on Communications, 2023, 44(6): 103-116.

[13] Nakkar M, Altawy R, Youssef A. GASE: a lightweight group authentication scheme with key agreement for edge computing applications[J]. IEEE Internet of Things Journal, 2023, 10(1): 840-854.

[14] Nakkar M, AlTawy R, Youssef A. Lightweight group authentication scheme leveraging Shamir's secret sharing and PUFs[J]. IEEE Transactions on Network Science and Engineering, 2024, 11(4): 3412-3429.

[15] Yang Y Y, Cao J, Ma R H, et al. FHAP: fast handover authentication protocol for high-speed mobile terminals in 5G satellite-terrestrial-integrated networks[J]. IEEE Internet of Things Journal, 2023, 10(15): 13959-13973.

[16] Li Z, Liu D, Li P, et al. Seamless group pre-handover authentication scheme for 5G high-speed rail network[M]. Berlin: Springer, 2022.

[17] Guo C, Hu G Y, Pan C L, et al. Authentication for satellite Internet resource slicing access based on trust measurement[J]. IEEE Internet of Things Journal, 2024, 11(12): 21788-21806.

[18] Fidler M. WLC15-2: a network calculus approach to probabilistic quality of service analysis of fading channels[C]//Proceedings of the IEEE Globecom 2006. Piscataway: IEEE Press, 2006: 1-6.

[19] Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey[J]. ACM Computing Surveys, 2009, 41(3): 1-58.

[20] Li X F, Wang Q, Li R. A trustworthiness sequence prediction scheme based on neural networks and mathematical calculations[J]. IEEE Internet of Things Journal, 2024, 11(12): 22643-22655.

[21] Shafi M, Jha R K, Jain S. Intelligent trust ranking security preserving model for B5G/6G[J]. IEEE Transactions on Network and Service Management, 2023, 20(3): 3549-3561.

[22] Cao J, Ma M D, Li H, et al. EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wireless networks[J]. Journal of Network and Computer Applications, 2018, 102: 1-16.

[23] Ma R H, Cao J, Feng D G, et al. FTGPHA: fixed-trajectory group pre-

handover authentication mechanism for mobile relays in 5G high-speed rail networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(2): 2126-2140.

[24] Liu X, Wang J Y, Wang M, et al. Improved LTE-R access authentication scheme based on blockchain and secgear[J]. IEEE Internet of Things Journal, 2024, 11(6): 10537-10550.

[作者简介]

郭超（1987– ），女，博士，中国科学院信息工程研究所在站博士后，北京电子科技学院副教授、硕士生导师，主要研究方向为网络与信息安全、数据安全。

于梦格（2000– ），女，北京电子科技学院硕士生，主要研究方向为网络认证协议。

张玲翠（1986– ），女，博士，中国科学院信息工程研究所高级工程师、硕士生导师，主要研究方向为网络与信息安全、数据安全。

翟佳乐（2000– ），男，中国科学院信息工程研究所硕士生，主要研究方向为网络与信息安全、数据安全。

邓溶（2002– ），女，北京电子科技学院硕士生，主要研究方向为安全协议、抗量子密码等。