文章编号:1007-5321(2021)02-0054-07 **DOI**:10.13190/j.jbupt.2020-203

一种信息中心移动自组网中的数据访问控制机制

刘宁春[1], 郜 帅[1,2], 侯心迪[1], 国兴昌[1]
(1. 北京交通大学 电子信息工程学院, 北京 100044; 2. 鹏城实验室 网络通信研究中心, 深圳 518052)

摘要: 针对信息中心移动自组网场景中节点间间歇连接和网内泛在缓存的特点,提出一种基于门限秘密共享机制的数据访问控制机制. 通过构建辅助密钥块,降低了消费者解密的开销和网络节点的存储资源消耗. 同时,通过引入双变量单向函数,保障了消费者子秘密份额的唯一性,减少了消费者侧秘密份额管理所带来的空间开销. 仿真和理论分析结果表明,该机制显著降低了消费者侧的解密开销,良好地适应了信息中心移动自组织网络场景.

关 键 词: 信息中心移动自组网; 数据访问控制; 门限秘密共享; 双变量单向函数
中图分类号: TP393 **文献标志码**: A

A Data Access Control Scheme in Information-Centric Mobile Ad Hoc Networks

LIU Ning-chun[1], GAO Shuai[1,2], HOU Xin-di[1], GUO Xing-chang[1]
(1. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China;
2. Peng Cheng Laboratory Research Center of Networks and Communications, Peng Cheng Laboratory, Shenzhen 518052, China)

Abstract: Aiming at the characteristics of intermittent connections between nodes and ubiquitous caching in the information-centric mobile Ad hoc networks, a data access control scheme based on threshold secret sharing scheme is proposed. By constructing an auxiliary key block, the consumer's decryption overhead and the storage resource consumption of network nodes are reduced. At the same time, by combining a two-variable one-way function, the uniqueness of the consumer's shares is guaranteed, and the cost of key management is decreased. Simulations show that this mechanism dramatically reduces the decryption overhead on the consumer side, which indicates its well suited for information-centric mobile Ad hoc network scenarios.

Key words: information-centric mobile Ad hoc network; data access control; threshold secret sharing; two-variable one-way function

为了保持与传统的传输控制协议/网际协议(TCP/IP, transmission control protocol/Internet protocol)栈的兼容性,当前的移动自组织网络(MANET, mobile Ad hoc networks)架构大多采用面向主机的通信模式,通常假定在通信过程中节点间至少存在 1 条完整的端到端通信路径,这与 MANET 环境下节点存在频繁移动导致网络拓扑的动态变化以及节点之间间歇连接的特点互相矛盾[1].

收稿日期: 2020-10-08
基金项目: 国家重点研发计划项目(2019YFB1802503); 国家自然科学基金项目(61972026, 61802014); 鹏城实验室大湾区未来网络试验与应用环境项目(LZC0019)
作者简介: 刘宁春(1994—), 男, 博士生.
通信作者: 郜 帅(1980—), 男, 教授, E-mail: shgao@bjtu.edu.cn.

近年来，作为一种颠覆式的网络架构，信息中心网络（ICN，information-centric networking）的研究受到广泛关注[2]. 在 ICN 通信过程中，通信双方无须建立和维护端到端的持续连接，这符合 MANET 中网络节点之间间歇连接的特点. 同时，ICN 具有支持网内泛在缓存、基于全网唯一的内容名称进行寻址路由等特性，使得 MANET 中的网络节点可以借助无线信道的广播特性缓存更多的内容，进一步提高内容的利用率. 因此，信息中心移动自组网（ICMANET，information-centric mobile Ad hoc networks）逐渐成为一个全新的交叉研究领域[1].

由于 ICN 具有上述新特性，在 ICN 安全相关的研究中，研究者更加关注如何保证内容本身的安全，而非传统上基于 TCP/IP 网络架构中通信信道的安全[3]. 因而，数据访问控制（DAC，data access control）成为 ICN 安全的重要研究方向[4]. 具体来说，ICN 中泛在缓存的目的是使消费者可以就近从不受内容生产者（CP，content producer）控制的中间路由器获得缓存内容，从而节省了网络带宽. 与之矛盾的是，CP 只希望合法的消费者才能获取对应的内容. 由于中间路由器的转发行为通常不受 CP 的控制，所以，如何在中间路由器进行 DAC 成为难点[5]. 在 ICMANET 场景中，节点间歇性连接导致 CP 与网络的连接时断时续，这一问题更加突出.

当前，ICMANET 的研究工作主要集中在以内容为中心的路由机制方面，在 DAC 机制方面的研究工作较为缺乏[1].

按认证实体分布的不同位置进行划分，ICN 中 DAC 机制主要分为 3 类. 第 1 类是基于节点认证技术的访问控制机制[6]. 在这类机制中，消费者在获取 CP 生产的加密内容后，仍需要与 CP 委托的认证实体进行认证，进而获得相应的解密密钥. 保证消费者和认证实体之间的可靠连接，由于在 ICMANET 场景中节点之间间歇性连接，而在上述机制中，消费者和认证实体之间需要保证可靠连接. 因此，这类机制并不适用于 ICMANET 场景. 第 2 类机制是通过使用特定的数据加密技术（属性加密技术[7]和身份加密技术[8]等）保障 DAC，即 CP 使用特定的加密技术加密内容，并将加密后的内容发布到网络，消费者在获取加密内容后，可以使用自身的属性或身份信息解密，获得内容. 这类机制虽然不需要消费者和 CP 之间的可靠连接，但却存在初始化开销大、消费者解密开销大和缺乏对消费者撤销的支持等问题，并不适用于网络节点资源受限的 ICMANET 场景. 第 3 类机制是基于秘密共享机制保障 DAC[9-10]. 这类机制可保障 CP 离线下的 DAC. 在上述机制中，消费者为解密不同 CP 生产的加密内容，需要保存不同 CP 为其分发的秘密份额，极大地占用了节点资源，并不适用于网络节点资源受限的 ICMANET 场景，且这些秘密份额在系统初始化后均不再变化，这又成为了网络安全的潜在隐患.

因此，在已有研究工作[9]的基础上，设计了一种可用于 ICMANET 场景的 DAC 机制，引入 Shamir 门限秘密共享机制，将 DAC 和 CP 解耦；引入辅助密钥块并进行预先计算和网内缓存，减少了消费者获取辅助密钥块的时延，降低了消费者进行解密的开销和网络节点的存储资源消耗；引入二维单向函数，保障了消费者秘密份额的唯一性，减少了消费者侧秘密份额管理所带来的空间开销.

1　基本定义与符号描述

表 1 所示为方案设计中所使用符号的含义.

表 1　符号描述

符号	含义
$\mathrm{GF}(Q)$	Q 元有限域
Z_Q^*	以 Q 为阶的乘法群
G_Q	以 Q 为阶的循环群
g	G_Q 的生成元
Q	大素数
$f(x,y)$	双变量单向函数
$h_t(x)$	一维 t 阶多项式
a_0	$h_t(x)$ 的常数项
t	$h_t(x)$ 的次数和支持撤销用户数量的阈值
n	合法消费者的数量
R	已撤销消费者的数量，$R \leqslant t$
γ	数据加密所使用的对称密钥
l	加密后的对称密钥
$T_i=(x_i,h(x_i))$	合法消费者 C_i 的子秘密份额
$T_r=(x_r,h(x_r))$	已撤销消费者 C_r 的子秘密份额
χ	合法消费者随机参数 x_i 的集合
$(P_c,\ \mathrm{PR}_c)$	CP 的公私钥对
(P_i,PR_i)	合法消费者 C_i 的公私钥对

定义 1　Shamir 门限秘密共享机制

在 Shamir 秘密共享机制中，一个秘密可以分享给 n 个用户，至少需要 $t+1(t+1\leqslant n)$ 个用户联合使用自身秘密份额，才能还原秘密. 该机制可使用一

维 t 阶多项式 $h(x)=a_0+a_1x^1+a_2x^2+\cdots+a_tx^t$ 实现. 由于一维 t 阶多项式 $h(x)$ 可以被式中的 $t+1$ 个点唯一确定,当 $t+1$ 个用户把各自的秘密份额结合起来时,可使用拉格朗日插值方法构建出唯一的一维 t 阶拉格朗日插值多项式 $h_t(x)$,在此基础上可以得到秘密 $a_0=h_t(0)$[11].

2 方案设计

2.1 系统模型与假设

在系统模型中,通信节点包括合法的消费者 $C_i(i=1,2,\cdots,n)$、CP 以及已撤销的消费者 C_r,指挥中心为负责安全机制预配置的实体,转发节点是网络中具有缓存功能的无线路由器.

由于命名数据网络(NDN, name data networking)是一种典型的 ICN 架构,下文将以 NDN 为背景详细阐述 DAC-ICMANET 机制的设计细节、理论分析和仿真验证. 考虑到 ICN 架构的共性特点,本机制可以扩展至其他的 ICN 架构中.

此外,由于不同内容生产者在本机制中所进行的初始化、内容生产加密与辅助密钥块构建和分发的过程相同,为了便于描述,规定网络中仅有 1 个 CP 和 n 个合法的消费者 $C_i(i=1,2,\cdots,n)$. 此外,假设消费者的设备终端在解密内容后,不存储加密内容所使用的对称密钥. 同时,针对通过持续请求不流行的内容来操纵兴趣包到达 NDN 中间节点的分布特性,最后达到控制 NDN 中间节点的缓存内容分布这一缓存污染攻击. 由于其仅仅改变了中间节点的缓存内容分布,使得在中间节点,包含辅助密钥块的 Data 包被消费者请求的命中率降低,但并不会篡改缓存内容,对本机制的整体策略影响较小,因此,假设中间节点不会遭受缓存污染攻击.

所设计机制的安全性建立在以上假设和判定性 Diffie-Hellman 难题(DDH, decisional Diffie-Hellman problem)[12]的基础之上.

2.2 机制概述

DAC-ICMANET 机制的工作流程包含 3 个主要步骤,如图 1 所示,其中,第 1 步是系统初始化,包括指挥中心为消费者和 CP 分发公私钥对、消费者注册、CP 侧的多项式和秘密份额生成. 第 2 步是辅助密钥块的生成和内容的加密处理,包括 CP 使用对称密钥对内容进行加密并对对称密钥进行分割并构建辅助密钥块. 第 3 步是加密内容/辅助密钥块获取与内容解密,包括加密内容块获取,辅助解密块获取和解密对称密钥. 在本机制中,第 1 步需要指挥中心为网络节点分发公私钥对(或预先配置),同时消费者和 CP 进行协商;第 2 步在 CP 侧完成,第 3 步在消费者 C_i 侧完成.

考虑到本机制的系统初始化阶段中,需要消费者能够主动发送包含消费者参数信息的 Data 包. 同时,在辅助密钥块的生成阶段,需要 CP 能够主动发送包含辅助密钥块的 Data 包. 为此,需要修改原始 NDN 中的 Data 包格式. 在本机制中,通过在 Data 包中增加了 Flag 字段对 2 类 Data 包进行区分.

2.3 系统预配置和初始化

在系统预配置和初始化阶段,指挥中心会选择一个有限域 GF(Q)上的双变量单向函数 $f(x,y)$[13],作为公开参数公布,并为每一个合法的网络节点(包括 CP 和消费者 C_i)生成唯一的公私钥对(P_c, PR_c)和(P_i, PR_i),其中公钥公开发布,私钥通过离线预配置的方式发送给网络节点. 同时,网络

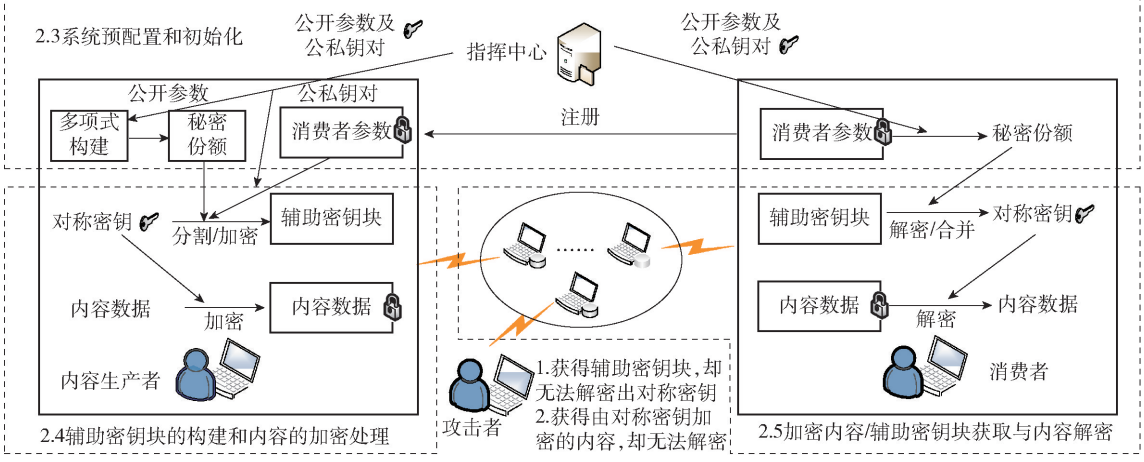

图 1 DAC-ICMANET 机制的工作流程

内消费者 C_i会向 CP 进行注册,其注册步骤如下:

1) 消费者 C_i生成随机参数 $x_i \in Z_Q^*$,并使用 CP 的公钥 P_c将该 x_i 加密,并将加密后的内容发送给 CP;

2) CP 首先使用私钥 PR_c解密数据包后获得随机参数 x_i,并验证该随机参数是否与已有消费者随机参数的集合 χ 中的元素相同. 如果不相同,则将 x_i 存入消费者随机参数的集合 χ 中;如果相同,则要求该消费者 C_i重新生成 x_i,直至满足唯一性,得到消费者随机参数的集合 $\chi = \{x_1, x_2, \cdots, x_n\}$.

在此基础上,CP 侧需要构建多项式并生成子秘密份额,具体流程如算法 1 所示.

算法 1　多项式构建和子秘密份额的生成

输入: 合法消费者的数量 n;$h_t(x)$ 的次数和支持撤销用户数量的阈值 t;大素数 Q;双变量单向函数 $f(x,y)$;消费者随机参数的集合 χ.

输出: $T_i = [x_i, h(x_i)]\ (i = 1,2,\cdots,n)$,公开参数 Θ.

1) 生成 $t+1$ 个随机数 $a_i \in Z_Q^*\ (i = 0,1,2,\cdots,t)$.

2) 使用步骤 1 中的随机数,生成一维 t 阶多项式 $h_t(x) = a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_t x^t$.

3) 随机生成 t 个 $x_j \in Z_Q^*\ (j = 0,1,2,\cdots,t-1)$.

4) 计算 $h(x_j) = h_t(x_j) \in Z_Q^*$.

5) 存储 t 个秘密份额 $T_j = [x_j, h(x_j)]$(保留在 CP 处).

6) 随机生成 $\rho \in Z_Q^*$,并作为公开参数发布.

7) 计算 $h(x_i) = h_t(x_i) \in Z_Q^*$.

8) 计算 $\Theta = \{S_i \mid S_i = h(x_i) + f(x_i, \rho)\}\ (i = 1, 2,\cdots,n)$,其中 $x_i \in \chi$,Θ 作为公开参数发布.

9) 存储 n 个消费者的子秘密份额 $T_i = [x_i, h(x_i)]$.

2.4　辅助密钥块的构建和内容的加密处理

考虑到 ICMANET 场景中网内泛在缓存的特点,为了减小消费者解密对称密钥数据块的开销,构建辅助秘密钥块数据包. 为保障消费者撤销的后向安全性,将辅助密钥块单独命名为 1 个 Data 包,其缓存策略与普通的 Data 包一致. 以指挥中心发出数据 A 为例,其辅助密钥块名称前缀为("/military/center/data/A/aux"). 由于辅助密钥块是消费者解密过程中的中间量,所以,本机制可减小消费者解密对称密钥数据块的开销. 同时,为了保证辅助密钥块的真实性,辅助密钥块使用 CP 的私钥进行签名. 此外,考虑到用于内容加密的对称密钥通常位数较多〔在高级加密标准(AES, advanced encryption standard)中使用的 256 位对称密钥〕. 因此,首先需要对于对称密钥 γ 进行分割,以保证分割后的每一个子对称密钥 $\gamma_1, \gamma_2, \cdots, \gamma_m \in Z_Q^*$,在消费者 C_i处,对 m 个子对称密钥进行聚合. 在算法 2 中,描述了 CP 构建辅助密钥块并进行内容加密处理的详细过程.

算法 2　内容加密和辅助密钥块的生成

输入: G_Q 的生成元 g,以 Q 为阶的循环群 G_Q,对称密钥 γ(包含 m 个子对称密钥).

输出: 辅助密钥块 AUX.

1) 生成随机数 $r \in Z_Q^*$.

2) 计算 $l_i = \gamma_i g^{ra_0}$,其中,ra_0 和 $\gamma_i g^{ra_0} \in Z_Q^*$.

3) 计算 $g^r \in Z_Q^*$.

4) 计算部分拉格朗日系数:

$$\Lambda = \left\{ \hat{\lambda}_j \mid \hat{\lambda}_j = \prod_{0 \le i \ne j \le t-1} \frac{-x_j}{x_i - x_j} \in Z_Q^* \right\}$$

5) 计算 CP 处的 t 个秘密份额 x_j 及 $g^{rh(x_j)}\ (j = 0,1,2,\cdots,t-1)$,其中 $rh(x_j)$ 和 $g^{rh(x_j)} \in Z_Q^*$.

6) 辅助密钥块为

$$\mathrm{AUX} = \langle l_i, g^r, \Lambda, x_j, g^{rh(x_j)} \rangle,$$
$$i = 1,2,\cdots,m \text{ 及 } j = 0,1,2,\cdots,t-1$$

7) 当消费者 C_i撤销后,CP 需使用 C_i对应的子秘密份额 $[x_i, h(x_i)]$ 替换步骤 5) 中的任一秘密份额,并重新执行步骤 5) 和 6).

2.5　加密内容/辅助密钥块获取与内容解密

消费者 C_i在获取由对称密钥 γ 加密的内容(名称前缀为/military/center/data/A)后,根据加密内容的内容名称构建 Interest 包(名称前缀为/military/center/data/A/aux)请求相应的辅助密钥块数据包,结合自身拥有的秘密份额 $\langle x_i, S_i \rangle$,进而计算出对称密钥 γ. 以任一子对称密钥为例,算法 3 描述了消费者 C_i使用辅助密钥块结合自身拥有的秘密份额解密获得加密对称密钥,并通过加密对称密钥解密内容的详细过程.

算法 3　加密内容的获取与解密

输入: 辅助解密块 AUX;消费者 C_i的随机参数秘密份额 x_i;包含 S_i 的公开参数 Θ;双变量单向函数 $f(x,y)$;随机数 ρ.

输出: 解密内容块所使用的子对称密钥 $\gamma_i\ (i = 1,2,\cdots,m)$.

1) 计算拉格朗日系数 $\lambda_j = \hat{\lambda}_j \dfrac{-x_i}{x_j - x_i} \in Z_Q^*$, $\forall \hat{\lambda}_j \in \Lambda$.

2）计算 $\vartheta_1 = \prod_{0\leqslant j\leqslant t-1} g^{rh(x_j)\lambda_j}, \vartheta_1 \in Z_Q^*$.

3）计算 $h(x_i) = S_i - f(x_i,\rho)$（结合辅助解密块计算对称密钥 γ）.

4）计算 $\vartheta_2 = (g^r)^{h(x_i)\lambda_i}$，其中 $\lambda_i = \prod_{0\leqslant j\leqslant t} \frac{-x_j}{x_i - x_j}$.

5）计算对称密钥 $\gamma_i = \frac{l_i}{\vartheta_1\vartheta_2}$（证明过程详见定理1）.

6）使用对称密钥 γ 对所获得的加密内容进行解密.

定理1 根据算法3，一个合法的消费者 C_i 能够使用辅助密钥块 AUX、包含 S_i 的公开参数 Θ、双变量单向函数 $f(x,y)$、随机数 ρ 和自身的秘密份额 x_i 正确地解密获得子对称密钥 $\gamma_i(i=1,2,\cdots,m)$，进而获得对称密钥 γ.

证明

1）由定义1可知，$h_t(0) = h(x_0)\lambda_0 + h(x_1)\lambda_1 + \cdots + h(x_t)\lambda_t$ 且 $a_0 = h_t(0)$. 其中

$$\lambda_i = \prod_{0\leqslant i\neq j\leqslant t} -\frac{x_j}{x_i - x_j}$$

2）由算法3知，$\vartheta_1 = \prod_{0\leqslant j\leqslant t-1} g^{rh(x_j)\lambda_j}$，$\vartheta_2 = (g^r)^{h(x_i)\lambda_i}$. 其中

$$\lambda_i = \prod_{0\leqslant j\leqslant t} \frac{-x_j}{x_i - x_j}, h(x_i) = S_i - f(x_i,\rho)$$

$$\vartheta_1\vartheta_2 = \prod_{0\leqslant j\leqslant t-1} g^{rh(x_j)\lambda_j}(g^r)^{h(x_i)\lambda_i} =$$

$$g^{r[h(x_0)\lambda_0 + h(x_1)\lambda_1 + \cdots + h(x_{t-1})\lambda_{t-1})]}(g^r)^{h(x_i)\lambda_i} =$$

$$g^{r[h(x_0)\lambda_0 + h(x_1)\lambda_1 + \cdots + h(x_{t-1})\lambda_{t-1} + h(x_i)\lambda_i]} =$$

$$g^{r[h(x_0)\lambda_0 + h(x_1)\lambda_1 + \cdots + h(x_t)\lambda_t]} = g^{rh_t(0)} = g^{ra_0}$$

3）由算法2已知，$l_i = \gamma_i g^{ra_0}(i=1,2,\cdots,m)$，故 $\frac{l_i}{\vartheta_1\vartheta_2} = \gamma_i$，由此可以恢复出对称密钥 γ，得证.

3 安全性分析

3.1 辅助密钥块的安全性

在本机制中，攻击者无法通过辅助密钥块提供信息解密获得原始数据，形式化证明如下. 由定义1可知，一维 t 阶多项式可以被多项式上的 $t+1$ 点唯一确定. 同时，根据算法2知，辅助密钥块 AUX 仅包含 t 个秘密份额 $\langle x_j, g^{rh(x_j)}\rangle (j=0,1,2,\cdots,t-1)$. 因此，通过辅助密钥块无法在多项式时间内解密获得对称密钥 γ，保障了数据的真实性.

3.2 消费者子秘密份额的安全性

由于消费者 C_i 仅在注册阶段向 CP 提供经过 CP 公钥加密的 x_i，而在后续包含 S_i 的辅助密钥块 AUX 的获取中，消费者的秘密份额 x_i 并不需要在网络上传输. 由双变量单向函数的定义知，消费者可根据包含在辅助密钥块 AUX 中的 S_i，结合双变量单向函数 $f(x_i,\rho)$，计算 $h(x_i) = S_i - f(x_i,\rho)$，进而可解密获得对称密钥. 由双变量单向函数的单向性可知，该计算不可逆，即通过 $h(x_i)$ 和 S_i 无法得出消费者的秘密份额 x_i. 因此，即便攻击者获得了辅助密钥块中的 S_i 和 ρ，也无法解密获得原始数据. 基于这一特性，与文献[10]中描述的机制不同，本机制可以在消费者 C_i 子秘密份额 x_i 保持不变的情况下，针对来自不同 CP 加密内容的获取，即消费者仅需要事先向不同 CP 进行注册，而不需要为不同 CP 在本地保存不同的子秘密份额，从而在保障安全性的前提下，节约了消费者侧秘密份额管理的开销.

3.3 消费者撤销的后向安全性

当已撤销消费者数量 R 小于等于一维多项式 $h_t(x)$ 次数 t 的情况下，本机制可以保障消费者撤销的后向安全性，并可以防止已撤销消费者的共谋攻击，形式化证明如下.

在本机制中，当消费者 C_i 撤销后，根据算法2知，CP 需要执行步骤7），因此，已撤销的消费者手中的秘密份额必然与辅助密钥块中 t 个秘密份额中的某一份额相同，最多可以获得 t 个秘密份额. 由定义1可知，一维 t 阶多项式可以被多项式上的 $t+1$ 点唯一确定. 因此，已撤销的消费者通过辅助密钥块无法在多项式时间内解密而获得对称密钥 γ. 同时，由假设知，已撤销消费者数量 R 小于等于一维多项式 $h_t(x)$ 的次数 t. 因此，即使已撤销消费者进行共谋攻击，也最多可以获得 t 个秘密份额，无法最多可以获得 t 个秘密份额，从而保障了消费者撤销的后向安全性.

4 性能评估

4.1 仿真环境

为了评估所提出 DAC 机制的性能，在 ndnSIMv2.5 仿真平台[14]上，分别构建了包含 50、100、150 和 200 节点的网络拓扑，并进行了仿真验证. 仿真环境为 3.3 GHz Intel Core i5-4590 处理器；8 GB 内存；Ubuntu 16.04 操作系统. 仿真实验中，Data 包采用 AES256 对称加密算法，使用改进后的 Shamir 门限秘密共享机制对 256 位对称密钥进行分割加

密. 同时,使用了自由软件基金会高精度算术运算库 v6. 2. 0[15]. 部分仿真参数设置如表 2 所示.

表 2　仿真参数设置

参数	值
网络节点数量/个	50/100/150/200
节点的初始间距/m	20
节点运动范围/m^2	1 000 ×600
数据模型/($Mbit^{-1}\cdot s^{-1}$)	OfdmRate24
最大传输距离/m	50
Interest 包发送速率/($个\cdot s^{-1}$)	10
Data 包载荷大小/KB	4

4. 2　仿真验证

1) 初始化时间开销

本机制的初始化时间开销主要包括 CP 侧的多项式及子秘密份额生成时间和辅助密钥块的构建时间.

首先选取 CP 侧的多项式及子秘密份额生成时间作为评估参数. 图 2 所示为网络节点数量 n 分别为 50、100、150、200 个情况下的仿真结果. 其中,随机选取 1 个网络节点为 CP,其他节点为消费者. 从仿真结果发现,初始化时间与阈值 t 呈正相关,同时随着网络节点数量 n 的增大,初始化时间也不断增大. 在 200 节点网络规模下,阈值 t 选取 50,此时的多项式和子秘密份额生成的时间为 468 ms.

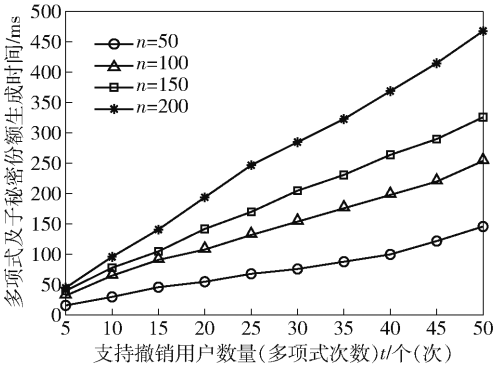

图 2　多项式及子秘密份额的生成时间

2) 加密内容和辅助密钥块的获取时延

为评估本机制在获取额外的辅助密钥块所带来的时间开销,将获取加密内容及辅助密钥块的时间作为评估参数,与传统 DAC-Shamir 机制(该机制将 Shamir 门限秘密共享机制用于 DAC 中,通过分别获取其他 t 个秘密份额数据包,还原原始秘密,CDAC 机制[9]与其类似)和 AccConF 机制[10]进行对比. 仿真结果如图 3 所示,选取的支持撤销用户数量的阈值 t 为 10.

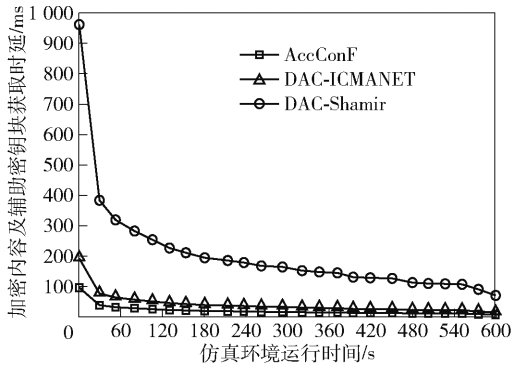

图 3　获取加密内容和辅助密钥块的时间

由于在机制中引入了辅助密钥块这一消费者解密的中间变量,使解密加密内容增加了获取辅助密钥块这一步骤,与 AccConF 机制相比,虽然在仿真环境运行的初始阶段增加了少量的时间开销,但保障了消费者撤销的后向安全性. 同时,由于辅助密钥块包含 t 个秘密份额,避免产生传统 DAC-Shamir 机制中,消费者需要分别获取其他 t 个秘密份额数据包的额外步骤,减少了这些额外步骤所带来的额外时延. 同时,由于在 DAC-ICMANET 机制中,网络中间节点只需要缓存 1 个辅助密钥块数据包,而不是传统 DAC-Shamir 机制中的 t 个数据包. 所以,也减少了网络节点的存储资源消耗. 此外,随着仿真环境运行时间的增加,辅助密钥块(包括秘密份额)的获取时延明显降低. 其主要原因是,ICMANET 环境的网内泛在缓存特性使得辅助密钥块数据包在网络节点中被大量缓存.

3) 消费者解密开销

为了评估本机制消费者侧的解密开销,选取消费者通过使用自身的秘密份额结合辅助密钥块数据包解密对称密钥的时间开销作为评估参数,与传统 DAC-Shamir 机制和 AccConF 机制进行对比. 仿真结果如图 4 所示.

根据仿真结果,在消费者解密获得对称密钥的时间开销方面,在传统 DAC-Shamir 机制中,消费者解密获得对称密钥的时间开销与支持撤销用户数量的阈值呈正相关,所提 DAC-ICMANET 机制相比传统 DAC-Shamir 机制体现出巨大的优势,原因是所设计机制对传统 DAC-Shamir 机制进行了改进,在辅助密钥块中对于 t 个秘密份额进行了预先计算,降低了消费者侧的解密开销. 同时由于 DAC-ICMANET

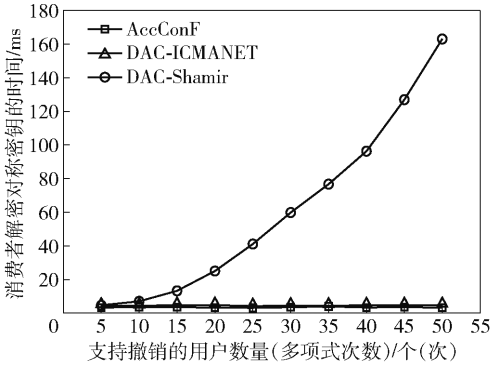

图4 消费者解密对称密钥的时间

机制相比于 AccConF 机制在消费者侧多出通过计算双变量单向哈希函数获得子秘密份额 $h(x_i)$ 的步骤,增加了极少量消费者解密获得对称密钥的时间开销,并以此为代价保障了消费者秘密份额的唯一性.

5 结束语

提出了一种适用于 ICMANET 场景的 DAC 机制 DAC-ICMANET,并详细阐述了该机制的设计细节,包括系统预配置和初始化、辅助密钥块的构建和内容的加密处理、加密内容/辅助密钥块的获取和内容解密. 最后通过理论分析和仿真实验验证了所提机制在 ICMANET 场景具有良好的适应性并显著降低了消费者侧的解密开销.

参考文献:

[1] Liu X, Li Z, Yang P, et al. Information-centric mobile Ad hoc networks and content routing: a survey[J]. Ad Hoc Networks, 2017, 58: 255-268.

[2] Yu K, Eum S, Kurita T, et al. Information-centric networking: research and standardization status[J]. IEEE Access, 2019, 7: 126164-126176.

[3] Zhang Z, Yu Y, Zhang H, et al. An overview of security support in named data networking[J]. IEEE Communications Magazine, 2018, 56(11): 62-68.

[4] Xue K, He P, Zhang X, et al. A secure, efficient, and accountable edge-based access control framework for information centric networks[J]. IEEE/ACM Transactions on Networking, 2019, 27(3): 1220-1233.

[5] Kim D, Bi J, Vasilakos A V, et al. Security of cached content in NDN[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(12): 2933-2944.

[6] Li Q, Zhang X, Zheng Q, et al. LIVE: lightweight integrity verification and content access control for named data networking[J]. IEEE Transactions on Information Forensics and Security, 2014, 10(2): 308-320.

[7] Li B, Huang D, Wang Z, et al. Attribute-based access control for ICN naming scheme[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(2): 194-206.

[8] Hamdane B, El Fatmi S G. A credential and encryption based access control solution for named data networking[C]//2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). Ottawa: IEEE, 2015: 1234-1237.

[9] Liu N, Gao S, Hou N. CDAC: a collaborative data access control scheme in named data networking[C]//2019 2nd International Conference on Hot Information-Centric Networking (HotICN). Chongqing: IEEE, 2019: 44-49.

[10] Misra S, Tourani R, Natividad F, et al. AccConF: an access control framework for leveraging in-network cached data in the ICN-enabled wireless edge[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 16(1): 5-17.

[11] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[12] Boneh D. The decision diffie-hellman problem[C]//International Algorithmic Number Theory Symposium. Springer: Heidelberg, 1998: 48-63.

[13] He J, Dawson E. Multisecret-sharing scheme based on one-way function[J]. Electronics Letters, 1995, 31(2): 93-95.

[14] Mastorakis S, Afanasyev A, Zhang L. On the evolution of ndnSIM: an open-source simulator for NDN experimentation[J]. ACM SIGCOMM Computer Communication Review, 2017, 47(3): 19-33.

[15] Free Software Foundation. The GNU multiple precision arithmetic library[EB/OL]. 2020(2020-01-17)[2020-09-30]. https://gmplib.org/.