文章编号：2095-4980(2023)12-1492-08

车联网环境下基于Cuckoo过滤器的轻量V2I认证算法

王正育[1]，徐丽燕[2]

(1.浙江农业商贸职业学院 基础教学部，浙江 绍兴 312088；2.绍兴文理学院 元培学院，浙江 绍兴 312000)

摘　要：基于假名认证机制是保护车与路边设施间通信(V2I)隐私的有效方法，传统的基于证书撤销清单(CRL)方法存在通信和计算开销大的问题。为此，提出基于布谷鸟(Cuckoo)过滤器的轻量V2I认证算法(CFLA)。CFLA算法通过局部信任中心(LTA)给其覆盖内的车辆分配假名，并利用Merkle散列树(MHT)存储车辆假名，每辆车维持一棵独立MHT。同时，采用布谷鸟过滤器(CF)数据结构，降低存储、计算和通信开销。安全性能分析表明，提出的CFLA算法能够具有防御中间攻击、重放攻击的能力。相比于相关的同类算法，CFLA算法降低了认证开销。

关键词：车联网；认证；假名；Merkle散列树；布谷鸟过滤器

中图分类号：TP393　　**文献标志码：**A　　**doi：**10.11805/TKYDA2022076

A lightweight V2I authentication algorithm based on Cuckoo Filter in VANETs

WANG Zhengyu[1]，XU Liyan[2]

(1.Department of Basic Education，Zhejiang Agricultural Business College，Shaoxing Zhejiang 312088，China；
2.College of Yuanpei，Shaoxing University，Shaoxing Zhejiang 312000，China)

Abstract：Pseudonym based authentication algorithm is an effective method to protect the privacy of Vehicle-to-Infrastructure(V2I) communication. Conventional solutions based on Certificate Revocation List(CRL) bear large overhead on communication and computation. Therefore, Lightweight V2I Authentication algorithm based on Cuckoo Filter(CFLA) is proposed in this paper. In CFLA, Local Trusted Authority(LTA) assigns a set of pseudonyms to all vehicles in its region. The Merkle Hash Tree (MHT) is employed to maintain the set of pseudonyms associated with a vehicle. In addition, CFLA algorithm leverages Cuckoo Filter(CF) to reduce the storage, computation and communication overhead associated with the CRL. Security analysis demonstrate that the proposed CFLA is robust against man-in-the-middle attacks and replay attack. Performance evaluation also shows that the proposed scheme has a significantly lower authentication overhead than other related schemes.

Keywords：Vehicular Ad Hoc Networks(VANETs)；authentication；pseudonym；Merkle Hash Tree；Cuckoo Filter

车联网(VANETs)已成为智能交通系统的重要组成部分[1]。VANETs利用车辆间的通信(Vehicle-to-Vehicle, V2V)和车辆与路边设施(V2I)通信，提高了道路行驶安全，但VANETs网络面临诸多安全问题[2]，如恶意消息插入、消息篡改、消息重放。因此，车辆用户需对所接收的消息进行认证，确保所接收消息的完整性以及消息发送方的合法性，只有被认证过的消息才能被接纳。

假名机制[3]是确保车辆用户安全和隐私的有效措施。在假名机制中，合法车辆拥有经过认证中心(Certificate Authority，CA)或信任中心(Trusted Authority，TA)颁发的多个假名，车辆利用假名参与V2V和V2I通信。为避免假名遭受连接攻击，车辆需不断地更换假名。

为保证假名机制具有条件隐私保护性能，TA依据假名追溯到车辆的真实身份，进而在发生纠纷时，TA能够裁决相应的车辆。当TA发现恶意车辆时，能够撤消这些车辆的证书和假名。证书撤消清单(Certificate

收稿日期：2022-03-29；修回日期：2022-05-09
基金项目：浙江省绍兴市科技研究资助项目(135D039)

Revocation List，CRL)[4]存储了被撤消的证书和假名，TA 周期地广播 CRL，接收车辆通过存储 CRL 和确认 CRL 信息，对其他车辆进行认证。

由于 CRL 随撤销车辆数呈线性增加，当车辆数较多时，处理 CRL 就增加了存储容量和计算开销；同时，也增加了更新 CRL 的时延。为控制 CRL 大小，研究人员提出了不同策略。文献[5]提出基于局部身份的匿名消息认证协议(Local Identity–based Anonymous message authentication Protocol，LIAP)。LIAP 采用 CRLs，利用其存储需要撤消的证书和假名车辆。此外，文献[6]和文献[7]分别提出了基于混合 D2D(Device–To–Device)的假名消息认证机制(Hybrid D2D Message Authentication，HDMA)和基于线性对认证机制。这些机制为减少 CRL，只允许恶意车辆的真实 ID 号加入 CRL；同时，也没有将消息时间戳加入消息中，使得它们不能防御重放攻击。

布谷鸟过滤器(CF)具有优良的计算性能，广泛用于 VANETs。文献[8]结合 CF 提出了基于边缘计算的消息认证机制。文献[9]利用 CF 存储并管理认证请求，降低了认证开销，但没有通过 Merkle 散列树(MHT)管理假名。文献[10]利用 CF 提出假名证书撤销机制。在这些机制中，CA 将所有撤销车辆的所有未过期的证书指纹(Fingerprints)存储于 CF 中。此外，为方便认证过程，CA 向整个网络广播 CF。相比于传统的 CRL 机制，基于 CF 的 CRL 撤销机制控制了计算开销，但这些机制将所有未过期的假名加入 CF，增加了存储和计算开销。

为此，本文提出基于 CF 的轻量 V2I 认证算法(CFLA)。CFLA 算法利用 MHT 存储车辆多个假名，且每辆车维护一棵独立 MHT。每个 LTA 拥有 2 个 CFs，用于存储车辆的 MHT 的根指纹。采用 CF 能够有效降低通信和计算开销。

1　系统模型

1.1　网络模型

网络由 TA、LTA、路边设施(Road Side Units，RSUs)和车辆四类实体构成，如图 1 所示。TA 位于网络顶层，每个 LTA 作为局部信任实体，需要向 TA 注册。LTA 负责为 RSU 以及其覆盖范围内的车辆进行注册，并为它们产生公钥和私钥对。

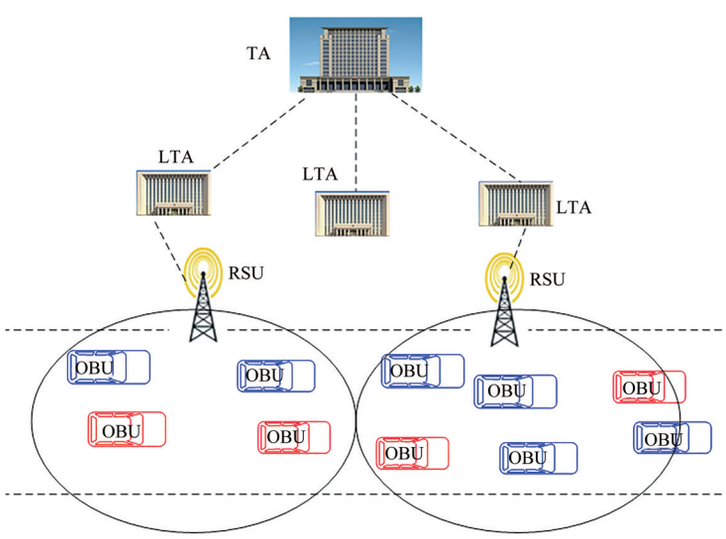

Fig.1 System model
图 1　系统模型

当一辆车利用实名在 LTA 注册后，LTA 给该车辆分配多个假名，这些假名存储于车载单元(On–Board–Unit，OBU)。车辆利用其假名通信，并周期地更换假名，避免假名遭受连接攻击。

任意车辆能够从一个 LTA 区域移动至另一个 LTA 区域，当车辆进入一个新的 LTA 区域后，从新的 LTA 区域内获取新的假名，并利用这些新的假名在该区域内通信。

每个 LTA 给其覆盖区域内的每辆车构建一个独立的 MHT[11]，MHT 的每个叶节点存储一个假名，所有非叶节点关联到其子节点的密码散列的指纹，由 8 bit 的散列构成。

此外，每个 LTA 初始拥有 2 个 CFs：积极 CF(Positive CF，PCF)和消极 CF(Negative CF，NCF)。PCF 存储有效车辆的 MHT 根指纹，NCF 存储恶意车辆的 MHT 根指纹。令 PCF_{RSU} 和 NCF_{RSU} 表示存储有效 RSU 和恶意 RSU 的 CF；PCF_V 和 NCF_V 表示存储有效车辆和恶意车辆的 CF。

1.2 布谷鸟过滤器概述

CF 是一种基于 Cuckoo 散列算法的数据结构[12]。CF 不是存储原始数据 x，而是存储数据 x 的指纹 $F(x)$，进而提升空间利用率。一个 CF 有 m 个一维的组桶，每个组桶有 n 行。每个数据 x 有 2 个候选组桶。令 B_i 和 B_j 分别表示这 2 个候选组桶，其由 2 个散列函数表示：

$$\begin{cases} B_i = H_1(x) = Hash(x) \bmod m \\ B_j = H_2(x) = \left(H_1(x) \oplus\right) Hash\left(F(x)\right) \bmod m \end{cases} \tag{1}$$

图 2 为一个 $m=8, n=4$ 的 CF 操作过程。CF 计算数据 x 的指纹 $F(x)$，利用 2 个散列函数 $(H_1(x), H_2(x))$ 计算 CF 内的候选组桶。若任意 2 个组桶都是空闲的，则将 $F(x)$ 插入空闲的组桶内。若 2 个候选的组桶都被占用，则从 CF 中随机选择 1 个组桶，并以 $F(x)$ 替换该组桶内数据 y 的指纹 $F\left(y\right)$。之后，再在 CF 中随机选择一个组桶，并将 $F\left(y\right)$ 接入该组桶。

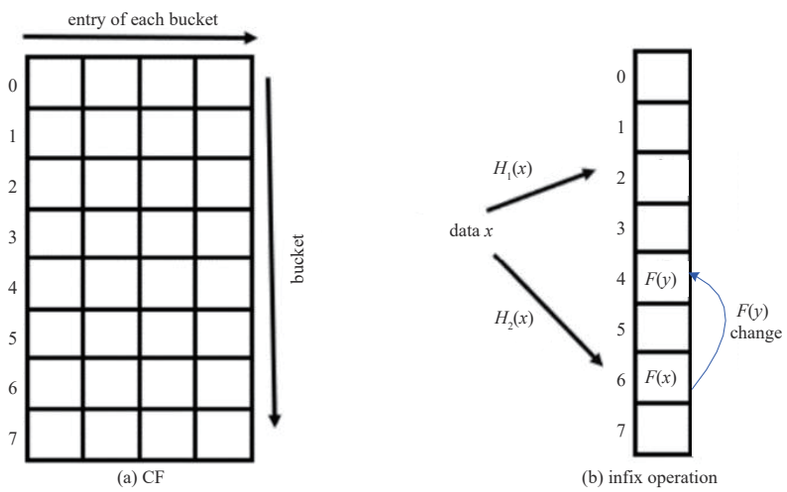

Fig.2 Operating CF
图2 CF示例

2 CFLA 算法

所有车辆需要进行 LTA 注册，获取属于自己的假名集。对于已向 LTA 注册的车辆，LTA 为每个车辆构建一个关于该车辆假名的 MHT；同时，LTA 将假名的过期日期传输给车辆。图 3 为拥有 128 个假名的 MHT，其中 MHT_{root} 表示车辆的 MHT 根；PID_{V_1} 表示车辆 V 的第一个假名，相应地，$PID_{V_{128}}$ 表示车辆 V 的第 128 个假名。

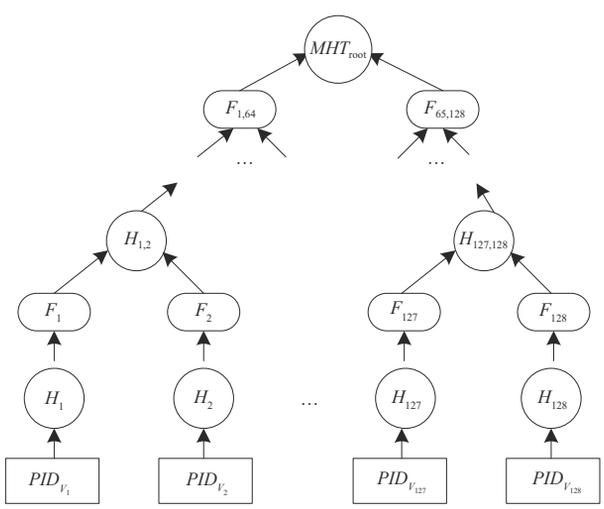

Fig.3 A sample MHT saving 128 pseudonyms
图3 存储128个假名的MHT

2.1 基于车辆认证的CF构建

为方便车辆认证，每个LTA构建PCF和NCF，在PCF和NCF中完成插入、查询和删除操作。

1) 车辆向它的归属LTA注册

LTA给每个注册的车辆产生一些假名，并构建1个MHT；同时，LTA为每个有效车辆计算其MHT_{root}的指纹$F\left(MHT_{\text{root}}\right)$，并将$F\left(MHT_{\text{root}}\right)$插入$PCF_V$。

2) $Exp_{MHT_{\text{root}}}$过期

$Exp_{MHT_{\text{root}}}$为LTA给车辆产生的假名有效期。当车辆的MHT_{root}过期，LTA从队列中将过期的MHT_{root}移除；同时，再找到$F\left(MHT_{\text{root}}\right)$，并将其在$PCF_V$和$NCF_V$中删除。

3) LTA在其覆盖范围内发现恶意车辆

当车辆发现恶意车辆时，向LTA报告恶意消息Mes_mis，其包含了发送者的假名$PID_{V_{\text{sender}}}$和恶意车辆的假名$PID_{V_{\text{malicious}}}$。LTA收到Mes_mis，先验证$PID_{V_{\text{sender}}}$的有效性。如果$PID_{V_{\text{sender}}}$有效，LTA就认定该恶意车辆是恶意车辆。随后，LTA将该恶意车辆的$F\left(MHT_{\text{root}}\right)$插入$NCF_V$中。

4) 车辆离开原注册的LTA区域

当车辆准备离开一个LTA区域，则向该LTA区域发送离开消息Mes_mov，其包含车辆当前使用的假名以及此存储该假名的MHT_{root}和查询$F\left(MHT_{\text{root}}\right)$的索引号$B_{\text{ndx}}$。当LTA收到Mes_mov，验证该车辆的身份。如果验证通过，将$F\left(MHT_{\text{root}}\right)$从$PCF_V$中删除。

5) 车辆进入新的LTA区域

当车辆进入新的LTA区域，需向此LTA请求新的假名。车辆向LTA发送请求假名消息Mes_req，其包含请求车辆的假名PID_V以及存储假名的MHT_{root}和车辆旧的LTA的ID号。收到Mes_req消息后，新的LTA与旧的LTA进行通信，验证车辆的身份。旧的LTA在CF中查询假名证书，如果车辆身份真实，新的LTA就给该车辆分配新的假名，并为此车辆构建存储假名的MHT；同时，将$F\left(MHT_{\text{root}}\right)$插入到$PCF_V$。

2.2 基于RSU认证的CF构建

除了给车辆构建CF外，LTA还给RSU构建CF，为后续对RSU认证提供基础。与2.1节类似，LTA为其覆盖范围内的RSUs构建PCF_{RSU}。若某一个RSU存在恶意行为，LTA就将该RSU的公钥的指纹从PCF_{RSU}中删除。随后，将该RSU公钥的指纹插入NCF_{RSU}。

2.3 基于CF的V2I的相互认证

在CFLA算法中，LTA给合法车辆构建PCF，并利用PCF存储$F\left(MHT_{\text{root}}\right)$；同时，LTA给恶意车辆构建NCF，并将NCF存在车辆的$F\left(MHT_{\text{root}}\right)$。类似地，LTA也为合法RSU和恶意RSU分别构建了PCF和NCF。

为了能够完成V2I的相互认证，LTA对PCF_{RSU}、NCF_{RSU}和PCF_V、NCF_V进行签名，并周期广播这2个CF的消息Mes_CF。令$Sig_{\text{LTA}}\left(PCF_V,NCF_V\right)$、$Sig_{\text{LTA}}\left(PCF_{RSU},NCF_{RSU}\right)$分别表示LTA对车辆的CF和RSU的CF签名。车辆和RSUs利用收到的Mes_CF消息完成V2I通信阶段认证。

CFLA算法中，RSU周期广播beacon消息，其包含ID_{RSU_i}、PU_{RSU_i}和消息时间戳t_s。其中ID_{RSU_i}表示第i个RSU的ID；PU_{RSU_i}表示第i个RSU的公钥。收到beacon消息，车辆V_i首先确认beacon消息是否过期。如果过期，直接丢弃；否则，车辆V_i计算PU_{RSU_i}，并验证PU_{RSU_i}的有效性。

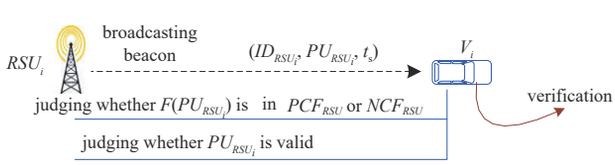

Fig.4 Process of RSU authentication by vehicle

图4 车辆验证RSU流程

验证过程如图4所示。车辆V_i首先在PCF_{RSU}和NCF_{RSU}内查询是否存储了$F\left(PU_{RSU_i}\right)$。若PCF_{RSU}内有$F\left(PU_{RSU_i}\right)$，则进一步判断$F\left(PU_{RSU_i}\right)$是否也在NCF_{RSU}内。若$F\left(PU_{RSU_i}\right)\notin NCF_{RSU}$，车辆$V_i$认为$PU_{RSU_i}$有效；若

$F\left(PU_{RSU_i}\right) \in NCF_{RSU}$，车辆 V_i 需求助于 LTA，向其发送消息。**Algorithm 1** 给出验证过程。

Algorithm 1: V_i authenticates PU_{RSU_i}

RSU periodically broadcasts beacon message(ID_{RSU_i}, PU_{RSU_i}, t_s)

Upon receiving the beacon message V_i verifies PU_{RSU_i} as follows

```
Checks the freshness of received message using t_s;
if t_s is valid then
    Looks up into the positive CF PCF_RSU and negative CF NCF_RSU for F(PU_RSU_i);
    if F(PU_RSU_i) ∈ PCF_RSU then
        if F(PU_RSU_i) ∉ NCF_RSU then
            PU_RSU_i is considered valid;
        else
            PU_RSU_i sends message to LTA for verification;
        end if
    end if
    if F(PU_RSU_i) ∉ PCF_RSU then
        if F(PU_RSU_i) ∈ NCF_RSU then
            PU_RSU_i is considered malicious;
        else
            V_i waits for updated CFs from LTA;
        end if
    end if
else
    Drops the beacon message;
end if
```

若 $F\left(PU_{RSU_i}\right)$ 不在 PCF_{RSU} 内，进一步判断 $F\left(PU_{RSU_i}\right)$ 是否在 NCF_{RSU} 内。如果 $F\left(PU_{RSU_i}\right) \in NCF_{RSU}$，认为 PU_{RSU_i} 无效；否则，车辆 V_i 等待从 LTA 中更新 CFs。

当 RSU_i 通过车辆 V_i 验证后，车辆 V_i 向 RSU_i 发送验证通过消息 Mes_aut。之后，RSU_i 对车辆 V_i 进行验证。消息 Mes_aut 包含车辆 V_i 的假名 PID_{V_i}、指纹追踪值 MFV、PCF_V 的组桶索引号 B_{ndx}、RSU_i 的 ID 和消息时间戳。RSU_i 利用 MFV 可计算车辆假名的 MHT_{root}。

为保证消息 Mes_aut 的安全性，车辆 V_i 在向 RSU_i 传输消息 Mes_aut 前，用 RSU_i 的公钥对其进行加密。因此，当 RSU_i 收到此消息后，利用自己的私钥对其解密，进而提取消息内容。

RSU_i 首先验证消息 Mes_aut 的时效性。若此消息未过期，RSU_i 依据 MFV 和 PID_{V_i} 计算车辆 V_i 对应的 MHT_{root}。随后，RSU_i 判断 MHT_{root} 的指纹 $F\left(MHT_{root}\right)$，并依据组桶索引号 B_{ndx}，确认 $F\left(MHT_{root}\right)$ 是否在相应的 PCF_V 和 NCF_V 中。验证过程如 **Algorithm 2** 所示。

Algorithm 2: Authentication of V_i by RSU_i

V_i sends $E((PID_{V_i}, MFV_s, B_{ndx}, PU_{V_i}, ID_{RSU_i}, t_s), PU_{RSU_i})$ to RSU_i

Upon receiving the above message RSU_i verifies V_i as follows

```
Decrypts the message using private key PR_RSU_i;
Checks the freshness of received message using t_s;
if t_s is valid then
    Calculates the MHT_root value using MFV_s and PID_Vi;
    Looks up into the PCF_V with B_ndx and NCF_V for F(MHT_root) corresponding to V_i ;
    if F(MHT_root)∈PCF_V with B_ndx then
        if F(MHT_root)∉NCF_V then;
```

V_i is considered valid;
else
RSU_i sends message to LTA for verification;
end if
end if
if $F\left(MHT_{\text{root}}\right) \notin PCF_V$ with B_{ndx} **then**
if $F\left(MHT_{\text{root}}\right) \in NCF_V$ **then**
V_i is considered malicious;
else
RSU_i waits for updated CFs from LTA;
end if
end if
else
Drops the received message;
end if

若 $F\left(MHT_{\text{root}}\right)$ 在 PCF_V 中，进一步判断 $F\left(MHT_{\text{root}}\right)$ 是否在 NCF_V。若 $F\left(MHT_{\text{root}}\right)$ 不在 NCF_V，则认为车辆 V_i 有效；若 $F\left(MHT_{\text{root}}\right)$ 在 NCF_V，则求助 LTA，并向 LTA 发送求助消息。

若 $F\left(MHT_{\text{root}}\right)$ 不在 PCF_V 中，进一步判断 $F\left(MHT_{\text{root}}\right)$ 是否在 NCF_V。若 $F\left(MHT_{\text{root}}\right)$ 在 NCF_V，则认为车辆 V_i 无效；若 $F\left(MHT_{\text{root}}\right)$ 不在 NCF_V，就等待 LTA 对 CFs 的更新。

3　性能分析

3.1 安全性能分析

在 CFLA 算法中，车辆和 RSU 在通信前均利用 CF 进行认证。只有验证通过，才能进行通信，提升了通信安全。此外，CFLA 算法在通信过程进行了身份匿名。因此，即使所有 RSUs 全部被攻击，也无法窃取车辆真实 ID 信息。

此外，CFLA 算法具有防御消息篡改攻击的能力。对于接收的 beacon 消息，车辆先验证 RSU 的公钥。车辆利用车辆的公钥加密消息，再将加密后的消息传输至 RSU。只有预期的 RSU 才能解密消息，防御消息被篡改；同时，CFLA 算法也能够防御重放攻击。不论车辆还是 RSU，其发送的消息均附加上时间戳。一旦接收了消息，接收者首先验证消息在时间上的有效性，有效地防御重放攻击。

3.2 算法的复杂度

在 Windows 7 操作系统、8 GB 内存，core i7 CPU 的 PC 上分析 CFLA 算法的复杂度。

首先，验证 V2I 间通信的认证开销。令 $T_{\text{RSA\_E}}$ 表示执行 RSA−1 048 bit 的加密操作所消耗的时间[13]；$T_{\text{RSA\_D}}$ 表示执行 RSA−1 048 bit 的解密操作所消耗的时间；$T_{\text{RSA\_V}}$ 表示执行 RSA−1 048 bit 验证操作所消耗的时间；H 表示执行 SHA−256 散列操作所消耗的时间[14]；T_{MUL} 表示执行点乘操作所消耗的时间；T_{MTP} 表示执行 Map−To−Point 散列操作所消耗的时间；T_{PAR} 表示执行双线性对操作所消耗的时间。表 1 给出 CFLA、LIAP、HDMA 算法和基于 RSU 的有效认证(New and Efficient RSU based Authentication，NERA)算法完成认证的开销。

表1 CFLA、LIAP、HDMA 和 NERA 算法的认证开销

Table1 Authentication overheads

algorithm	vehicle end	RSU end
LIAP	$T_{\text{MUL}}+T_{\text{MTP}}+3T_{\text{PAR}}$	$T_{\text{MUL}}+T_{\text{MTP}}+3T_{\text{PAR}}$
HDMA	$T_{\text{RSA\_V}}+T_{\text{RSA\_D}}$	$T_{\text{RSA\_V}}+T_{\text{RSA\_D}}+T_{\text{RSA\_E}}$
NERA	$T_{\text{MUL}}+T_{\text{MTP}}+3T_{\text{PAR}}$	$T_{\text{MUL}}+T_{\text{MTP}}+3T_{\text{PAR}}$
CFLA	$T_{\text{RSA\_E}}$	$(\log n+1)H+T_{\text{RSA\_D}}$

在 CFLA 算法中，车辆先在 PCF_{RSU} 和 NCF_{RSU} 中查询，进而验证 RSU 的公钥。随后，车辆向 RSU 发送消息，RSU 再对车辆进行验证。即车辆和 RSU 通过验证 CRLs，实现相互认证。因此，在相互认证过程中，车辆端产生的开销为 $T_{\text{RSA\_E}}$；RSU 端产生的开销为 $\left(\log n+1\right)H+T_{\text{RSA\_D}}$，其中 n 表示给一辆车分配的假名数。相比于 LIAP、

HDMA 和 NERA 算法，CFLA 算法降低了认证过程中的开销。

图 5 和图 6 分别为车辆端和 RSU 端认证所消耗的时间，其中 $T_{MUL}=0.39$ ms、$T_{MTP}=0.09$ ms、$T_{PAR}=3.21$ ms、$T_{RSA\_E}=0.08$ ms、$H=111$ μs、$T_{RSA\_D}=0.08$ ms、$T_{RSA\_V}=0.07$ ms。图 5 为 RSU 认证车辆所消耗的时间，从图 5 可知，RSU 认证车辆所消耗的时间随车辆数呈线性增加。LIAP 算法和 NERA 算法中 RSU 认证车辆所消耗的时间远多于 HDMA 算法和 CFLA 算法，其中 CFLA 算法中 RSU 认证车辆所消耗的时间最少。

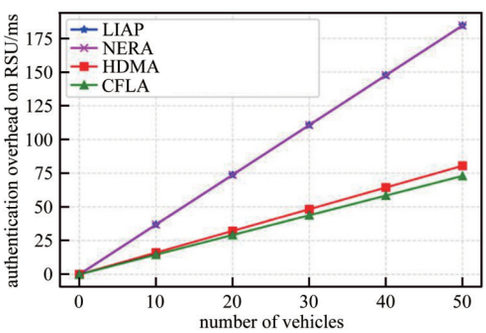

Fig.5 Time consumption for RSU certificating vehicle
图 5 RSU 认证车辆所消耗的时间

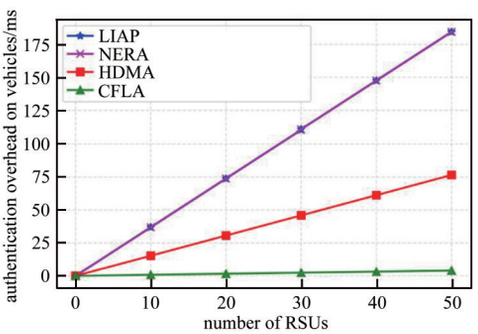

Fig.6 Time consumption for vehicle certificating RSU
图 6 车辆认证 RSU 所消耗的时间

图 6 为车辆认证 RSU 所消耗的时间，从图 6 可知，相比于 LIAP、HDMA 和 NERA 算法，CFLA 算法中车辆认证 RSU 所消耗的时间最少。如，当 RSU 数达到 30，CFLA 算法中车辆认证 RSU 所消耗的时间只有 2.4 ms，而 LIAP、NERA 和 HDMA 算法的时间分别达到 115 ms、115 ms 和 45 ms。

4 结论

为减少认证开销，本文提出了轻量的 V2I 认证算法 CFLA。CFLA 算法通过引入 CFs 降低了存储、通信和计算开销。相比基于 CRL 的认证机制，CFLA 算法降低了认证开销。安全性能分析表明，CFLA 算法满足安全要求。本文仅讨论了 V2I 认证，为提高整个 VANETs 的通信安全性，后期工作的研究重点为 V2V 认证。

参考文献：

[1] 姚行洲,赵红梅,李恒广. 车联网中基于动态传输距离的多跳稳定路由[J]. 太赫兹科学与电子信息学报, 2020,18(4):620-624. (YAO Xingzhou,ZHAO Hongmei,LI Hengguang. Dynamic transmission range-based multi-hop stable routing in vehicular Ad-hoc networks[J]. Journal of Terahertz Science and Electronic Information Technology, 2020,18(4):620-624.)

[2] 安涛,马文平,刘小雪. VANET 中基于 SM9 密码算法的聚合签名方案[J]. 计算机应用与软件, 2020,37(12):280-284. (AN Tao, MA Wenping, LIU Xiaoxue. Aggregate signature scheme based on SM9 cryptographic algorithm in VANET[J]. Computer Applications and Software, 2020,37(12):280-284.)

[3] 张文波,黄文华,冯景瑜. 基于无证书签密的车联社会网络安全通信机制[J]. 通信学报, 2021,42(7):128-136. (ZHANG Wenbo, HUANG Wenhua, FENG Jingyu. Secure communication mechanism for VSN based on certificateless signcryption[J]. Journal on Communications, 2021,42(7):128-136.)

[4] 王青龙,乔瑞,樊娜,等. 一种面向车联网的高效条件匿名认证方案[J]. 北京交通大学学报, 2019,43(5):80-86. (WANG Qinglong,QIAO Rui,FAN Na,et al. An efficient conditional anonymity authentication scheme for VANETs[J]. Journal of Beijing Jiaotong University, 2019,43(5):80-86.)

[5] WANG Shibin, YAO Nianmin. LIAP: a local identity-based anonymous message authentication protocol in VANETs[J]. Computer Communications, 2017,112(6):154-164.

[6] WANG Peng, CHEN C M, KUMARI S, et al. HDMA: hybrid D2D message authentication scheme for 5G-enabled VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2021,21(8):5071-5080.

[7] BAYAT M, POURNAGHI M, RAHIMI M, et al. NERA: a new and efficient RSU based authentication scheme for VANETs[J]. Wireless Networks, 2020,26(5):3083-3098.

[8] CUI Jie, WEI Lu, ZHANG Jing, et al. An efficient message authentication scheme based on edge computing for vehicular Ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2019,20(5):1621-1632.

（下转第 1506 页）