5G-V2X 中基于轨迹预测的安全高效群组切换认证协议

张应辉[1,2]，钱佳乐[1,2]，曹进[3]，郑东[1,2]

（1. 西安邮电大学网络空间安全学院，陕西 西安 710121；
2. 西安邮电大学无线网络安全技术国家工程研究中心，陕西 西安 710121；
3. 西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘 要：针对 5G-V2X 场景中大量车辆执行切换认证的效率问题，提出了一种基于轨迹预测的安全高效群组切换认证协议。首先，通过预测车辆轨迹，提前完成密钥协商协议。其次，通过用户分组算法将具有移动相关性的车辆视为同一群组，再采用无证书聚合签名技术批量验证群组内所有车辆。再次，针对聚合签名技术易遭受拒绝服务攻击的弊端，采用二分查找法快速定位恶意用户，提高群组切换认证协议的效率。最后，利用形式化验证工具 Scyther 对所提协议进行了安全性分析，与现有最优协议相比，所提协议的计算效率提高了 30%。

关键词：5G-V2X；群组切换认证；用户分组；无证书聚合签名；Scyther

中图分类号：TN918

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023136

Secure and efficient group handover authentication protocol based on trajectory prediction in 5G-V2X

ZHANG Yinghui[1,2], QIAN Jiale[1,2], CAO Jin[3], ZHENG Dong[1,2]

1. School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
2. National Engineering Research Center for Secured Wireless, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
3. School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract: Aiming at the efficiency issue of handover authentication for a large number of vehicles in the 5G-V2X scenario, a secure and efficient group handover authentication protocol based on trajectory prediction was proposed. Firstly, the effect of completing key agreement protocol in advance was achieved by predicting vehicle trajectories. Secondly, vehicles with mobility relevance were treated as the same group through user grouping algorithms, and then all vehicles within the group were batch verified using certificateless aggregation signature technology. In addition, to address the vulnerability of aggregated signature technology to DoS attacks, a binary search method was used to quickly locate malicious users and improve the efficiency of group handover authentication protocol. Finally, the security analysis of the protocol was conducted using the formal verification tool Scyther, and compared with the existing optimal protocol, the computational efficiency is improved by 30%.

Keywords: 5G-V2X, group handover authentication, user grouping, certificateless aggregation signature, Scyther

---

收稿日期：2023−05−09；**修回日期：**2023−07−16

基金项目：国家自然科学基金资助项目（No.62072369, No.62072371）；陕西高校青年创新团队基金资助项目；陕西省特支计划青年拔尖人才支持计划基金资助项目；陕西省重点研发计划基金资助项目（No.2021ZDLGY06-02, No.2020ZDLGY08-04）；陕西省技术创新引导计划基金资助项目（No.2023-YD-CGZH-31）

Foundation Items: The National Natural Science Foundation of China (No.62072369, No.62072371), The Youth Innovation Team of Shaanxi Universities Foundation, The Shaanxi Special Support Program Youth Top-notch Talent Program, The Key Research and Development Program of Shaanxi (No.2021ZDLGY06-02, No.2020ZDLGY08-04), The Technology Innovation Leading Program of Shaanxi (No.2023-YD-CGZH-31)

0　引言

近年来，随着智能汽车领域的发展，人们对汽车的需求量日益增长，车用无线通信技术 V2X（vehicle-to-everything）受到工业界和学术界的广泛关注[1]。V2X 泛指车辆使用邻近服务实现和其他任意网络、任意个体间的通信，包含车辆到车辆（V2V, vehicle-to-vehicle）、车辆到行人（V2P, vehicle-to-pedestrian）、车辆到路边基础设施（V2I, vehicle-to-infrastructure）等多种通信形式[2]，可为许多新的应用场景提供支持，如车辆自动驾驶、公路安全系统、交通信息管理等[3-8]。V2X 融合了车辆和基站之间的蜂窝通信以及车辆之间的直接通信，2 种模式相互补充，实现基站和车辆之间的负载均衡[9]。为充分利用蜂窝移动通信网络的技术优势，基于蜂窝网络的车用无线通信技术（C-V2X, celluar vehicle-to-everything）应运而生。C-V2X 是由 3GPP 定义的 V2X 技术，包含基于长期演进（LTE, long term evolution）以及 5G 的 V2X 系统，是专用短程通信（DSRC, dedicated short range communication）技术的有力补充[10]。

随着 5G 大规模车辆连接和车辆数量的快速增长，当大量车辆在短时间内从源基站（s-gNB, source-generation nodeB）移动到目标基站（t-gNB, target-generation nodeB）范围内时，所有车辆会同时向 t-gNB 发起切换认证请求，这可能会造成严重的信号超载和网络拥堵。所以，将大量车辆分成不同群组进行监控管理已被视为一种道路交通管理策略[11]。例如，文献[12]提出了一种资源分配策略，以支持多车道队列系统中更大的队列规模。但是，目前的协议标准关于群组切换认证协议执行效率的讨论尚有不足之处。一方面，5G 的部署会引起互联网主干流量增加，端到端时延中传播时延所占比例增大[13]。另一方面，5G 基站分为宏基站和小基站，其中，宏基站体型大、覆盖面积广，主要用于室外覆盖；小基站发射功率较小，根据覆盖范围大小可分为微基站、皮基站和飞基站。因此，5G 网络环境下不同大小的基站覆盖范围相互交错，可能会导致更加频繁的切换认证。此外，目前的标准在保护用户隐私方面也有不足。文献[14-16]研究表明，在切换认证过程中仍存在着许多安全问题，包括缺乏相互认证、密钥确认、完美前/后向安全（PFS/PBS, perfect forward/backward secrecy）、易遭受拒绝服务（DoS, denial of service）攻击等。

虽然目前关于无线网络中大量车辆的切换认证协议的研究工作非常多，但是，在无线网络中的车辆接入认证的过程中，车辆的真实身份会以明文的形式发送到无线网络，这可能导致车辆的身份被伪造基站或被动攻击者获取，造成车辆隐私泄露和后续的切换认证过程失败，对车辆行驶安全造成威胁。在 5G 网络的车辆接入认证协议过程中，车辆的真实身份会以密文的形式发送到 5G 核心网络，不仅保证了车辆隐私安全和后续的切换认证过程安全，而且由于 5G 的低时延、高速率、高带宽等特点，也提高了 5G-V2X 场景下大量车辆执行切换认证协议的效率，保障车辆行驶安全。但是，到目前为止，关于 5G-V2X 场景下车辆群组切换认证协议的研究很少。此外，现有的研究工作在安全性和效率方面也存在缺陷。文献[12]提出了一种针对 5G 网络中车辆队列的认证和再认证协议，由于它只使用了简单的密码操作，计算开销不高。但是，因为消息的长度与群组内车辆数目的平方成正比，该协议具有较高的通信成本。此外，该协议并不能保护车辆的隐私。文献[17]提出了一种 5G-V2X 网络的群组认证切换协议，该协议采用聚合消息验证码（AMAC, aggregated message authentication code）技术降低了信令开销。但是，该协议在切换认证过程中需要进行多次点乘运算，非常耗时。此外，该协议不能保护车辆的隐私，因为车辆的真实身份通过不安全的信道以明文的形式传输给车辆群组的组长，其中，在不同车辆群组内负责接收来自基站的消息，以及接收群组内其他车辆的消息再转发给基站的车辆，称为该车辆群组的组长，表示为 V_1；群组内其他车辆称为组员，表示为 $V_i(i=2,3,\cdots,n)$。此外，该协议易受到 DoS 攻击，因为只有当所有组员都合法时，AMAC 才能被成功验证，攻击者可以向组长发送错误的消息验证码，使整个群组验证失败。这个问题发生在所有采用聚合技术的协议中，当然，对于本文所采用的聚合技术也存在此问题，但本文提出了应对策略。对于文献[18]，主移动中继节点（MRN, mobile relay node）首先执行切换认证程序，然后一般的 MRN 才开始执行切换认证程序，这将导致切换时间延长。

文献[19]中提出了 2 种用于 5G 高速铁路网络的群组切换认证协议。第一种协议是轻量级的群组切换认证协议，它可以满足大部分安全属性，并且只

消耗少量的信令和计算开销。第二种协议是安全性增强的群组切换认证协议，它可以实现相互认证、密钥协商、PFS/PBS、匿名性、不可链接性以及抵抗多种协议攻击。但是，这 2 种协议都只适用于固定轨迹移动。此外，由于分别采用了聚合消息验证码和聚合签名技术，且没有提出解决聚合技术易遭受攻击者破坏聚合验证的方法，这 2 种协议都易遭受 DoS 攻击。文献[20]提出了一种无证书、安全高效的车辆群组切换认证协议，同文献[18]的问题一样，该协议在大量车辆同时到达目标基站范围内时，到达的第一辆车先进行切换认证，其余车辆在第一辆车的协助下执行切换认证协议，这也将导致切换时间延长。

针对 5G-V2X 场景下，大量车辆在密集部署的 5G 小基站网络范围内频繁进行切换认证时所面临的效率和隐私问题，本文主要做出了以下贡献。

1) 提出了 5G-V2X 场景下的基于轨迹预测的安全高效的群组切换认证协议，根据车辆群组的移动信息对车辆轨迹进行预测，提前完成密钥协商协议。

2) 源基站根据用户分组算法[21]先将范围内的大量车辆分为不同临时组。然后，结合车辆与源基站和周围基站的信干噪比（SINR, signal to interference plus noise ratio）等信息将临时组内具有移动相关性的不同车辆视为一个群组。最后，执行群组切换认证协议。

3) 在验证车辆群组时，采用无证书聚合签名技术[22]批量验证群组内所有车辆，减少了证书管理和认证开销。为了保证无证书聚合签名的有效性，对于车辆群组内出现的恶意用户，采用二分查找法快速定位恶意用户产生的无效签名，提高群组切换认证效率。

4) 在安全分析方面，先通过 Scyther 进行形式化安全分析，然后进一步采用非形式化安全分析。

5) 在效率方面，通过图表分析比对，与现有最优协议相比，本文协议的计算效率提高了 30%。

1 系统模型与攻击模型

1.1 系统模型

如图 1 所示，5G 核心网络的系统架构包括多种功能，如接入和移动管理功能（AMF, access and mobility management function）、认证服务器功能（AUSF, authentication server function）、会话管理功能（SMF, session management function）、策略控制功能（PCF, policy control function）和统一数据管理（UDM, unified data management）功能、认证凭证存储和处理功能（ARPF, authentication credential repository and processing function）等。在 5G 核心网络中，每个网络功能（NF, network function）使用基于服务的接口进行交互（如 Npcf、Nsmf、Nudm、Naprf 等）。NF 通过这些应用程序接口（API, application programming interface）向其他 NF 提供一项或多项服务，其中，API 可用于交互应用层信息和配置参数，包括对车辆 V_i 和 V2X 通信有用的应用层信息和配置参数。N2 接口是 AMF 和基站之间的通信接口，Uu 接口是终端和基站之间的蜂窝网通信接口，PC5 是终端与终端之间的直接通信接口。PCF 为车辆 V_i 提供基于 PC5 接口和 Uu 接口的用于 V2X 通信的授权和策略参数，也为 AMF 提供车辆 V_i 的必要参数，用于配合和管理 V2X 通信[23]。在切换认证期间，由 AMF 负责车辆 V_i 的切换认证和密钥管理。

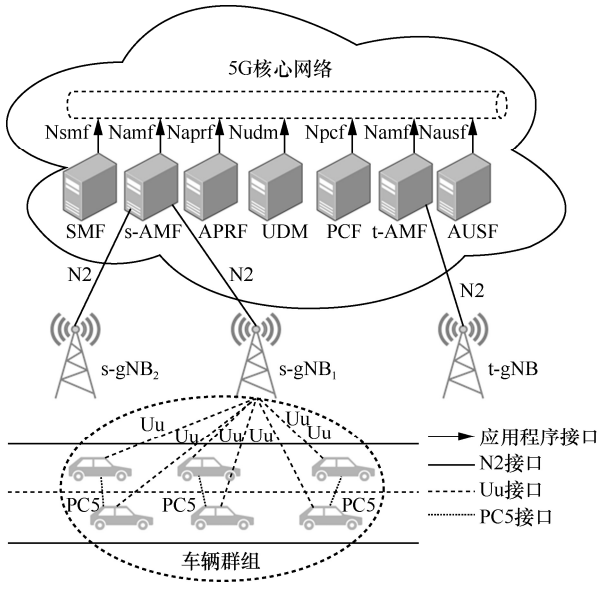


图 1 5G-V2X 场景下的系统模型

3GPP R16 标准下的 V2X 通信仅支持一对用户设备（UE, user equipment）之间进行直接通信的单播传输。3GPP R17 标准[24]正在进行一个新的研究项目，以讨论在 5G-V2X 中对广播和组播传输的支持。其中，广播是单个 UE 向无线电传输范围内的所有 UE 发送消息，所有 UE 可以对该消息进行解码；组播是单个 UE 向一组满足特定条件（如作为一个组的成员）的 UE 发送消息[25]。在切换认证期

间，组长V_1向组员V_i组播消息，组员V_i向组长V_1单播消息。

在切换认证期间，AMF 可以根据车辆群组的移动信息预测车辆轨迹，判断车辆群组将要进入的下一个目标基站位置，并选择执行不同的群组切换认证程序。若在同一 AMF 中切换，则执行 AMF 域内切换程序，在图 1 中表示为从 s-AMF 内的基站 s-gNB$_1$ 切换到 s-AMF 内的基站 s-gNB$_2$；若在不同 AMF 之间切换，则执行 AMF 域间切换程序，在图 1 中表示为从 s-AMF 内的源基站 s-gNB$_1$ 切换到 t-AMF 内的目标基站 t-gNB。本文将讨论车辆群组在以上 2 种切换场景下的协议流程。其中，协议共涉及 3 个实体，即车辆V_i、基站 gNB 和 AMF。

1.2　攻击模型

本文中的网络攻击模型为 Dolev-Yao 模型，该模型通常用于呈现各种无线网络的安全漏洞，模型的攻击者可以监听、拦截、分析和操纵无线信道上传输的信息。本文假设 5G 核心网络和基站之间的连接是安全的，因为核心网络和基站通常采用光纤等固定线路连接。同时，假设车辆和基站之间的连接不安全，因为基站通常被放置在远离核心网络的地方，而且保护措施有限。此外，假设 5G 核心网络中包括 AMF 在内的所有网络功能都是可信的，无线接入网中的实体车辆和基站是不可信的。

2　协议设计

本节将详细介绍在 5G-V2X 场景中，车辆群组在不同切换场景下进行群组切换认证的协议流程，本文协议 TPGHA 共包括 3 个阶段：1) 初始认证；2) 群组切换准备；3) 群组切换认证。表 1 列出了本文协议中用到的部分符号含义。

2.1　初始认证

在本阶段，所有车辆$V_i\left(i=1,2,\cdots,n\right)$、AUSF 和 ARPF 都将执行 3GPP TS33.501 R16 标准[26]的 5G 身份认证与密钥协商（5G-AKA, 5G authentication and key agreement）协议。首先，SEAF 由 5G-AKA 协议得到的密钥K_{SEAF}派生出密钥$K_{\text{s-AMF}}$，并发送给 s-AMF。然后，车辆V_i和 s-AMF 由密钥$K_{\text{s-AMF-}i}$得到NH_i值和密钥$K_{\text{s-gNB}_{1\text{-}i}}$，密钥$K_{\text{s-gNB}_{1\text{-}i}}$有一个相对应的$\text{NH}_i$链路计数器值$\text{NCC}_i$，其中，$\text{NH}_i$和$\text{NCC}_i$都用于派生出新会话密钥$K_{\text{gNB-}i}$。

表 1　　**符号含义**

符号	含义
λ	系统主密钥
$K_{\text{SEAF-}i}$	车辆V_i访问 SEAF 的对称密钥
$K_{\text{AMF-}i}$	车辆V_i访问 AMF 的对称密钥
$K_{\text{gNB-}i}$	车辆V_i与基站 gNB 的会话密钥
SUPI_i	车辆V_i的永久身份标识符
SUCI_i	车辆V_i的SUPI_i经加密后的身份标识符
TID_i	车辆V_i的临时身份标识符
NH_i	车辆V_i的下一跳参数值
NCC_i	车辆V_i的NH_i链路计数器
GID	车辆群组的标识符
ID_{gNB}	基站 gNB 的身份标识符
PCI_{gNB}	基站 gNB 的物理单元标识符
$\text{ARFCN-DL}_{\text{gNB}}$	基站 gNB 的下行链路的绝对射频信道号
Sig_m	m 的签名
$\{x\}_K$	用对称密钥 K 加密 x
MAC	消息验证码
t	时间戳

初始认证后，s-gNB$_1$根据用户分组算法将同一时间点内处于 s-gNB$_1$ 范围内的车辆视为一个临时组。然后，系统执行无证书聚合签名技术的初始化，具体步骤如下。

步骤 1　s-AMF 首先选择q阶循环加法群G_1，P为其生成元，和q阶循环乘法群G_2，形成双线性映射$e:G_1\times G_1\to G_2$。然后，s-AMF 选取系统主密钥$\lambda\in Z_q^*$，生成系统公钥$P_T=\lambda P$，再选取哈希函数$H_{1\sim4}:\{0,1\}^*\to Z_q^*$，$H_5:\{0,1\}^*\to Z_q^*$。接着，s-AMF 为车辆$V_i$生成用于聚合签名的部分私钥$(D_{i,0},D_{i,1})=(\lambda Q_{i,0},\lambda Q_{i,1})$，其中，$Q_{i,0}=H_1(\text{SUCI}_i,0)$，$Q_{i,1}=H_1(\text{SUCI}_i,1)$。再为 s-AMF 域内的所有基站 gNB 生成部分私钥$(D_{\text{gNB},0},D_{\text{gNB},1})=(\lambda Q_{\text{gNB},0},\lambda Q_{\text{gNB},1})$，其中，$Q_{\text{gNB},0}=H_1(\text{ID}_{\text{gNB}},0)$，$Q_{\text{gNB},1}=H_1(\text{ID}_{\text{gNB}},1)$。然后，s-AMF 通过安全信道发送$(D_{i,0},D_{i,1})$给车辆$V_i$，并发送$(D_{\text{gNB},0},D_{\text{gNB},1})$给基站 gNB。最后，s-AMF 公布系统参数列表$\text{params}=\{G_1,G_2,e,P,P_T,H_{1\sim5}\}$。

步骤 2　车辆V_i选择随机数$x_i\in Z_q^*$作为自己的私钥，计算并公布公钥$P_i=x_iP$。

步骤 3 gNB 选择随机数 $x_{\text{gNB}} \in Z_q^*$ 作为自己的私钥，计算并公布公钥 $P_{\text{gNB}} = x_{\text{gNB}} P$。

2.2 群组切换准备

本阶段发生在下一次群组切换认证之前，流程如图 2 所示，各步骤详细描述如下。

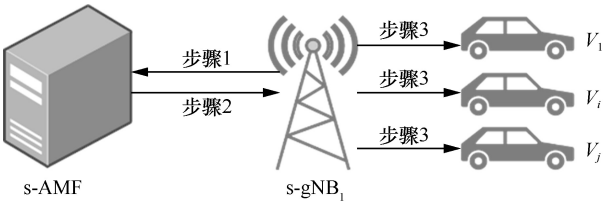


图 2 群组切换准备

步骤 1 s-gNB$_1$ 通过用户分组算法结合源基站和周围基站的 SINR、车辆的移动方向和车辆与当前基站以及周围基站的距离，判断车辆临时组内两两车辆之间是否具有移动相关性，将具有移动相关性的不同车辆视为一个群组。然后，s-gNB$_1$ 发送同一群组内车辆的 TID_i 和群组切换准备请求到 s-AMF，其中，TID_i 在初始认证或群组切换认证结束后根据式(1)计算得出。

$$\text{TID}_i = H(\text{SUCI}_i \| \text{NH}_i \| K_{\text{s-AMF-}i}) \tag{1}$$

步骤 2 s-AMF 接收到来自 s-gNB$_1$ 的 TID_i 和群组切换准备请求消息后，根据式(2)～式(5)计算出 GID_1、GID、MAC_1 和 MAC_i，然后通过安全信道发送 $\{\text{TID}_i, \text{GID}_1, \text{GID}, \text{MAC}_1, \text{MAC}_i, \{\text{NCC}_i, t_1\}_{K_{\text{s-AMF-}i}}\}$ 到 s-gNB$_1$，其中，t_1 为 s-AMF 新生成的时间戳，用于抵抗重放攻击。

$$\text{GID}_1 = H\left(\sum_{i=2}^{n} H(\text{TID}_i)\right) \tag{2}$$

$$\text{GID} = H(\text{GID}_1 \oplus H(\text{TID}_1)) \tag{3}$$

$$\text{MAC}_1 = H(\text{GID}_1 \| \text{NCC}_1 \| K_{\text{s-AMF-1}} \| t_1) \tag{4}$$

$$\text{MAC}_i = H(\text{GID} \| \text{NCC}_i \| K_{\text{s-AMF-}i} \| t_1) \tag{5}$$

步骤 3 s-gNB$_1$ 接收到请求响应后，对群组内的不同车辆发送不同消息。①对组长 V_1 发送消息 $\{\text{GID}_1, \text{MAC}_1, \{\text{NCC}_1, t_1\}_{K_{\text{s-AMF-1}}}\}$。$V_1$ 接收到 s-gNB$_1$ 的消息后，首先，由初始认证阶段获得的密钥 $K_{\text{s-AMF-1}}$ 检验时间戳 t_1 的新鲜性，然后根据式(4)检验 NCC_1 和 GID_1 的完整性和有效性。②对组员 V_i（$i = 2,3,\cdots,n$）发送消息 $\{\text{GID}, \text{MAC}_i, \{\text{NCC}_i, t_1\}_{K_{\text{s-AMF-}i}}\}$，然后和组长 V_1 一样检验消息。③对于刚执行过初始认证并被划分到群组内的车辆 $V_j (j = 1,2,\cdots,n)$，首先，s-AMF 为其生成部分私钥 $(D_{j,0}, D_{j,1}) = (\lambda Q_{j,0}, \lambda Q_{j,1})$，并通过安全信道发送给 V_j。然后，由 s-gNB$_1$ 发送消息 $\{\text{GID}, \text{MAC}_j, \{\text{NCC}_j, t_1\}_{K_{\text{s-AMF-}j}}\}$ 到车辆 V_j。车辆 V_j 收到消息后，首先选择随机数 $x_j \in Z_q^*$ 作为自己的私钥，然后计算并公布公钥 $P_j = x_j P$，最后，和车辆 $V_i (i = 2,3,\cdots,n)$ 一样检验消息。

2.3 群组切换认证

本阶段发生在满足切换触发阈值条件时，如车辆群组停留在 s-gNB$_1$ 范围内的时间不超过 3 s。即车辆群组在即将离开当前基站进入目标基站范围内的短时间里，开始执行群组切换认证阶段。群组切换认证流程如图 3 所示，各步骤详细描述如下。

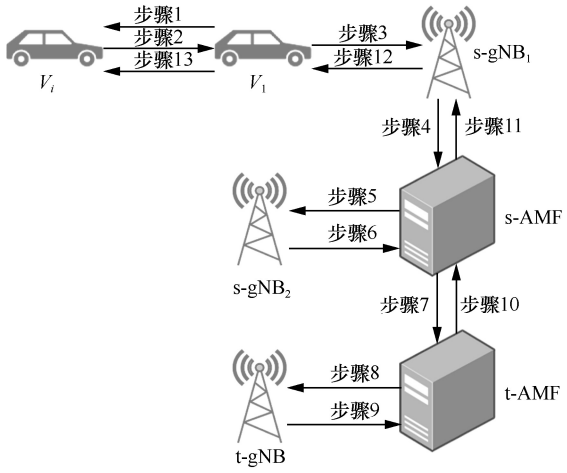


图 3 群组切换认证流程

步骤 1 组长 V_1 通过 V2V 接口组播身份验证请求信息 $\{\text{TID}_1, \text{GID}_1, t_2\}$ 到组员 $V_i (i = 2,3,\cdots,n)$。

步骤 2 组员 V_i 接收到身份验证请求信息后，先检查时间戳 t_2 的新鲜性，然后根据式(3)验证组长 V_1 的身份。如果身份验证通过，V_i 选择随机数 $r_i \in Z_q^*$，计算 $R_i = r_i P$。然后，根据式(6)～式(10)计算签名所需信息 T、V、W、h_i 和 S_i，得到签名 $\text{Sig}_i = (R_i, S_i)$。最后，单播签名 Sig_i 到组长 V_1。

$$T = H_2(\text{GID}) \tag{6}$$

$$V = H_3(\text{GID}) \tag{7}$$

$$W = H_4(\text{GID}) \tag{8}$$

$$h_i = H_5(\text{TID}_i \| \text{GID} \| \text{SUPI}_i \| P_i) \tag{9}$$

$$S_i = D_{i,0} + x_i V + h_i (D_{i,1} + x_i W) + r_i T \tag{10}$$

步骤 3 组长 V_1 接收到所有组员的签名 Sig_i

后，先生成自己的签名 Sig_1。然后，生成聚合签名 $\mathrm{Sig}=(R,S)$，其中，$R=\sum_{i=1}^{n}R_i$，$S=\sum_{i=1}^{n}S_i$。最后，发送切换请求信息 $\{\mathrm{Sig},\mathrm{Info},t_3\}_{K_{\text{s-gNB}_{1\text{-}1}}}$ 到 s-gNB$_1$，其中，Info 为群组的移动信息，包括群组位置、移动方向、移动速度等信息。

步骤 4　s-gNB$_1$ 接收到切换请求信息后，先检查时间戳 t_3 的新鲜性，根据式(6)～式(10)和在初始认证阶段获得的 SUPI_i 来计算车辆签名所需信息 T、V、W、h_i 和 $(Q_{i,0},Q_{i,1})$。然后，根据式(11)验证聚合签名 Sig。如果验证成功，通过安全信道发送移动信息 Info 到 s-AMF。如果验证失败，则通过二分查找法快速查找恶意用户，流程如下。① s-gNB$_1$ 请求组长 V_1 把聚合签名 Sig 分为 2 份，其中，每一份包含组内一半车辆的聚合签名。然后，V_1 将 2 份签名发送给 s-gNB$_1$；②s-gNB$_1$ 验证 2 份聚合签名，将其中未通过验证的聚合签名再发送给 V_1，请求 V_1 将未验证通过的聚合签名再次分为 2 份。重复步骤①和步骤②，直到查找到组内恶意用户。最后，组长 V_1 重新发送聚合签名到 s-gNB$_1$，s-gNB$_1$ 再重新执行本步骤。

$$e(S,P)=e\left(P_T,\sum_{i=1}^{n}Q_{i,0}+\sum_{i=1}^{n}h_iQ_{i,1}\right)\cdot e\left(V,\sum_{i=1}^{n}P_i\right)e\left(W,\sum_{i=1}^{n}h_iP_i\right)e(T,R) \tag{11}$$

步骤 5　s-AMF 根据接收到的移动信息 Info 选择执行域内切换程序或域间切换程序，如果是域间切换则执行步骤 7。AMF 域内切换程序根据移动信息 Info 选择域内的 s-gNB$_2$，然后，通过安全信道发送域内−切换请求信息 $\{\mathrm{Info},\mathrm{NH}_i,\mathrm{NCC}_i,\mathrm{SUCI}_i,\mathrm{GID},\mathrm{TID}_i,K_{\text{s-AMF-}i}\}$ 到 s-gNB$_2$。

步骤 6　s-gNB$_2$ 接收到域内−切换请求信息后，由 NH_i 计算 $\mathrm{NH}_i^*=H(\mathrm{NH}_i)\oplus\mathrm{NH}_i$，根据式(12)计算与车辆 V_i 的新会话密钥 $K_{\text{s-gNB}_{2\text{-}i}}$，其中，KDF 为密钥派生函数。然后，更新相应的 NCC_i 值，选择随机数 $r_{\text{s-gNB}_2}\in Z_q^*$，计算 $R_{\text{s-gNB}_2}=r_{\text{s-gNB}_2}P$，再根据式(6)～式(8)和式(13)～式(14)计算签名所需信息 T、V、W、$h_{\text{s-gNB}_2}$ 和 $S_{\text{s-gNB}_2}$，得到签名 $\mathrm{Sig}_{\text{s-gNB}_2}=(R_{\text{s-gNB}_2},S_{\text{s-gNB}_2})$。最后，计算 $\mathrm{sMAC}=H(\mathrm{Sig}_{\text{s-gNB}_2}\|\mathrm{ID}_{\text{s-gNB}_2}\|\mathrm{PCI}_{\text{s-gNB}_2}\|\mathrm{NCC}_i\|\mathrm{ARFCN-DL}_{\text{s-gNB}_2}\|t_4)$，并发送域内−切换响应信息 $\{\mathrm{ID}_{\text{s-gNB}_2},\mathrm{PCI}_{\text{s-gNB}_2},\mathrm{Sig}_{\text{s-gNB}_2},t_4,\mathrm{ARFCN-DL}_{\text{s-gNB}_2},\mathrm{sMAC}\}_{K_{\text{s-AMF-1}}}$ 到 s-AMF，接着执行步骤 11。

$$K_{\text{s-gNB}_{2\text{-}i}}=\mathrm{KDF}(K_{\text{s-AMF-}i}\|\mathrm{NH}_i^*\|\mathrm{Info}\|\mathrm{PCI}_{\text{s-gNB}_2}\|\mathrm{ARFCN-DL}_{\text{s-gNB}_2}) \tag{12}$$

$$h_{\text{s-gNB}_2}=H_5(\mathrm{Info}\|\mathrm{GID}\|\mathrm{ID}_{\text{s-gNB}_2}\|P_{\text{s-gNB}_2}) \tag{13}$$

$$S_{\text{s-gNB}_2}=D_{\text{s-gNB}_{2,0}}+x_{\text{s-gNB}_2}V+h_{\text{s-gNB}_2}(D_{\text{s-gNB}_{2,1}}+x_{\text{s-gNB}_2}W)+r_{\text{s-gNB}_2}T \tag{14}$$

步骤 7　s-AMF 根据接收到的移动信息 Info 选择域外的 t-AMF，执行域间切换程序，根据式(15)为 t-AMF 和车辆 V_i 计算新密钥。然后，通过安全信道把系统参数、会话密钥和身份信息等安全上下文发送给 t-AMF，并删除相关信息。

$$K_{\text{t-AMF-}i}=\mathrm{KDF}(K_{\text{s-AMF-}i}\|\mathrm{TID}_i\|\lambda P_i) \tag{15}$$

步骤 8　t-AMF 接收到安全上下文信息后，根据移动信息 Info 选择域内的 t-gNB。然后，t-AMF 通过安全信道发送域间−切换请求信息 $\{\mathrm{NH}_i,\mathrm{NCC}_i,K_{\text{t-AMF-}i},K_{\text{t-AMF-1}},\mathrm{GID},\mathrm{TID}_i,\mathrm{SUCI}_i,\mathrm{Info}\}$ 到 t-gNB。

步骤 9　t-gNB 接收到来自 t-AMF 的域间−切换请求信息后，计算 $\mathrm{NH}_i^*=H(\mathrm{NH}_i)\oplus\mathrm{NH}_i$，根据式(12)和从 t-AMF 获得的 $K_{\text{t-AMF-}i}$、Info 等信息计算出新会话密钥 $K_{\text{t-gNB-}i}$，更新相应的 NCC_i 值。然后，t-gNB 选择随机数 $r_{\text{t-gNB}}\in Z_q^*$，计算并公布 $R_{\text{t-gNB}}=r_{\text{t-gNB}}P$，再根据式(6)～式(8)和式(13)～式(14)计算签名所需要的信息 T、V、W、$h_{\text{t-gNB}}$ 和 $S_{\text{t-gNB}}$，得到签名 $\mathrm{Sig}_{\text{t-gNB}}=(R_{\text{t-gNB}},S_{\text{t-gNB}})$。最后，计算消息验证码 $t\mathrm{MAC}=H(\mathrm{ID}_{\text{t-gNB}}\|\mathrm{Sig}_{\text{t-gNB}}\|\mathrm{PCI}_{\text{t-gNB}}\|\cdot\|\mathrm{NCC}_i\|t_5\mathrm{ARFCN-DL}_{\text{t-gNB}})$。t-gNB 发送域间−切换响应信息 $\{\mathrm{PCI}_{\text{t-gNB}},\mathrm{ARFCN-DL}_{\text{t-gNB}},\mathrm{Sig}_{\text{t-gNB}},\mathrm{ID}_{\text{t-gNB}},\mathrm{tMAC},t_5\}_{K_{\text{t-AMF-1}}}$ 到 t-AMF。

步骤 10　t-AMF 转发响应信息到 s-AMF。

步骤 11　s-AMF 转发响应信息到 s-gNB$_1$。

步骤 12　s-gNB$_1$ 转发响应信息到组长 V_1。

步骤 13　①如果是 AMF 域内切换，组长 V_1 先计算 $\mathrm{NH}_1^*=H(\mathrm{NH}_1)\oplus\mathrm{NH}_1$，再根据式(12)计算出新会话密钥 $K_{\text{s-gNB}_{2\text{-}1}}$。然后，由消息验证码 sMAC 检验 t_4 的新鲜性和 NCC_1 的正确性，并更新 NCC_1 值，再根据式(6)～式(8)和式(13)计算 T、V、W、$h_{\text{s-gNB}_2}$ 和 $(Q_{\text{s-gNB}_{2,0}},Q_{\text{s-gNB}_{2,1}})$。最后，根据式(16)验证 s-gNB$_2$ 的签名。

$$e(S_{\text{s-gNB}_2},P)=e(P_T,Q_{\text{s-gNB}_{2,0}}+h_{\text{s-gNB}_2}Q_{\text{s-gNB}_{2,1}})\cdot$$
$$e(V,P_{\text{s-gNB}_2})e(W,h_{\text{s-gNB}_2}P_{\text{s-gNB}_2})e(T,R_{\text{s-gNB}_2}) \quad (16)$$

如果签名验证成功，组长V_1通过 V2V 接口向组员V_i组播新会话密钥生成信息$\{\text{PCI}_{\text{s-gNB}_2},\text{ARFCN}-\text{DL}_{\text{s-gNB}_2},\text{ID}_{\text{s-gNB}_2},\text{Info},t_6\}$。组员$V_i$接收到组播信息后，先检验$t_6$的新鲜性，再根据接收到的信息计算$\text{NH}_i^*$和$K_{\text{s-gNB}_{2\text{-}i}}$，更新$\text{NCC}_i$值。最后，s-AMF 和车辆群组更新$\text{TID}_i^*=H(\text{NH}_i^*\ \ \text{SUCI}_i\|K_{\text{s-AMF-}i})$。②如果是 AMF 域间切换，组长$V_1$先计算$\text{NH}_1^*=H(\text{NH}_1)\oplus\text{NH}_1$和新密钥$K_{\text{t-AMF-1}}=\text{KDF}(K_{\text{s-AMF-1}}\|\text{TID}_1\|x_1P_T)$，因为$P_T=\lambda P$且$P_1=x_1P$，所以，$\lambda P_1=x_1P_T$成立。然后，由消息验证码 tMAC 检验$t_5$的新鲜性和$\text{NCC}_1$的正确性，并更新$\text{NCC}_1$值，接下来的流程如步骤①所述。组员$V_i$在接收到组播消息后，先检查时间戳$t_7$，然后计算$\text{NH}_i^*$、$K_{\text{t-AMF-}i}$和$K_{\text{t-gNB-}i}$，之后的流程如步骤①所述。最后，t-AMF 和车辆群组更新身份$\text{TID}_i^*=H(\text{NH}_i^*\|\text{SUCI}_i\|K_{\text{t-AMF-}i})$，为下次切换认证做准备。

3 安全分析

3.1 基于 Scyther 的安全分析

Scyther 是一种形式化安全协议分析工具，可以自动检测协议是否存在潜在攻击，如 DoS 攻击和重放攻击等。根据文献[27]对本文协议建模分析，建模共包括 2 个实体，即V_i和 t-gNB。

Scyther 形式化分析结果如图 4 所示。从图 4 可知，所有实体都可以满足文献[28]中的认证属性。此外，身份信息、密钥材料和新生成的会话密钥$K_{\text{t-gNB}}$也是保密的。

3.2 非形式化安全性分析

本节采用非形式化安全性分析的方式，进一步分析说明本文协议如何满足所有的安全属性。

相互认证。对于本文协议，每个V_i都通过安全信道从 s-AMF 处获得部分私钥$(D_{i,0},D_{i,1})$，用于生成自己的签名Sig_i。然后，V_i将签名发送到V_1处生成聚合签名 Sig，V_1再将 Sig 发送到 s-gNB$_1$进行无证书聚合签名验证。若存在任何一个无效的签名，则聚合验证就会失败，只有车辆群组内所有的车辆都产生有效的签名时，才能验证成功。因此，s-gNB$_1$可以通过检查无证书聚合签名验证结果来认证车辆群组。另一方面，目标基站 s-gNB$_2$（t-gNB）也从 s-AMF（t-AMF）处通过安全信道获得自己的部分私钥，然后生成签名，发送给V_1进行签名验证。由于目标基站只能从与 AMF 相连的安全信道中获得派生新会话密钥的NH_i、GID、Info 等材料信息。因此，V_1可以通过检查基站签名验证结果来认证基站。

Claim			Status	Comments
TPGHA Vi	TPGHA,Vi2	Secret_Hidden_ 1	ok Verified	No attacks.
	TPGHA,Vi3	Secret n_1	ok Verified	No attacks.
	TPGHA,Vi4	Secret info	ok Verified	No attacks.
	TPGHA,Vi5	Secret NH	ok Verified	No attacks.
	TPGHA,Vi6	Secret n_2	ok Verified	No attacks.
	TPGHA,Vi7	Secret kt-gNB	ok Verified	No attacks.
	TPGHA,Vi8	Secret ID	ok Verified	No attacks.
	TPGHA,VI9	Alive	ok Verified	No attacks.
	TPGHA,Vi10	Weakagree	ok Verified	No attacks.
	TPGHA,Vi11	Niagree	ok Verified	No attacks.
	TPGHA,Vi12	Nisynch	ok Verified	No attacks.
t-gNB	TPGHA,t-gNB$_2$	Secret_ Hidden_ 2	ok Verified	No attacks.
	TPGHA,t-gNB$_3$	Secret ID	ok Verified	No attacks.
	TPGHA,t-gNB$_4$	Secret n_2	ok Verified	No attacks.
	TPGHA,t-gNB$_5$	Secret kt-gNB	ok Verified	No attacks.
	TPGHA,t-gNB$_6$	Secret n_1	ok Verified	No attacks.
	TPGHA,t-gNB$_7$	Secret info	ok Verified	No attacks.
	TPGHA,t-gNB$_8$	Secret NH	ok Verified	No attacks.
	TPGHA,t-gNB$_9$	Alive	ok Verified	No attacks.
	TPGHA,t-gNB$_{10}$	Weakagree	ok Verified	No attacks.
	TPGHA,t-gNB$_{11}$	Niagree	ok Verified	No attacks.
	TPGHA,t-gNB$_{12}$	Nisynch	ok Verified	No attacks.

图 4 Scyther 形式化分析结果

密钥协商。1) 在执行 AMF 域内切换时，车辆和目标基站都通过式(12)派生新会话密钥$K_{\text{s-gNB2-}i}$，其中，s-gNB$_2$只能从与 s-AMF 相连接的安全信道中获得派生新会话密钥的 Info 和NH_i等材料信息，且车辆V_i只能从 s-gNB$_2$处获得 s-gNB$_2$的$\text{PCI}_{\text{s-gNB}_2}$和$\text{ARFCN}-\text{DL}_{\text{s-gNB}_2}$等标识符信息，如果缺少以上任何一个参数都无法计算出新会话密钥$K_{\text{s-gNB}_{2\text{-}i}}$。2) 在执行 AMF 域间切换时，车辆$V_i$和 t-AMF 分别通过方法$\text{KDF}(K_{\text{s-AMF-}i}\|\text{TID}_i\|x_iP_T)$和$\text{KDF}(K_{\text{s-AMF-}i}\|\text{TID}_i\|\lambda P_i)$来计算新密钥$K_{\text{t-AMF-}i}$，其中，$P_i=x_iP$、$P_T=\lambda P$、$P$是系统公共参数、参数$x_i$和$\lambda$分别是车辆$V_i$和 t-AMF 的秘密参数，在不知道参数$x_i$和$\lambda$的前提下，计算出$P_i$或$P_T$求解新密钥$K_{\text{t-AMF-}i}$等价于求解椭圆曲线迪菲−赫尔曼密钥交换（ECDH, elliptic curve Diffie-Hellman key exchange）问题或求

解椭圆曲线离散对数（ECDL, elliptic curve discrete logarithm）问题。

隐式密钥确认。当车辆群组执行完群组切换认证协议后，车辆与目标基站会协商出一个新会话密钥 $K_{\text{t-gNB}}$，但是，车辆并不会立即采用新会话密钥与目标基站交互信息获取网络服务，完成显式密钥确认，而是当车辆到达目标基站服务范围内时，才使用新会话密钥 $K_{\text{t-gNB}}$ 与目标基站交互信息，目标基站确认会话密钥的正确性后，为车辆提供网络服务，完成隐式密钥确认。

抵抗重放攻击。本文协议在车辆第一次连接到 5G 核心网络时，都会先对车辆进行初始认证，然后对系统进行初始化，用于更新关键的系统参数等信息，防止重放攻击。一方面，V_1 与 V_i 进行通信时，通过 V2V 接口采用单播与组播的方式保证信息传输安全，首先，V_i 采用群组切换准备阶段生成的临时身份标识符 TID_i 生成签名所需材料 h_i，然后单播签名到组长生成聚合签名，TID_i 在每次切换认证协议执行前后都会更新，防止重放攻击；V_1 向 V_i 组播信息时，会包含新生成的时间戳，用于 V_i 验证组播消息的新鲜性，防止重放攻击。另一方面，V_1 与基站之间采用无线信道进行不安全的通信，采用临时身份标识符 TID_i、时间戳 t 和移动信息 Info 抵抗重放攻击，其中，Info 在每次协议执行过程中由 V_1 临时生成。

隐私保护（匿名性和不可链接性）。在本文协议中，V_i 采用临时身份标识符 TID_i，而非车辆的永久身份标识符 SUPI_i。因为车辆的真实身份只有合法的基站和核心网络知道，所以车辆的匿名性得到了满足。此外，TID_i 在每次协议执行前后都会更新，所以无法确定 2 个 TID_i 是否属于同一车辆。因此，也无法将车辆的移动信息 Info 与车辆联系起来，从而保证了不可链接性。

抵抗 DoS 攻击。针对 3GPP 的 5G-AKA 协议标准，攻击者可以模拟一个合法的基站，并向车辆群组发送大量虚假的 NCC 值来破坏密钥派生过程。本文协议通过添加 MAC 来确保 NCC 值的机密性和完整性。此外，对于聚合签名技术易遭受 Dos 攻击的缺陷，本文提出了一种通用的基于二分查找法的解决方法来快速定位恶意用户，提高群组切换认证协议的执行效率。

抵抗伪造基站攻击。在本文协议中，车辆群组和目标基站通过无证书聚合签名技术相互认证。此外，只有合法基站才能通过 AMF 的安全信道获得 NH_i 和 Info 等用于派生新会话密钥的材料信息，缺少任何一个材料信息，伪造基站都无法与车辆群组建立通信。因此，本文协议可以抵抗伪造基站攻击。

完美前向安全和抵抗密钥泄露。为了防止目标基站知道未进入其覆盖范围的 V_i 的会话密钥，本文协议通过 $\text{NH}_i^* = H(\text{NH}_i) \oplus \text{NH}_i$ 方法对 NH_i 值进行加密。这样，目标基站只有从与 AMF 相连接的安全信道中获得 NH_i 值，才能派生出新的会话密钥。此外，即使当前的 NH_i^* 值泄露，由于哈希映射的单向性，攻击者也无法推理出之前的 NH_i 值，从而保证了完美前向安全。

完美后向安全。本文协议在每次开始执行时都会先对车辆进行初始认证，然后对系统进行初始化，用于更新关键的系统参数等信息。此外，在每次执行群组切换认证阶段，V_1 都会生成临时的移动信息 Info，经 s-gNB_1 验证聚合签名成功后，通过安全信道发送 Info 给 AMF 用于选择目标基站，再派生出与目标基站交互的新会话密钥。所以，即使当前会话的 NH_i 值等关键密钥信息泄露也不会影响之后的会话安全，从而提供了完美后向安全。

为了体现本文协议的功能和特征，进一步将本文协议与文献[19]、文献[20]和文献[26]中的群组切换认证协议进行了比较，文献[19]中的 2 个协议分别记为文献[19]协议 1 和文献[19]协议 2，具体如表 2

表 2　　**功能和特征对比**

协议	轨迹不固定	组员无等待	隐私保护	双向认证	PFS/PBS	抗 DoS 攻击	抗重放攻击
文献[19]协议 1	×	√	×	√	×	×	√
文献[19]协议 2	×	√	√	√	√	×	√
文献[20]协议	√	×	√	√	√	√	√
文献[26]协议	×	×	×	×	×	×	×
本文协议	√	√	√	√	√	√	√

所示，其中，组员无等待是指当车辆群组进入目标基站范围内时，组员 V_i 可以直接进行认证，不需要等待组长 V_1 认证完成后再进行认证。此外，由于所有协议均与标准兼容，且存在密钥协商过程，便不再把标准兼容和密钥协商加入表 2 中对比。

4 性能评估

本节将本文协议与文献[19]协议 1 与协议 2、文献[20]协议和文献[26]5G 标准协议进行比较。在仿真中，假设所有对称加密密钥为 256 位，MAC 为 160 位，NH、H(NH)、hash、TID、GID、ID、SUPI、SUCI、PCI 和 ARFCN-DL 为 128 位，时间戳 t 为 32 位，群 G_1 和 G_2 中的元素的大小分别为 1 024 位和 320 位。

4.1 信令开销

本文通过各协议的信令开销来评估造成网络拥堵的可能性，其中，信令开销是根据 n 辆车所构成的群组和网络之间的消息数来计算的。此外，本文只统计切换认证期间的消息数。各协议的信令开销对比结果如表 3 所示。

表 3 包含 n 辆车的群组的信令开销

协议	信令开销/个
文献[19]协议 1	$2n+12$
文献[19]协议 2	$2n+12$
文献[20]协议	$n+11$
文献[26]协议	$8n$
本文协议	$n+11$

从表 3 中可以看出，本文协议的信令开销明显低于文献[26]5G 标准协议。

4.2 计算开销

对于计算开销，本节遵循文献[19]协议中的评估工作，先构建一个测试环境，采用 C/C++ OpenSSL 库来计算这些密码学操作的计算开销，将该库在搭载 CPU 0.9 GHz 处理器的英特尔酷睿 m3-6Y30 上的测试用时作为车辆的计算用时，在搭载 CPU 2.70 GHz 处理器的英特尔酷睿 i7-7500U 上的测试用时作为基站的计算用时。经测试得到车辆和基站执行点乘计算 T_{M} 分别用时 960 μs 和 500 μs，执行对称加解密计算 T_{S} 分别用时 2.26 μs 和1.05 μs，执行哈希计算 T_{H} 分别用时 2.38 μs 和1.21 μs。忽略异或计算、乘法计算和算术计算等计算开销。

经分析统计各协议流程的执行过程，得到各协议内车辆群组和基站所需要的计算开销，结果如表 4 所示，本文仅统计群组切换认证期间所需要的计算操作数。通常，不同的车辆可以并行地进行计算。由表 4 可知，在群组切换认证期间内，本文协议的车辆群组和基站的计算开销和为 $7.18n+7.83$，现有效率最优的文献[20]协议为$10.49n+6.62$，当群组内车辆数 n 取 10 的时候，本文协议与文献[20]协议相比较，计算效率提高了约 29%，当群组内车辆数 n 取 50 和 100 时，计算效率均提高了约 31%，所以，与现有最优协议相比，本文协议计算效率提高了约 30%。

通过以上测试计算和统计分析，得出各协议执行车辆群组切换认证协议期间，车辆群组和基站的计算开销之和随着群组内车辆总数变化的增长趋势，如图 5 所示，其中，群组切换认证期间车辆群组和基站的计算开销之和简称为总计算开销。通过表 3～表 4 和图 5 可知，本文协议在信令开销和计算开销上均优于其他协议。此外，因为本文协议通过对车辆群组行驶轨迹进行预测，提前执行密钥协商过程，所以，在协议执行的时间开销上也远低于文献[20]协议。综上所述，本文协议在效率上优于现有最优协议。

表 4 包含 n 辆车的车辆群组和基站的计算开销

协议	车辆群组计算开销/μs	基站计算开销/μs
文献[19]协议 1	$5nT_{\mathrm{H}}+T_{\mathrm{S}}$	$5nT_{\mathrm{H}}+T_{\mathrm{S}}$
文献[19]协议 2	$3nT_{\mathrm{M}}+(3n+1)T_{\mathrm{H}}+T_{\mathrm{S}}$	$(2n+4)T_{\mathrm{M}}+(4n+1)T_{\mathrm{H}}+T_{\mathrm{S}}$
文献[20]协议	$2nT_{\mathrm{H}}+(n+2)T_{\mathrm{S}}$	$2nT_{\mathrm{H}}+(n+2)T_{\mathrm{S}}$
文献[26]协议	$4nT_{\mathrm{H}}$	$4nT_{\mathrm{H}}$
本文协议	$2nT_{\mathrm{H}}+3T_{\mathrm{S}}$	$2nT_{\mathrm{H}}+T_{\mathrm{S}}$

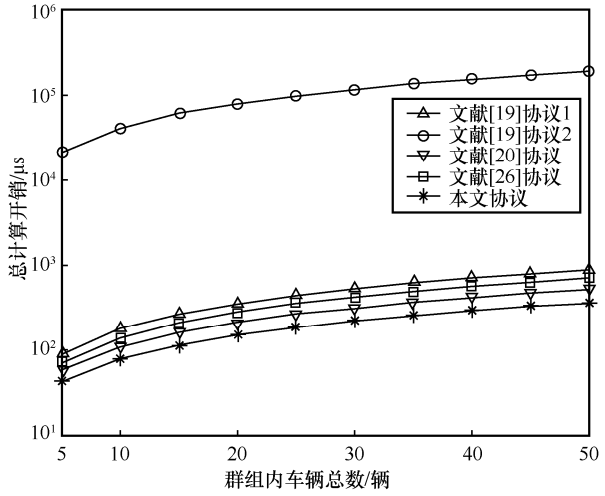


图 5　总计算开销对比

5　结束语

本文针对 5G-V2X 场景中大量车辆执行切换认证的效率以及安全问题，提出了一种基于轨迹预测的安全高效群组切换认证协议。考虑到车辆轨迹可预测的特点，提前完成密钥协商协议。根据用户分组算法结合源基站和周围基站的信干噪比和距离等信息，源基站将具有移动相关性的车辆视为同一群组，再采用无证书聚合签名技术批量验证群组内所有车辆。针对聚合签名技术易遭受 DoS 攻击的弊端，采用二分查找法快速定位恶意用户，提高群组切换认证协议的执行效率。安全性分析表明，本文协议可以保护车辆隐私安全，抵抗重放攻击、DoS 攻击等传统攻击。效率分析表明，本文协议与现有最优协议相比，计算效率提高了 30%。

参考文献：

[1] 徐哲鑫, 高楷蒙, 贾文康, 等. 负载约束的 C-V2X 车辆缓存节点选择算法[J]. 通信学报, 2021, 42(3): 171-182.
XU Z X, GAO K M, JIA W K, et al. Vehicular cache nodes selection algorithm under load constraint in C-V2X[J]. Journal on Communications, 2021, 42(3): 171-182.

[2] SUN S H, HU J L, PENG Y, et al. Support for vehicle-to-everything services based on LTE[J]. IEEE Wireless Communications, 2016, 23(3): 4-8.

[3] 邵雯娟, 沈庆国. 软件定义的 D2D 和 V2X 通信研究综述[J]. 通信学报, 2019, 40(4): 179-194.
SHAO W J, SHEN Q G. Survey of software defined D2D and V2X communication[J]. Journal on Communications, 2019, 40(4): 179-194.

[4] WIEST J, HÖFFKEN M, KREBEL U, et al. Probabilistic trajectory prediction with Gaussian mixture models[C]//Proceedings of 2012 IEEE Intelligent Vehicles Symposium. Piscataway: IEEE Press, 2012: 141-146.

[5] HOUENOU A, BONNIFAIT P, CHERFAOUI V, et al. Vehicle trajectory prediction based on motion model and maneuver recognition[C]//Proceedings of 2013 IEEE/RSJ International Conference on Intelligent Robots and Systems. Piscataway: IEEE Press, 2014: 4363-4369.

[6] ALTCHÉ F, DE-LA-FORTELLE A. An LSTM network for highway trajectory prediction[C]//Proceedings of 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC). Piscataway: IEEE Press, 2018: 353-359.

[7] MA Y X, ZHU X G, ZHANG S B, et al. TrafficPredict: trajectory prediction for heterogeneous traffic-agents[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2019, 33(1): 6120-6127.

[8] 张应辉, 胡凌云, 李艺昕, 等. 空间信息网络中基于动态撤销机制的安全高效批量认证方案[J]. 通信学报, 2022, 43(4): 164-176.
ZHANG Y H, HU L Y, LI Y X, et al. Secure and efficient batch authentication scheme based on dynamic revocation mechanism in space information network[J]. Journal on Communications, 2022, 43(4): 164-176.

[9] CHEN S, HU J, SHI Y, et al. A vision of C-V2X: technologies, field testing and challenges with Chinese development[J]. arXiv Preprint, arXiv: 2002.08736, 2020.

[10] KENNEY J B. Dedicated short-range communications (DSRC) standards in the United States[J]. Proceedings of the IEEE, 2011, 99(7): 1162-1182.

[11] GHARSALLAH I, SMAOUI S, ZARAI F. An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks[J]. IET Information Security, 2020, 14(1): 21-29.

[12] WANG P F, DI B Y, ZHANG H L, et al. Platoon cooperation in cellular V2X networks for 5G and beyond[J]. IEEE Transactions on Wireless Communications, 2019, 18(8): 3919-3932.

[13] 杨芫, 徐明伟, 陈浩. 5G/后 5G 部署对互联网主干影响的分析与建模[J]. 通信学报, 2019, 40(8): 36-44.
YANG Y, XU M W, CHEN H. Analysis and modeling of Internet backbone traffic with 5G/B5G[J]. Journal on Communications, 2019, 40(8): 36-44.

[14] ZHANG Y H, DENG R H, BERTINO E, et al. Robust and universal seamless handover authentication in 5G HetNets[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 858-874.

[15] CAO J, MA M D, LI H, et al. A survey on security aspects for 3GPP 5G networks[J]. IEEE Communications Surveys & Tutorials, 2020, 22(1): 170-195.

[16] SHARMA A, JAIN A, SHARMA I. Exposing the security weaknesses of fifth generation handover communication[C]//Proceedings of 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Piscataway: IEEE Press, 2019: 1-6.

[17] LI G J, LAI C Z. Platoon handover authentication in 5G-V2X[C]//Proceedings of 2020 IEEE Conference on Communications and Network Security (CNS). Piscataway: IEEE Press, 2020: 1-2.

[18] PAN M S, LIN T M, CHEN W T. An enhanced handover scheme for

mobile relays in LTE-a high-speed rail networks[J]. IEEE Transactions on Vehicular Technology, 2015, 64(2): 743-756.

[19] 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.

[20] YAN X B, MA M D, SU R. A certificateless efficient and secure group handover authentication protocol in 5G enabled vehicular networks[C]//Proceedings of IEEE International Conference on Communications. Piscataway: IEEE Press, 2022: 1678-1684.

[21] LEE H J, KIM D, CHUNG B, et al. Adaptive hysteresis using mobility correlation for fast handover[J]. IEEE Communications Letters, 2008, 12(2): 152-154.

[22] ZHANG L, QIN B, WU Q, et al. Efficient many-to-one authentication with certificateless aggregate signatures[J]. Computer Networks, 2010, 54(14): 2482-2491.

[23] GARCIA M H C, MOLINA-GALAN A, BOBAN M T, et al. A tutorial on 5G NR V2X communications[J]. IEEE Communications Surveys & Tutorials, 2021, 23(3): 1972-2026.

[24] 3GPP. Architectural enhancements for 5G multicast-broadcast services (Release 17)[R]. 2021.

[25] HAROUNABADI M, SOLEYMANI D M, BHADAURIA S, et al. V2X in 3GPP standardization: NR sidelink in release-16 and beyond[J]. IEEE Communications Standards Magazine, 2021, 5(1): 12-21.

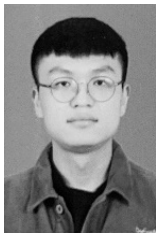
[26] 3GPP. Security architecture and procedures for 5G system (Release 16): TS33.501[S]. 2022.

[27] CREMERS C S. Scyther: semantics and verification of security protocols[D]. Eindhoven: Eindhoven University of Technology, 2006.

[28] LOWE G. A hierarchy of authentication specifications[C]//Proceedings of the 10th Computer Security Foundations Workshop. Piscataway: IEEE Press, 2002: 31-43.

[作者简介]

张应辉（1985− ），男，陕西西安人，博士，西安邮电大学教授，主要研究方向为公钥密码学、云安全和无线网络安全等。



钱佳乐（1997− ），男，河南周口人，西安邮电大学硕士生，主要研究方向为无线网络安全和 5G 安全。

曹进（1985− ），男，陕西西安人，博士，西安电子科技大学教授，主要研究方向为应用密码学和 5G、6G、天地一体化网络安全等。

郑东（1964− ），男，山西临汾人，博士，西安邮电大学教授，主要研究方向为编码密码学和网络安全。