一种新的隐私保护型车载网络切换认证协议

周治平* 张惠根 孙子文 李 静
(江南大学物联网技术应用教育部工程研究中心 无锡 214122)

摘 要：该文针对现有车载网络切换认证协议存在的安全性、隐私等方面的不足，在 LIAP 协议的基础上提出改进方案。首先将随机数与伪标识串联，再用二次模运算对串联的信息进行加密，以生成动态身份标识保护用户位置隐私；与此同时，在移动终端切换过程中，新路侧单元重新生成新会话秘密序列，并与终端伪标识进行异或加密，对 LIAP 协议中存在的平行会话攻击进行安全防护。理论分析及实验表明，改进协议不仅满足终端匿名性和抵御各种攻击的安全需求，也实现了较快的切换速度，与同类切换认证协议相比，实用中具明显优越性。

关键词：车载网络；切换认证；二次剩余定理；隐私防护；平行会话攻击
中图分类号：TP309.2 **文献标识码**：A **文章编号**：1009-5896(2016)10-2633-07
DOI: 10.11999/JEIT160015

Improved Privacy Protection Handover Authentication Protocol for Vehicular Ad Hoc Networks

ZHOU Zhiping ZHANG Huigen SUN Ziwen LI Jing
(*Engineering Research Center of Internet of Things Technology Applications of Ministry of Education, Jiangnan University, Wuxi* 214122, *China*)

Abstract: To overcome the shortages in security and privacy of existing handover authentication protocols for vehicle network, an improved scheme based on the Lightweight Identity Authentication Protocol (LIAP) protocol is proposed in this paper. Firstly, terminal's pseudo-identity is concatenated with a random number, then quadratic residues operation is utilized to encrypt the connected information and to generate a dynamic identity, which can protect the user's location privacy. Meanwhile, the new road side unit regenerates a new session secret sequence and computes the challenge sequence with the terminal user's pseudo-identity by XOR encryption, which can provide secure protection against parallel session attack during the handover process. Theoretical analysis and experiments show that the proposed protocol can not only meet security requirements of providing terminal anonymity and defending various attacks, but also achieve a faster switching speed. Therefore, the improved protocol shows obvious superiorities over most existing schemes.

Key words: Vehicle network; Handover authentication; Quadratic residue theorem; Privacy protection; Parallel session attack

1 引言

由于无线网络信息传输无物理连接链路，攻击者可以在信息到达指定接收者之前侦听、分析并修改任何传输信息。因此，无线网络尤其是车载网络切换认证协议中的安全和隐私问题已成为无线网络安全领域的严重关切[1,2]。一般而言，性能优越的切换认证协议应符合以下认证需求[3]：(1)双向验证；(2)用户匿名性和不可追踪性；(3)有条件的隐私保护；(4)提供用户撤销功能；(5)抗攻击性；(6)低切换延时。

为避免由于切换而导致的连接中断，通常对切换过程施加严格的时间限制。例如，IEEE建议切换延迟不应超过50 ms，其认证过程更应低于20 ms[4,5]。因此，设计一种兼具安全隐私防护和快速切换的认证协议极具挑战性。

2012 年，文献[6]基于双线性对映射原理提出了一种无服务器式的切换认证协议，该协议利用双线性映射函数验证通信实体的合法性，切换认证过程无需服务器参与，也无需在各网络接入点之间建立信任关系，相比传统基于 AAA 服务器的切换认证

收稿日期：2016-01-04；改回日期：2016-05-19；网络出版：2016-07-15
*通信作者：周治平 zzp@jiangnan.edu.cn
基金项目：国家自然科学基金(61373126)；中央高校基本科研业务费专项资金(JUSRP51510)；江苏省自然科学基金(BK20131107)
Foundation Items: The National Natural Science Foundation of China (61373126), The Fundamental Research Funds for the Central Universities (JUSRP51510), The Natural Science Foundation of Jiangsu Province (BK20131107)

协议更具高效性。文献[7]也基于该思想提出了类似的切换认证协议，但考虑到移动终端有限的运算能力和存储空间，该协议中多次双线性对映射的使用对终端计算能力提出了较高要求。随后，文献[8]发现文献[6]中存在密钥破译问题，一旦敌方获取用户签名证书后即可根据互质性破译出用户私钥。2013 年，文献[9]创新性地提出了一种基于动态会话秘密过程的车载网络切换认证协议(Lightweight Identity Authentication Protocol, LIAP)，该协议中车载终端只使用了哈希散列、异或、随机序列生成等轻量级运算，具有认证延时低、切换速度快等优点，但经仔细分析，该协议易遭受位置追踪攻击及平行会话攻击[10]。2014 年，文献[11]基于双陷门变色龙哈希函数和椭圆曲线签名理论提出了一种可证明安全的切换认证协议，该协议在通信过程中明文传输了终端标识及证书，同样易遭受位置追踪隐患。随后，文献[12~14]相继提出了新的用户匿名保护、防位置追踪的切换认证协议，此类协议为解决匿名追踪问题，预配置阶段服务器需为移动终端加载一系列防位置链接的伪标识对，终端每次发起登录或切换请求时均需向接入点发送一未使用的伪标识对，因此该方案对终端内存开销较大；文献[15]和文献[16]又利用双线性映射理论相继提出了新的车载网络切换认证协议，其中文献[15]的切换认证过程需新旧路侧单元和车载终端的三方参与，认证中心需为各路侧单元建立信任关系，且双线性映射函数的使用代价较高。文献[17]基于变色龙哈希函数及椭圆曲线签名理论为车载终端设计了一种动态标识，有助于切换过程的匿名隐私保护，但较多的点乘运算使得传输的数据包信息字节数较大，增长的通信开销反而会影响协议性能；文献[18]提出了一种基于代理签名的认证方案，但模幂、模乘运算的多次执行难以满足漫游切换的快速性。2015 年，文献[19]为解决位置追踪隐患同样采用了预配置阶段加载一系列伪标识对的方法，因此该协议也存在文献[12~14]的不足。

为设计出一种满足安全快速、匿名隐私防护的切换认证协议，本文首先指出并分析了 LIAP 协议存在的隐私及安全隐患；然后针对其认证方式和安全威胁提出了改进方案；最后，详细分析了新协议的安全性、效率及开销。

2 LIAP 协议相关描述

2.1 系统模型与假设

车载网络由一个服务器、多个网络接入点(路侧单元)和移动设备(车载终端)组成，网络接入点能提供合法终端用户相应的网络服务，但每个用户在访问网络资源前须在服务中心注册帐号、密码等信息。一般地，终端和网络接入点的传输信道为不安全的，攻击者能使用双向侦听技术获取该信道的所有信息，并尝试利用获取的信息伪装合法装置。

2.2 协议符号说明

LIAP 协议由 4 个阶段组成：预配置阶段、初始化阶段、快速切换认证阶段以及更新阶段。协议中所用符号注释说明如表 1 所示。该协议采用了动态会话秘密过程 DSSP 来减少终端与接入点之间的网络接入与切换认证延时，相关过程详见文献[9]。

表 1 协议使用符号及相应注释

符号	注释
OBU_i, RSU_j, Server	车载终端，路侧单元，服务器
N_0, N_R, N_A	终端，路侧单元，服务器生成的随机数
UID_i, PWD_i	终端用户标识，密码
$\mathrm{metaUID}_i$	终端用户伪标识
K_i	终端和服务器的共享密钥
A_i	有效期内终端和服务器的共享凭证
EKu(·), DKr(·)	用公/私钥对信息加/解密
AKu, AKr	服务器的公，私钥
RKu, RKr	路侧单元的公，私钥
g, h	2 个大素数(私钥)
n	两个大素数的乘积(公钥)
S_r	单次随机会话秘密序列
RTA, ATA	挑战请求，应答请求序列
F(·), H(·)	单向哈希函数
$\oplus$	按位异或运算
$\|$	按位串联符

2.3 存在的安全隐患

2.3.1 隐私追踪问题 注意到 LIAP 协议中车载终端每次向路侧单元接入点发送接入网络或切换认证的请求时，发送的消息均为 $\mathrm{metaUID}_i$，而 $\mathrm{metaUID}_i = \mathrm{E}_{\mathrm{Ku}}(\mathrm{UID}_i)$，尽管 LIAP 协议未直接明文传输终端用户真实 ID，而是采用伪标识 $\mathrm{metaUID}_i$的形式隐藏了该信息，但是该车载终端在连接入网和接入点切换过程中公共信道中传输的 $\mathrm{metaUID}_i$ 是由服务器公钥加密而得是固定不变的。一旦敌方的这些窃听装置在一定时间内侦听到相同的接入或切换请求信息 $\mathrm{metaUID}_i$，便可对该车辆实行跟踪，攻击者后台处理中心也可利用部署在各个接入点附近的侦听装置分析出该车载终端用户的行驶路径，出入信息，行为习惯等私密信息，敌方甚至可以根据分析的结果对该特定用户进行尾随、埋伏。因此 LIAP 协议易遭受用户位置追踪攻击。

2.3.2 平行会话攻击问题　假设 RSU_{j+1} 和 RSU'_{j+1} 是路边架设的两个网络接入点，均从服务器端收到真实用户 OBU_i 的认证凭证 $A_{\mathrm{s},i}$，且 $A_{\mathrm{s},i}$ 未期满，敌方可通过执行如下步骤骗取网络准入，该攻击步骤如下，流程图如图 1 所示。

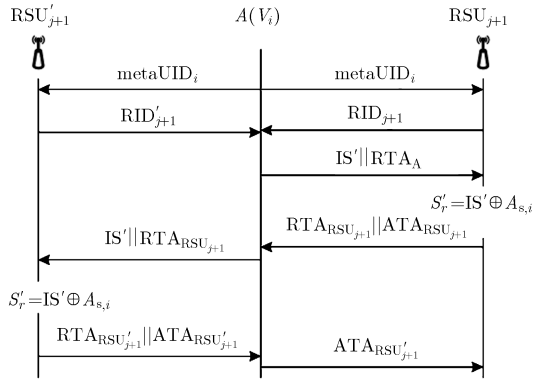

图 1 平行会话攻击流程

步骤 1　攻击者 A 向 RSU_{j+1} 和 RSU'_{j+1} 发起切换认证请求，并发送侦听截获的真实用户伪标识 $\mathrm{metaUID}_i$；

步骤 2　RSU_{j+1} (RSU'_{j+1})收到切换请求后先检测其待切换认证列表是否有该用户，根据假设，$\mathrm{metaUID}_i$ 确实存在于该列表中，RSU_{j+1} (RSU'_{j+1}) 再将其 ID 发送至 A；

步骤 3　当 A 收到接入点 RSU_{j+1} 和 RSU'_{j+1} 的身份标识后，A 选择一随机序列 IS′，并随机生成挑战请求 $\mathrm{RTA}_{\mathrm{A}}$，再发送 $\mathrm{IS}' \| \mathrm{RTA}_{\mathrm{A}}$ 至 RSU_{j+1}，值得注意的是，A 并无真实用户 OBU_i 的认证序列 $A_{\mathrm{s},i}$，A 也缺少会话秘密序列信息 S_r；

步骤 4　当 RSU_{j+1} 收到信息 $\mathrm{IS}' \| \mathrm{RTA}_{\mathrm{A}}$ 后，RSU_{j+1} 计算 $S'_r = \mathrm{IS}' \oplus A_{\mathrm{s},i}$，并根据 S'_r 生成 $\mathrm{RTA}_{\mathrm{A}}$ 的应答序列 $\mathrm{ATA}_{\mathrm{RSU}_{j+1}}$，随后再选择一新的挑战请求 $\mathrm{RTA}_{\mathrm{RSU}_{j+1}}$，将 $\mathrm{RTA}_{\mathrm{RSU}_{j+1}} || \mathrm{ATA}_{\mathrm{RSU}_{j+1}}$ 发送至 A；

步骤 5　A 收到信息 $\mathrm{RTA}_{\mathrm{RSU}_{j+1}} || \mathrm{ATA}_{\mathrm{RSU}_{j+1}}$ 后，暂先不对 $\mathrm{ATA}_{\mathrm{RSU}_{j+1}}$ 进行检测，也不对 $\mathrm{RTA}_{\mathrm{RSU}_{j+1}}$ 进行应答，而是先将 $\mathrm{IS}' \| \mathrm{RTA}_{\mathrm{RSU}_{j+1}}$ 发送至 RSU'_{j+1}，其中 IS′ 与步骤 3 中相同；

步骤 6　RSU'_{j+1} 收到信息 $\mathrm{IS}' \| \mathrm{RTA}_{\mathrm{RSU}_{j+1}}$ 后，计算 $S'_r = \mathrm{IS}' \oplus A_{\mathrm{s},i}$，再根据 S'_r 对 $\mathrm{RTA}_{\mathrm{RSU}_{j+1}}$ 进行应答产生 $\mathrm{ATA}_{\mathrm{RSU}'_{j+1}}$，再选择一新挑战请求 $\mathrm{RTA}_{\mathrm{RSU}'_{j+1}}$ 连同 $\mathrm{ATA}_{\mathrm{RSU}'_{j+1}}$ 一起发送至 A；

步骤 7　当A收到上述信息后，提取出 $\mathrm{ATA}_{\mathrm{RSU}'_{j+1}}$，并将其发送至 RSU_{j+1}，A 终止与 RSU'_{j+1} 的通信；

步骤 8　RSU_{j+1} 收到 $\mathrm{ATA}_{\mathrm{RSU}'_{j+1}}$ 后便验证其正确性，由于 RSU_{j+1} 和 RSU'_{j+1} 分别计算出的 $S'_r = \mathrm{IS}' \oplus A_{\mathrm{s},i}$ 是相等的，$\mathrm{ATA}_{\mathrm{RSU}'_{j+1}}$ 即是 $\mathrm{RTA}_{\mathrm{RSU}_{j+1}}$ 的正确应答，因此 RSU_{j+1} 认证了 A 的合法性，再计算 $\mathrm{E}_{\mathrm{AKU}}(\mathrm{metaUID}_i \| \mathrm{RID}_{j+1} \| N_A)$ 并将其发送至服务器；

步骤 9　服务器收到信息 $\mathrm{E}_{\mathrm{AKU}}(\mathrm{metaUID}_i \| \mathrm{RID}_{j+1} \| N_A)$ 后用私钥解密，再在数据注册表中对当前用户和其网络接入点进行数据更新。

通过上述分析，攻击者即使没有认证密钥或凭证，也可凭借截获的 $\mathrm{metaUID}_i$ 抢先于真实用户完成网络接入点的切换，而一旦上述攻击得手，服务器端注册表便执行错误的数据更新，导致合法用户在需要访问网络时无法及时连接入网。

3　新协议描述

为简便，新协议将更新阶段并入初始化阶段，因此新协议由：预配置、初始化(更新)、快速切换认证 3 个阶段组成。

3.1 预配置阶段

新协议预配置阶段大致与 LIAP 协议相同，动态会话秘密序列挑战应答协议 DSSP 执行过程详见文献[9]，新协议补充之处在于：认证中心预先产生 2 个大素数 g, h 作为私钥，计算出对应的公钥 $n = gh$。认证中心再将 g, h 和 n 分别存储至各路侧单元和车载终端内存中。新协议中所用符号注释说明同样如表 1 所示。

3.2 初始化阶段

该阶段由车载终端发起，流程如图 2 所示，并按如下步骤执行。

步骤 1　当车辆 OBU_i 需访问车载自组网络资源时，车载终端先向路侧单元接入点 RSU_j 发送接入请求Join Request；

步骤 2　接入点 RSU_j 收到请求后生成一随机数 N_R，并连同接入点标识 RID_j 一起发送至车载终端；

步骤 3　车载终端收到信息后立即生成随机数 N_0，计算 $\mathrm{DID}_i = (N_0 \| \mathrm{PID}_i)^2 \bmod n$ 和凭证 $A_S = \mathrm{H}(K_i \| N_0 \| N_R)$，再生成会话秘密随机序列 S_{r1}，计算 $\mathrm{IS}_1 = S_{r1} \oplus A_S$，再将消息 $\mathrm{DID}_i \| \mathrm{IS}_1 \| N_0 \| \mathrm{RTA}^1_{\mathrm{OBU}}$ 发送至路侧接入点 RSU_j；

步骤 4　RSU_j 根据中国剩余定理并利用预存储的私钥 g 和 h 解密 DID_i 得到 4 个不同的解，再用随机数 N_0 匹配出最终解 PID_i，RSU_j 再用服务器公钥对 $\mathrm{PID}_i \| \mathrm{IS}_1 \| N_0 \| N_R$ 进行加密并发送至服务器；

步骤 5 服务器收到信息后用其私钥解密，并解密出 OBU_i 的真实身份 UID_i，服务器利用其检索注册表搜索出该用户对应密钥 K_i，计算 $A_S=\mathrm{H}(K_i \| N_0 \| N_R)$，$S_{r1}=\mathrm{IS}_1 \oplus A_S$，并对凭证设置期限 T_s，再生成随机数 N_A，用接入点 RSU_j 的公钥加密并向其发送 $\mathrm{E}_{\mathrm{RKU}}(S_{r1} \| T_s \| N_A)$；

步骤 6 RSU_j 收到信息后解密得到 S_{r1}，执行 DSSP 操作对挑战请求 $\mathrm{RTA}^1_{\mathrm{OBU}_i}$ 进行应答，再根据 S_{r1} 生成新的挑战请求 $\mathrm{RTA}^1_{\mathrm{RSU}_i}$，再发送 $\mathrm{ATA}^1_{\mathrm{RSU}_j} \| \mathrm{RTA}^1_{\mathrm{RSU}_j}$ 至 OBU_i；

步骤 7 车辆OBU_i对 $\mathrm{ATA}^1_{\mathrm{RSU}_j}$ 进行验证，再执行DSSP操作生成 $\mathrm{RTA}^1_{\mathrm{RSU}_j}$ 的应答序列 $\mathrm{ATA}^1_{\mathrm{OBU}_i}$；

步骤 8 RSU_j对 $\mathrm{ATA}^1_{\mathrm{OBU}_i}$ 进行验证，通过后即认证了用户身份的真实性，允许其访问该接入点资源，RSU_j再向服务器发送信息 $\mathrm{E}_{\mathrm{AKU}}(\mathrm{RID}_j \| N_{\mathrm{A}})$ 以便服务器端对用户注册表及时更新；

步骤 9 服务器对 $\mathrm{E}_{\mathrm{AKU}}(\mathrm{RID}_j \| N_A)$ 解密，更新该用户连接入网信息，其中包括认证凭证序列 A_S、当前接入的路侧单元标识 RID_j、时戳等。

3.3 切换认证阶段

该阶段同样由车载终端发起，具体流程如图 3 所示，并按下述步骤进行。

步骤 1 服务器根据预测模型，预先将车辆 OBU_i 的凭证信息 $\mathrm{E}_{\mathrm{RKu}}(\mathrm{PID}_i \| A_S \| T_S \| N_A)$ 发送至待切换路侧单元 RSU_{j+1}；

步骤 2 当车辆发起切换认证请求时，车载终

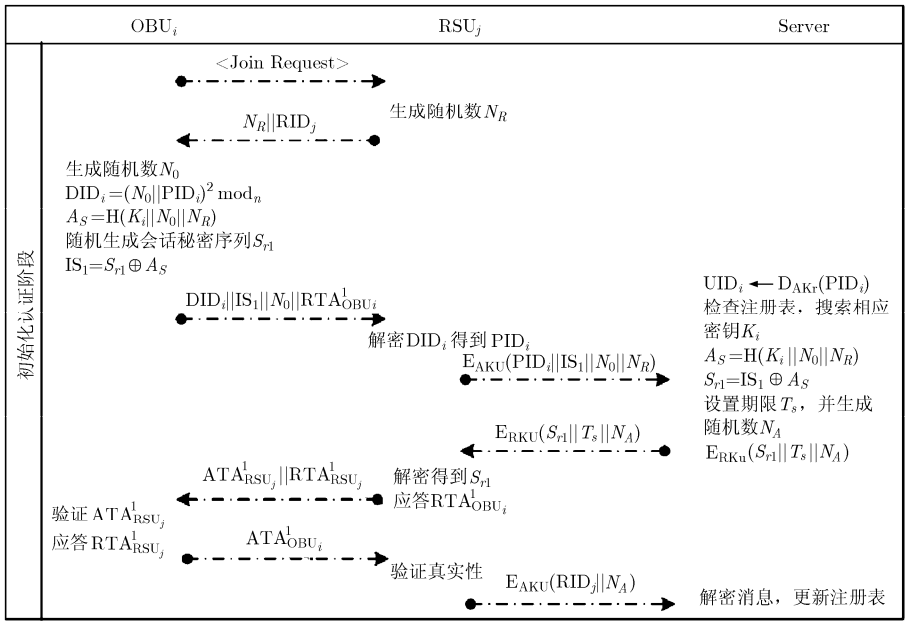

图 2 初始化认证流程

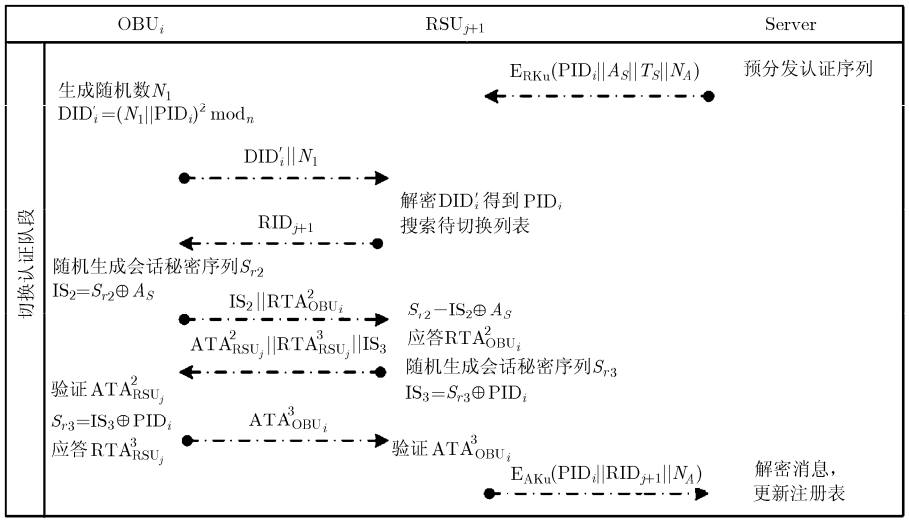

图 3 切换认证流程

端先生成新随机数N_1，计算$\mathrm{DID}_i^{'}=(N_1 \| \mathrm{PID}_i)^2 \bmod n$并将$\mathrm{DID}_i^{'} \| N_1$发送至新路侧单元$\mathrm{RSU}_{j+1}$；

步骤3　RSU_{j+1}收到切换请求后以前述同样方式先对$\mathrm{DID}_i^{'}$解密得到车载设备的伪标识PID_i，并依据其搜索待切换列表查阅是否有相应凭证序列，若有则回复其ID；

步骤 4　OBU_i收到新接入点标识符RID_{j+1}后生成新的随机会话秘密序列S_{r2}，计算$\mathrm{IS}_2=S_{r2} \oplus A_S$，再向该待接入点发送$\mathrm{IS}_2 \| \mathrm{RTA}_{\mathrm{OBU}_i}^2$；

步骤 5　RSU_{j+1}收到消息后利用待切换列表中对应的凭证A_S计算出$S_{r2}=\mathrm{IS}_2 \oplus A_S$，再执行DSSP操作对$\mathrm{RTA}_{\mathrm{OBU}_i}^2$进行应答生成$\mathrm{ATA}_{\mathrm{RSU}_j}^2$，新路测单元再随机生成新的会话秘密序列$S_{r3}$，计算$\mathrm{IS}_3=S_{r3} \oplus \mathrm{PID}_i$；将$\mathrm{ATA}_{\mathrm{RSU}_j}^2 \| \mathrm{RTA}_{\mathrm{RSU}_j}^3 \| \mathrm{IS}_3$一并发送至$\mathrm{OBU}_i$；

步骤 6　OBU_i收到消息后先对$\mathrm{ATA}_{\mathrm{RSU}_j}^2$进行验证，验证通过后再计算$S_{r3}=\mathrm{IS}_3 \oplus \mathrm{PID}_i$，执行DSSP 操作生成挑战请求$\mathrm{RTA}_{\mathrm{RSU}_j}^3$的应答序列$\mathrm{ATA}_{\mathrm{OBU}_i}^3$，并将其发送至$\mathrm{RSU}_{j+1}$；

步骤 7　RSU_{j+1}验证$\mathrm{ATA}_{\mathrm{OBU}_i}^3$的准确性，通过则允许该车载终端切换连接入网，再向服务器发送加密信息$\mathrm{E}_{\mathrm{AKu}}(\mathrm{PID}_i \| \mathrm{RID}_{j+1} \| N_A)$；

步骤 8　服务器解密消息，对该车辆和其接入点信息进行更新。

4　改进协议性能分析

本节从安全性、所需开销 2 个方面对现有协议和新协议进行分析比较。

4.1 安全性分析

假设攻击者具有如下能力：双向侦听、重放先前消息、冒充合法装置，此外本文同样假设车载终端的内存空间至少为 C 位(S_r：C_1 位，K：C_2 位，N_0：C_3位，N_R：C_4位)，哈希函数采用 SHA-1。此处分析总结了新方案抵御各种攻击行为的能力如下：

相互认证：新协议同样采用了挑战-应答的方式完成接入点和车载设备(用户)的相互认证，动态会话秘密序列的使用既简化了认证过程又隐藏了车载终端的认证凭证。协议中序列IS用于保护认证凭证，其中认证凭证包含两个元素：认证序列A_S和会话秘密序列S_r，由于S_r具有单次秘本属性，仅有合法的接入点和网络服务器才能从IS中分离出S_r，换言之，A_S和S_r在交互过程中已被直接隐藏，仅合法用户和路侧单元才能被彼此识别。

用户位置追踪隐患：对于用户或车载终端而言，虽然PID_i固定不变，但每次会话中消息内容$\mathrm{DID}_i \| \mathrm{IS}_1$，$\mathrm{DID}_i^{'}$均分别由新随机数$N_R$，$N_0$，$N_1$和新随机序列$S_{r1}$经过组合计算而得，同样$\mathrm{RTA}_{\mathrm{OBU}_i}^1$，$\mathrm{ATA}_{\mathrm{OBU}_i}^1$，$\mathrm{RTA}_{\mathrm{OBU}_i}^2$，$\mathrm{ATA}_{\mathrm{OBU}_i}^3$的生成均由新随机序列或随机数的参与计算而得，具有随机性和新鲜性，敌方无法通过上述信息对特定用户或终端进行跟踪，因此新协议对用户位置追踪实现了有效防护。

秘密会话序列猜测攻击：考虑到最坏情况下，认证过程中动态会话秘密序列使用的形式RTA为$\mathrm{RTA}=\{(r_i,q_i) \mid i=1 \sim L, L \le C_1/2, 1 \le r_i \le C_1, q_i=1\}$，每个应答序列ATA最多从序列$S_r$中选取$L$位元素，在认证过程中，路侧单元与车载终端根据序列$S_r$各进行挑战应答一次，若这两次挑战请求RTA中的元素r_i不重复，则攻击者在一次认证会话中能成功重构出会话序列S_r的概率为$1/L^2$。实际应用中，序列ATA长度可变，例如认证过程中车载终端和路侧单元所使用RTA序列的随机性决定了ATA的长度，因此敌方欲从单次认证过程获取完整的S_r序列非常困难。

共享密钥猜测攻击：假设攻击者获取了随机数N_0和N_R，由于其缺少共享秘钥K_i，其仍然无法从IS序列中分离出认证凭证A_S和会话序列S_r，即使攻击者足够幸运，知晓了共享秘钥K_i和动态会话序列S_r的长度，其计算出正确的密钥K_i平均需迭代复杂度为$2^{C_1} \cdot 2^{C_2}$次的计算时间。此外，若我们在实际应用中增加秘钥K_i和动态会话序列S_r的长度，敌方攻破密钥的复杂度也相应增大，因此，新协议同样提供了密钥抗破译的鲁棒性。

冒充攻击：一方面，初始化认证过程中，为成功冒充合法用户(合法车载终端)，攻击者需计算出有效的认证请求并正确应答出路侧单元的挑战请求，攻击者由于缺少用户标识信息无法计算出服务器端能识别的正确的伪标识PID_i，敌方也因缺少密钥K_i无法计算出正确的凭证A_S，同时，由于认证凭证由随机值的参与而构成，较短时间间隔中不易重复，另外在切换认证过程中，敌方因缺少伪标识PID_i信息，故无法从隐藏序列IS_3中提取出S_{r3}，无法回复正确的挑战应答$\mathrm{ATA}_{\mathrm{OBU}_i}^3$。故对于攻击者而言，若要冒充合法用户，其需同时满足两个条件：(1)敌方足够幸运能在单次认证过程中获取完整的S_r序列，(2)随机数N_R在较短时间内重复。因为N_R有2^{C_4}种可能，故上述条件难以成立；另外敌方缺少接入点和服务器的私钥g,h，RKr和AKr，故同样无法冒充路侧单元或服务器，因此新协议能抵御冒充攻击，同样也提供了防御侦听和重放攻击的保护。

平行会话攻击：原切换认证协议 LIAP 动态会话挑战应答过程中，为实现对方身份的识别，终端

和路侧单元均根据终端生成的会话序列发起挑战或应答，如此便造成平行会话攻击，而新协议中，路侧单元重新生成了新的动态会话序列S_{r3}，并根据其进行挑战提问，再将该序列与该终端伪标识PID_i异或形成消息隐藏序列IS_3，敌方即使将路测单元RSU_{j+1}的挑战提问$\mathrm{RTA}^3_{\mathrm{RSU}_{j+1}} \| \mathrm{IS}_3$转发至路侧单元$\mathrm{RSU}'_{j+1}$，路侧单元$\mathrm{RSU}'_{j+1}$收到挑战后将$\mathrm{IS}_3$与$A_S$异或形成错误的$S'_{r3}$，并做出错误的应答$\mathrm{ATA}^3_{\mathrm{RSU}'_{j+1}}$，敌方若再将其转发至原路侧单元$\mathrm{RSU}_{j+1}$，显然不能通过验证，如此便有效解决了平行会话攻击。

综上，本文又将新协议和现有典型的无线车载网络切换认证协议[9,11,15–17]就安全性及隐私保护进行比较如表 2 所示。经比较，仅文献[15～17]和本文所提协议在满足安全性需求的同时对终端匿名性、位置隐私提供了防护。

表 2 安全性能比较

安全性能	文献[11]	文献[15]	文献[16]	文献[17]	文献[9]	本文协议
双向认证	Y	Y	Y	Y	Y	Y
终端匿名性	×	√	√	√	√	√
终端位置隐私	×	√	√	√	×	√
条件隐私防护	×	√	√	√	√	√
重放攻击	√	√	√	√	√	√
冒充攻击	√	√	√	√	×	√
平行会话攻击	√	√	√	√	×	√

注：Y 表示提供；×表示不安全；√表示安全。

4.2 切换认证开销分析

此部分从车载终端内存开销、切换过程中通信开销以及切换延时 3 方面评估文献[9,14～17]与新协议的性能。为便于统一分析，文中设定随机数、随机数秘密序列、身份(伪)标识、哈希输出、共享密钥、证书、挑战请求及应答序列均为 160 bit，时间戳为 24 bit，公私钥均为 160 bit；有限域F_p上的超奇异曲线或非超奇异曲线E的阶q，p分别设为 512 bit 和 160 bit。

通信开销方面，实际应用中车载终端较服务器和路侧单元资源相对受限，因此本文侧重于比较车载终端收发数据包的大小。对比结果如表 3 所示，文献[17]通信开销最大，为 512000 B，文献[14]通信开销最小，仅为 100 B；本文切换认证协议由于使用DID_i隐藏了$\mathrm{metaUID}_i$、故增加N_1便于路侧单元解密，又在接入点 DSSP 应答环节增加了新会话序列IS_3以防平行会话攻击，车载终端通信开销为180B，低于文献[16～17]，较 LIAP 协议增加了 40 B，但考虑到新协议在安全性及隐私方面的优势，增加的些许开销是可以接受的。

终端内存开销方面，首先，LIAP 及本文协议只使用了哈希函数和随机数生成算法，而文献[14～17]相比之下还需分别存储基于椭圆曲线的双线性映射函数、变色龙哈希函数、双陷门变色龙哈希函数等算法，因此终端存储开销更大[18]；再者，为便于分析，此部分比较终端所存储的公共参数、共享密钥、预计算结果、证书、以及服务器公钥等切换过程较重要的信息，各协议终端存储开销如表 3 所示。文献[15～17]由于需存储基于椭圆曲线密码体制的公共参数[11]、服务器公钥以及终端用户证书等信息，所需内存空间均不低于 100 B。而文献[14]采用预配置阶段加载一组不可链接伪标识对的方法，伪标识对由标量乘计算而得，根据上述参数假设，存储一个伪标识对就需 3220 B，存储m个伪标识对就需$(3220m)$ B，因此该方案终端内存空间需求随着伪标识对数量的增加而线性增长。相比 LIAP 协议，新协议中车载终端多存储了一个公共参数n，因此比 LIAP 协议稍高 20 B，为 60 B，但相比前述几种方案节省了较多空间。

表 3 切换认证开销比较

协议	OBU_i通信开销(B)	OBU_i内存开销(B)	OBU_i计算开销	RSU_{j+1}计算开销	总计算开销	切换延时(ms)
文献[14]	100	$(140+3220m)$	1Pair+3H	1Pair+3H	2Pair+6H	18.118
文献[15]	160	100	$2\mathrm{P_M}$+1Pair+1H	$2\mathrm{P_M}$+1Pair+1H	$4\mathrm{P_M}$+2Pair+2H	31.414
文献[16]	256	160	1EN+1DE+1Pair+2H	1EN+1DE+1Pair	2EN+2DE+2Pair+2H	37.196
文献[17]	512000	120	$2\mathrm{P_M}$	$3\mathrm{P_M}$	$5\mathrm{P_M}$	16.760
文献[9]	140	40	--	1DE+1EN	1DE+1EN	9.595
本文	180	60	1 $\mathrm{M_M}$	$1\mathrm{M_R}$+1DE+1EN	$1\mathrm{M_M}$+$1\mathrm{M_R}$+1DE+1EN	14.972

注：$\mathrm{P_M}$(点乘)，Pair(双线性映射)，H(哈希)，$\mathrm{M_M}$(模乘)，$\mathrm{M_R}$(模开方)，EN(AES 加密)，DE(AES 解密)，--(忽略)，m(伪标识对数量)

切换延时方面，本文仅考虑计算相对较耗时的双线性映射、点乘、模乘、模开方等运算，而忽略随机数生成、模加/减、异或、移位比较等轻量级计算。基于开源标准密码库 MIRCAL[20]，仿真环境为：Intel Core i3-2.27 GHz, RAM-2 GB；由于每次运行时间有细微差异，故测试 20 次取平均值。点乘运算耗时约为 3.352 ms，双线性映射耗时约为 8.975 ms, AES 加密耗时 1.102 ms, AES 解密耗时为 8.493 ms，模乘运算耗时约为 1.896 ms，模开方运算约为 3.481 ms，哈希运算约为 0.028 ms，评估各协议认证延时如表 3 中所示，相较其他文献，LIAP 协议中车载终端只使用了随机数生成、异或、移位比较等轻量级运算，新路侧单元只需执行一次加/解密操作即可，故其切换认证延时最小，仅为 9.595 ms，文献[14~17]由于进行了多次复杂运算，认证耗时均超过 15 ms，而新协议相比 LIAP 协议只增加了模乘、模开方运算各一次，计算耗时为 14.972 ms。综上，所提方案在增强系统安全性、隐私保护的同时并未增加太多开销，相比现有大多文献，切换认证速度更快。

5　结束语

本文分析介绍了现有无线网络切换认证协议的特点及设计要求，并指出现有车载网络切换认证协议中存在的高认证延时和安全隐患难以确保实际应用中的通信服务质量和安全性需求，迫切需要构建一个低开销、安全快速的切换认证协议。基于此，本文又详细分析了 LIAP 协议的不足之处，在此基础上提出了一个改进的基于动态会话过程的切换认证协议，不仅实现了车载终端、路侧单元和后端服务器的相互认证，提高了终端使用者的隐私防护，同时也满足无线网络中登录、快速切换过程中的所有安全需求。相比现有大多切换协议，改进协议兼具隐私防护和低认证延时的优点，因此，实用性更好。

参 考 文 献

[1] LEE J H and BONNIN J M. HOTA: Handover optimized ticket-based authentication in network-based mobility management[J]. *Information Sciences*, 2013, 230(5): 64–77. doi:10.1016/j.ins.2012.11.006

[2] JIA X D, CHANG Y F, ZHANG Z Z, *et al*. A critique of a lightweight identity authentication protocol for vehicular network[J]. *Journal of Information Hiding and Multimedia Signal Processing*, 2015, 6(3): 183–188.

[3] YANG X, HUANG X, HAN J, *et al*. Improved handover authentication and key pre-distribution for wireless mesh networks[J]. *Concurrency and Computation*: *Practice and Experience*, 2015, 42(9): 621–628. doi: 10.1002/cpe.3544.

[4] XIAO P, HE J, and FU Y. An access authentication protocol for trusted handoff in wireless mesh networks[J]. *Computer Standards & Interfaces*, 2014, 36(3): 480–488.

[5] CHOI H H. Ad hoc cooperative vertical handover for next-generation heterogeneous networks[J]. *AEU-International Journal of Electronics and Communications*, 2015, 69(10): 1557–1561.

[6] HE D, CHEN C, CHAN S, *et al*. Secure and efficient handover authentication based on bilinear pairing functions[J]. *IEEE Transactions on Wireless Communications*, 2012, 11(1): 48–53.

[7] TSAI J L, LO N W, and WU T C. Secure handover authentication protocol based on bilinear pairings[J]. *Wireless Personal Communications*, 2013, 73(3): 1037–1047.

[8] YEO S L, YAP W S, LIU J K, *et al*. Comments on "analysis and improvement of a secure and efficient handover authentication based on bilinear pairing functions"[J]. *IEEE Communications Letters*, 2013, 17(8): 1521–1523.

[9] LI J S and LIU K H. A lightweight identity authentication protocol for vehicular networks[J]. *Telecommunication Systems*, 2013, 53(4): 425–438.

[10] JURCUT A D, COFFEY T, and DOJEN R. Design guidelines for security protocols to prevent replay & parallel session attacks[J]. *Computers & Security*, 2014, 45(6): 255–273.

[11] ZHANG Y, CHEN X, LI J, *et al*. Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks[J]. *Computer Networks*, 2014, 75(12): 192–211. doi:10.1016/j.comnet.2014.10.009.

[12] HE D, BU J, CHAN S C, *et al*. Handauth: efficient handover authentication with conditional privacy for wireless networks[J]. *IEEE Transactions on Computers*, 2013, 62(3): 616–622.

[13] WANG W and HU L. A secure and efficient handover authentication protocol for wireless networks[J]. *Sensors*, 2014, 14(7): 11379–11394.

[14] HE D, CHAN S, and GUIZANI M. Handover authentication for mobile networks: security and efficiency aspects[J]. *Network*, 2015, 29(3): 96–103.

[15] YEH L Y and HUANG J L. PBS: a portable billing scheme with fine-grained access control for service-oriented vehicular networks[J]. *IEEE Transactions on Mobile Computing*, 2014, 13(11): 2606–2619.

[16] WU H T, YEIN A D, and HAIEH W S. Message authentication mechanism and privacy protection in the context of vehicular Ad Hoc networks[J]. *Mathematical Problems in Engineering*, 2015, 501(12): 1–11.

[17] GUO S, ZENG D, and XIANG Y. Chameleon hashing for secure and privacy-preserving vehicular communications[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2014, 25(11): 2794–2803.

[18] CAO J, LI H, MA M, *et al*. A simple and robust handover authentication between HeNB and eNB in LTE networks[J]. *Computer Networks*, 2012, 56(8): 2119–2131.

[19] LI G, JIANG Q, WEI F, *et al*. A new privacy-aware handover authentication scheme for wireless networks[J]. *Wireless Personal Communications*, 2015, 80(2): 581–589.

[20] SHAMUS SOFTWARE LTD. Miracllibrary[OL]. http://www.shmus.ie/index.php?pages=home,2012.

周治平：　男，1962 年生，博士，教授，研究领域为检测技术与自动化装置、信息安全等.

张惠根：　男，1990 年生，硕士生，研究领域为物联网安全认证.

孙子文：　女，1968 年生，博士，教授，研究领域为无线传感器网络理论与技术，信息隐藏、模式识别与图像处理等.

李　静：　女，1992 年生，硕士生，研究领域为检测技术与自动化装置.