doi:10.3969/j.issn.1000-436x.2014.11.017

# 新的车辆远程诊断授权协议

焦政达，马建峰，孙聪，姚青松
(西安电子科技大学 计算机学院，陕西 西安 710071)

**摘 要**：诊断主体授权问题是车辆远程故障诊断中的关键问题。针对当前车辆远程诊断授权协议（PVAUDS）中存在的问题，提出了新的车辆远程诊断授权协议（PVAUDS+）。在保证原协议安全目标的前提下，为诊断主体提供双向认证和票据新鲜性验证，并保证发送票据的可信第三方能够有效抵御拒绝服务攻击。使用安全协议证明工具 ProVerif 对 PVAUDS+协议的安全属性进行自动化证明，通过增加发起代价的机制解决对可信第三方的拒绝服务攻击问题，从而说明 PVAUSD+协议能够满足提出的安全目标。定量分析结果说明本协议具有较好的可行性。

**关键词**：安全协议；车辆远程诊断；授权；协议自动化证明
**中图分类号**：TP393.0; TP918.1 **文献标识码**：A **文章编号**：1000-436X(2014)11-0146-08

# New remote authorization protocol for vehicle diagnosis

JIAO Zheng-da, MA Jian-feng, SUN Cong, YAO Qing-song
(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

**Abstract:** The authorization of diagnosis principals is a critical problem in the remote fault diagnosis of vehicles. Considering the defects of the previous authorization protocol for the remote diagnosis, i.e. PVAUDS, a novel authorization protocol is proposed, named PVAUDS+. In addition to the enforcement on the security properties of PVAUDS, the bidirectional authentication and the freshness of authorization tickets for the diagnosis principals are provided. The resistance of Denial-of-Service (DoS) attack for the trusted third party is also provided. The proposed security targets are achieved through the cost increasing of requests for the resistance of DoS attack, the automatic proof of security properties with the ProVerif tool. The results of quantitative analysis show proposed protocol is practical for use.

**Key words:** security protocol; remote vehicle diagnosis; authorization; automatic proof of protocol

## 1 引言

随着经济的发展和社会的进步，路网通行能力已无法满足日益增长的交通需求，并成为世界各国所面临和必须解决的重大问题。智能交通系统（ITS, intelligent transportation system）已经成为国际公认解决上述交通问题的根本途径，它的功能包括减少出行时间、保障交通安全、缓解交通拥挤、减少交通污染 4 个方面，其最终目标是建立一个实时、准确、高效的交通运输管理系统。智能交通系统越来越受到国内外政府、专家、学者的重视。

车辆远程故障诊断作为智能交通中保障交通安全的一部分，是汽车诊断技术未来的发展方向。

当前在车辆远程故障诊断方面的研究分为故障诊断系统和远程诊断通信 2 个方面。典型的远程诊断通信包含了汽车（V, vehicle）、诊断设备（DE,

收稿日期：2014-08-22；修回日期：2014-10-24
基金项目：国家自然基金委员会—广东联合基金重点基金资助项目（U1135002）；国家自然科学基金资助项目（61303033）；陕西省自然科学基础研究计划基金资助项目（2013JQ8036）；中央高校基本科研业务费专项资金资助项目（JB140309）；航空科学基金资助项目（2013ZC31003, 20141931001）
**Foundation Items:** The Key Program of NSFC-Guangdong Union Foundation (U1135002); The National Natural Science Foundation of China (61303033); The Natural Science Basis Research Plan in Shaanxi Province of China (2013JQ8036); The Fundamental Research Funds for the Central Universities (JB140309); The Aviation Science Foundation of China (2013ZC31003, 20141931001)

diagnostic equipment）、后端系统（BS, back-end system）以及连接它们的任意形式的网络。后端系统通常由车辆的生产厂商拥有和维护，其中存放了诊断所需的参数信息，例如车辆的配置参数或车载软件版本。在进行诊断时，诊断设备从生产商后端系统中检索出被诊断车辆必要的信息，向车辆的通信控制单元（CCU, communications control unit）发起连接请求。建立连接后诊断设备向车辆通信控制单元发出诊断请求，车辆通信控制单元再向车内不同的电子控制单元（ECU, electronic control unit）发送诊断命令，在确定故障后进行远程故障消除。

在诊断通信中需要解决的一个重要问题为验证通信方身份的合法性并授权。针对这一问题的一种典型解决方案是通过引入发送授权票据的可信第三方（TTP, trust third parties）来提供有效的身份认证，从而对可信主体进行诊断授权。TTP 可以是车辆生产厂商、维修商或者是被某组织授权的第三方部门。在这一框架下，远程诊断系统的通信主体包括 DE、V、TTP、BS 和连接它们的任意网络，其中 DE 和 V 为诊断主体，发放的票据使合法的诊断主体在诊断会话中持有有效的共享密钥。在基于 TTP 的诊断通信授权框架下，Kleberger 和 Olovsson 提出了一种防止车辆遭受非授权会话的授权协议，简称为 PVAUDS（protecting vehicles against authorized diagnostics sessions）协议[1]。该协议方案虽然提供了车辆对诊断设备的单向认证和票据的机密性、完整性、抗抵赖性保证，但忽略了诊断设备对车辆身份的认证、对接收票据新鲜性的判断以及对可信第三方的有效保护。

针对 PVAUDS 协议存在的安全隐患，本文提出了一种新的车辆诊断授权协议，在保护车辆的同时，对诊断设备和可信第三方进行有效的保护，以达到以下 4 项安全目标。

1) 通信主体间能够进行身份的相互认证；

2) 诊断主体能对票据的新鲜性进行判断；

3) 可信第三方能够保证票据有效、及时地发放；

4) 票据内容的机密性、完整性和抗抵赖性。

本文通过一阶定理证明工具 ProVerif 对新协议进行形式化描述和安全性证明，并对协议的性能进行定量分析和比较，说明了协议能够在合理的开销下实现以上安全目标。

## 2　相关工作

车辆的远程诊断技术已经成为汽车维护和发展的必然趋势，也成为智能交通体系中重要的一环，近年来，该领域受到越来越多的关注。例如，Jhou 等[2]提出通过对第二代车载诊断系统（OBD-II, on board diagnostics-II）、3.5G 无线网络和云计算技术进行整合来对车辆进行实时监控和故障诊断的方法。Chen 等[3]提出使用车载单元（OBU, on board unit）和车辆诊断服务器（VDS, vehicle diagnostics server）来构成一个线上的实时车辆故障检测和预期评估系统。OBU 将采集的数据经无线网络传送至 VDS，再由 VDS 中的专家系统对数据进行分析来进行诊断。针对诊断设备，Ashraf Tahat 等[4]提出使用蓝牙技术将车辆数据传输给基于安卓的移动设备，该设备再通过移动网络将数据传给车辆维护部门完成数据的分析和诊断。何金儿等[5]设计并制作了基于 GPS/GPRS 的数据采集及预处理车载远程诊断系统，上述的研究工作都致力于诊断系统的设计。

针对车辆诊断通信过程中的安全问题，目前的研究主要集中在通信消息的安全性以及对诊断主体的授权问题。在通信消息的安全性研究方面，Idrees 等[6]提出了通过在硬件安全模块（HSM, hardware security module）中存储通信密钥来实现车辆诊断的安全通信。Nilsson 等[7]提出了一种使用散列链的车辆诊断通信协议，用于诊断过程中对车内防火墙的安全更新。在诊断主体授权研究方面，Pierre 等[1]提出了基于 TTP 框架的远程车辆诊断授权协议，该方法对诊断主体实现了单向认证并保障了通信消息的安全性，但缺乏诊断主体的双向认证、消息新鲜性的验证以及对 TTP 的有效保护。针对目前的研究工作所暴露的问题，本文提出的新车辆远程诊断协议旨在提供通信消息安全性，并在此基础上实现诊断主体的双向认证、对接收票据信息的新鲜性验证以及对 TTP 的有效保护，完成对诊断主体的授权。

## 3　PVAUDS 协议及其存在的问题

在 Kleberger 和 Olovsson 提出的 PVAUDS 协议中，采用基于可信第三方的授权机制。协议的通信主体包括了诊断设备（DE）、被诊断车辆（V）以及可信第三方（TTP），其中诊断设备（DE）和被诊断车辆（V）为诊断主体。由于实际情况中，诊

断设备已经预先配置了可信第三方的信息，故可省略诊断用于设备请求可信第三方信息的后端系统（BS）。该协议的交互过程如图 1 所示，其中符号的含义在表 1 中说明。

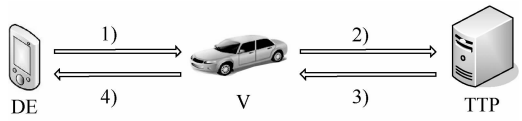



图 1 PVAUDS 协议示意

1) DE→V: $\mathrm{Cert_{DE}}||\mathrm{Cert_{TTP}}$

2) V→TTP: $\mathrm{Cert_{DE}}||\mathrm{Enc_{TTP}}(\mathrm{V_{ID}}||\mathrm{nonce_V})$

3) TTP→V: $\mathrm{Enc_V}(\mathrm{Ticket_V}||\mathrm{nonce_V})$
$||\mathrm{Enc_{DE}}(\mathrm{Ticket_{DE}})$

$\mathrm{Ticket_{DE}}=\{K_{\mathrm{DE,V}},\Delta t,\mathrm{V_{ID}},\mathrm{Sign_{DE}}(K_{\mathrm{DE,V}}||\Delta t||\mathrm{V_{ID}})\}$

$\mathrm{Ticket_V}=\{K_{\mathrm{DE,V}},\Delta t,\mathrm{V_{ID}},\mathrm{Sign_V}(K_{\mathrm{DE,V}}||\Delta t||\mathrm{V_{policy}})\}$

4) V→DE: $\mathrm{Enc_{DE}}(\mathrm{Ticket_{DE}})$

**表 1 协议描述符号说明**

| 符号 | 含义 |
|---|---|
| $\mathrm{Cert}_X$ | 通信主体 $X$ 的数字证书 |
| $\mathrm{Sign}_X$ | 使用 $X$ 的私钥进行的签名操作 |
| $\mathrm{Enc}_X$ | 使用 $X$ 的公钥进行的加密操作 |
| $\mathrm{nonce}_X$ | 通信主体 $X$ 生成的随机挑战 |
| $\mathrm{Ticket}_X$ | 经过 TTP 签名的发送给 $X$ 的票据 |
| $K_{X,Y}$ | 诊断主体 $X$、$Y$ 之间的共享密钥 |
| $\Delta t$ | 票据的生成时间 |
| $\mathrm{V_{ID}}$ | 车辆的身份标识 |
| $\mathrm{V_{policy}}$ | 车辆诊断的安全策略 |

该协议中，DE 首先向 V 发送自身的数字证书以及诊断所需 TTP 的数字证书。V 对所接收证书验证无误后生成一个随机挑战 $\mathrm{nonce_V}$ 以及身份标识 $\mathrm{V_{ID}}$，用 TTP 的公钥加密后连同 DE 的数字证书一同发送至 TTP，与此同时 V 会启动时钟以防收到 TTP 返回的延迟信息。此后，TTP 对收到的信息进行解密，验证无误后生成经 TTP 签名的加密票据 $\mathrm{Ticket_V}$ 以及 $\mathrm{Ticket_{DE}}$ 发送至 V。其中 $\mathrm{Ticket_V}$ 包含了 V 和 DE 用于通信的共享密钥 Key、密钥生成时间 $\Delta t$ 以及诊断策略 $\mathrm{V_{policy}}$，$\mathrm{V_{policy}}$ 用以告知 V 接收哪些诊断命令。$\mathrm{Ticket_{DE}}$ 为经过 TTP 签名的向 DE 发送的票据，其内容包含了 V 和 DE 用于通信的共享密钥 Key、密钥生成时间 $\Delta t$ 以及用来识别诊断车辆的 $\mathrm{V_{ID}}$。最后，V 将收到的经加密的 $\mathrm{Ticket_{DE}}$ 发送至 DE。

上述协议专注于对诊断车辆的保护，而忽略了对诊断设备和可信第三方的保护，因而存在以下安全问题。

1) 协议没有提供诊断主体间的双向认证以及对票据新鲜性的判断。即存在可能的重放攻击，使 DE 无法判断从 V 得到的票据是否新鲜。这源自于 DE 在消息 4 中接收到的信息不包含 V 的身份认证以及时效性验证（$\Delta t$ 仅描述了生成票据的时间差）。

2) 没有对任务繁重的票据发送方提供有效保护。即 TTP 无法抵御来自 V 的拒绝服务（DoS, denial of service）攻击。TTP 的提供者具有多样性，可为车辆生产厂商、维修商或者被某组织授权的第三方部门，因而 TTP 的性能存在差异。在上述协议的第 2 步中，敌手可以轻松获得 $\mathrm{V_{ID}}$ 和 nonce 以及 TTP 的公钥，而消息 3 中，TTP 需要进行共享密钥的生成、$\Delta t$ 的计算、$\mathrm{V_{policy}}$ 的获取以及签名、非对称加密计算。故攻击者可以利用消息 2 对 TTP 进行 DoS 攻击，导致一些性能较弱的 TTP 最终失效。

以上安全问题都会导致 DE 无法获取有效的票据信息，从而无法对车辆进行及时的诊断操作，使得正在行驶的车辆存在安全隐患。

## 4 PVAUDS+协议及形式化描述

本节将介绍一种新的车辆远程诊断授权协议，称为 PVAUDS+协议。本节还将使用应用 PI 演算（applied PI calculus）对协议进行的形式化描述，以便于使用自动化工具进行安全性证明。

### 4.1 PVAUDS+协议

鉴于 PVAUDS 协议暴露的安全问题，本文提出一种新的车辆诊断授权协议，即 PVAUDS+协议。PVAUDS+协议可表述如下

1) DE→V: $\mathrm{Cert_{DE}}||\mathrm{Cert_{TTP}}||\mathrm{nonce_{DE}}$

2) V→TTP: $\mathrm{Enc_{TTP}}(\mathrm{V_{ID}}||\mathrm{nonce_V})$

3) TTP→V: $\mathrm{Enc_V}(\mathrm{nonce_V}||\mathrm{puzzle})$

4) V→TTP:$\mathrm{Cert_{DE}}||\mathrm{Enc_{TTP}}(\mathrm{V_{ID}}||\mathrm{solution}||\mathrm{nonce_{V2}})$

5) TTP→V: $\mathrm{Enc_V}(\mathrm{Ticket_V}||\mathrm{nonce_{V2}})$
$||\mathrm{Enc_{DE}}(\mathit{Ticket}_{\mathrm{DE}})$

$\mathrm{Ticket_{DE}}=\{K_{\mathrm{DE,V}},\Delta t,V_{\mathrm{ID}},\mathrm{Sign_{DE}}(K_{\mathrm{DE,V}}||\Delta t||\mathrm{V_{ID}})\}$

$\mathrm{Ticket_V}=\{K_{\mathrm{DE,V}},\Delta t,V_{\mathrm{ID}},\mathrm{Sign_V}(K_{\mathrm{DE,V}}||\Delta t||\mathrm{V_{policy}})\}$

6) V→DE: $\mathrm{Enc_{DE}}(\mathrm{Ticket_{DE}})||K_{\mathrm{V,DE}}(\mathrm{nonce_{DE}},\mathrm{DE})$

该协议通过嵌入以下安全机制实现第 1 节中提出的 4 个安全目标。针对安全目标 2，新的协议在 DE 和 V 的通信中增加挑战-响应机制来解决票据新鲜性验证的问题，即在消息 1 中加入了 DE 的随机

挑战 $nonce_{DE}$。针对安全目标 1，消息 6 中使用该轮会话 $Ticket_V$ 中的共享密钥 $K_{DE,V}$ 对随机挑战 $nonce_{DE}$ 进行对称加密操作，保证 DE 对 V 的身份进行验证；针对安全目标 3，本文应用增加发起代价的策略来防止对可信第三方进行的 DoS 攻击，即在 TTP 接收到 V 的请求后首先发送给 V 一个 client-puzzle 问题来应对原协议面临的 DoS 问题，如消息 3，4 所描述，其中具体的 client-puzzle 问题将在 5.2 节中说明。

本文协议与 PVAUDS 协议的区别与联系如表 2 所示，表中的安全目标（T1～T4）对应第 1 节所列 4 个安全目标。

**表 2　PVAUDS 与 PVAUDS+的区别与联系**

| 安全目标 | PVAUDS | PVAUDS+ | 新协议增加机制 |
|---|---|---|---|
| T1 | × | √ | 挑战-响应/对称加密 |
| T2 | × | √ | 挑战-响应 |
| T3 | × | √ | client-puzzle |
| T4 | √ | √ | — |

## 4.2　PVAUDS+协议的形式化描述

本节使用应用 PI 演算对 PVAUDS+进行形式化描述。应用 PI 演算是自动化证明工具 ProVerif[8,9]的输入语言，使用应用 PI 演算对协议进行的形式化描述将用于 ProVerif 工具对安全属性的自动化证明。

ProVerif 是基于 Dolev-Yao 模型，用 Prolog 规则实现的形式化自动验证密码学协议工具。它能够形式化地描述各种密码学原语，包括：对称和非对称加密、数字签名、单向散列函数、bit 级承诺（bit-commitment）以及非交互零知识证明[10]。该工具能够对通信主体或信息的可达性、一致性断言、可观察等价性进行证明，从而实现对安全和身份认证属性的分析。ProVerif 证明器以应用 PI 演算描述的协议作为输入，将协议的 PI 演算描述转换为一阶逻辑规则，应用这些规则对用户提出的安全属性进行推理，得出安全属性是否满足的结论。若证明出协议不满足某一安全属性，该工具将返回一条攻击的迹（trace），用来说明存在的安全隐患。

### 4.2.1　形式化描述的前提

在描述协议主体之前，需对协议的通信主体、安全性假设以及密码学函数等进行定义。通信信道为公共信道，用于通信主体之间进行消息传送，包括敌手在内的任何人均可获取、篡改信道上的信息。

协议中用于对明文和密文进行操作的函数主要包括对称加/解密函数 senc/sdec、非对称加/解密函数 aenc/adec、签名函数 sign 以及签名的验证函数 checksign。函数功能之间的关系可简要归结为

$$\mathrm{sdec}(\mathrm{senc}(m, kY), kY) = m$$
$$\mathrm{adec}(\mathrm{aenc}(m, sskY), spkY) = m$$
$$\mathrm{checksign}(\mathrm{sign}(m, sskY), spkY) = m$$

其中，$kY$ 为对称密钥，$spkY/sskY$ 表示主体 $Y$ 的公/私钥对，$m$ 为消息。

与数字证书相关的操作主要包括证书生成函数 mkcert 及验证函数 checkcert。函数功能之间的关系可简要归结为

$$\mathrm{checkcert}(\mathrm{mkcert}(I), spkCA) = I$$

其中，$I$ 代表证书内容，$spkCA$ 为 CA 公钥。

### 4.2.2　协议的主体描述

本节对协议通信主体（DE、V、TTP）以及通信主过程进行形式化描述。

1) 诊断设备 DE 的过程描述

在协议消息 1 中，DE 生成随机挑战 Nde，连同自身证书 certDE 和 TTP 证书 certTTP 一起作为诊断请求信息发送给 V

out($c$, (certDE, certTTP, Nde))

在协议消息 6 中，DE 从 V 接收加密的票据 $x1$ 和用共享密钥加密的随机挑战 $x2$，对加密的票据 $x1$ 使用私钥 $skDE$ 解密得到 TicketDE，使用 TTP 的私钥 $skpTTP$ 验证 TicketDE 的签名并得到共享密钥 $k$，然后用 $k$ 解密 $x2$ 并验证主体标识 DE 和消息 1 中发送的随机挑战 Nde

let TicketDE = adec($x1$, $skDE$) in
checksign(TicketDE, $spkTTP$) in
let (Nde, DE) = sdec($x2$, $k$) in…

2) 车辆 V 的过程描述

在协议消息 1 中，V 获取 DE 发送的数字证书（包括 DE 证书 certDE 和 TTP 证书 certTTP）以及 DE 在消息 1 中发送的随机挑战 Nde，用 CA 公钥 $spkCA$ 对证书进行解析验证后发送请求连接消息

in($c$, (certDE, certTTP, Nde))
checkcert(certDE, $spkCA$)in
checkcert(certTTP, $spkCA$) in …

在协议消息 2 中，V 生成随机挑战 Nv，连同车辆标识 $v$ 经 TTP 公钥 $pkTTP$ 加密后发送至 TTP

out($c$, (aenc(($v$, Nv), $pkTTP$)))

在协议消息 3 中，V 接收到一个来自 TTP 的包含 client-puzzle 问题的消息 $m3$，使用 V 的私钥 $skV$

解密后验证在消息 2 中发送的 Nv 并得到 client-puzzle 问题

let(Nv, puzzle) = adec(*m*3, *skV*) in…

在协议消息 4 中，V 向 TTP 发送由 TTP 公钥 *pkTTP* 加密并包含 DE 证书 certDE 的票据请求消息，该消息的加密部分包含通过散列函数生成 client-puzzle 问题的解、车辆标识 *v*、V 生成的随机挑战 Nv2。

let solution = hash(puzzle) in

out(*c*, (certDE, aenc((*v*, solution, Nv2), *pkTTP*)))

在协议消息 5 中，V 接收由 TTP 发来的加密的 DE 票据 TicketDE 和自身票据 *x*，对自身票据 *x* 用 *skV* 解密得到 TicketV 和在消息 4 中发送的 Nv2。V 验证在消息 4 中发送的 Nv2 并用 TTP 的公钥 *spkTTP* 验证签名，验证无误后得到共享密钥

in(*c*, (*x*, TicketDE))

let(TicketV,Nv2)=adec(*x*, *skV*) in

checksign(TicketV, *spkTTP*) in…

在协议消息 6 中， V 向 DE 发送由共享密钥 k 加密并包含 TicketDE 的消息，该消息的加密部分包含在协议消息 1 中接收的 Nde、主体标识 DE。

out(*c*, (TicketDE, senc((Nde,DE),*k*)))

3) 可信第三方 TTP 的过程描述

在协议消息 2 中，TTP 接收来自 V 的请求连接信息 *m*2，经私钥 *skTTP* 解密得到随机挑战 Nv 和车辆标识 *v*

let ( *v*, Nv) = adec(*m*2, *skTTP*) in …

为了应对 DoS 问题，TTP 生成一个 client-puzzle 问题 puzzle，将该问题连同在消息 2 中接收的随机挑战信息 Nv 经 V 公钥 *pkV* 加密后向 V 发送（即协议消息 3），同时开始计时。

out(*c*, aenc((Nv, puzzle), *pkV*))

若在预设的时间 *T* 内没有得到 V 的反馈，协议终止。否则，在协议消息 4 中，TTP 接收来自 V 的票据请求信息，该信息包含 DE 证书 certDE 和密文 *m*4。TTP 使用 CA 公钥 *spkCA* 对 DE 证书进行验证，并使用自身私钥 *skTTP* 解密 *m*4，解密后得到随机挑战 Nv2、车辆标识 *v* 及 puzzle 的解 solution。最后使用散列对 solution 进行验证

checkcert(certDE, *spkCA*) in

let (*v*, solution, Nv2 ) = adec(*m*4, *skTTP*) in

if solution = hash(puzzle) then…

验证成功后，TTP 生成经自身私钥 *sskTTP* 签名的 DE 和 V 对应的票据 TicketDE 和 TicketV，票据内容包含共享密钥 *k*、票据生成时间 *dt*、以及 DE 和 V 各自所需的车辆标识 *v* 和安全策略 *p*。

let TicketV = sign((*k*, *dt*, *p*), *sskTTP*) in

let TicketDE = sign((*k*, *dt*, *v*), *sskTTP*) in…

在协议消息 5 中，TTP 将由 V 公钥 *pkV* 加密的 TicketV 和随机挑战 Nv2，连同由 DE 公钥 *pkDE* 加密的 TicketDE 发送给 V。

out(*c*,(aenc((TicketV,Nv2),*pkV*), aenc(TicketDE, pkDE)))

4) 主过程的形式化描述

通信主过程将各主体和 CA 的公钥 *spkY* 发布至信道上，然后，用 mkcert 函数生成各主体的数字证书 certY 并发布至信道上

let certY = mkcert(…) in

out(*c*, certY)

最后，启动各主体过程

((!processDE(…))|(!processV(…))

|(!processTTP(…)))

## 5 安全性分析

针对第 1 节提出的 4 个安全目标，本节对 PVAUDS+协议的安全性进行分析。由于票据中数字签名的使用，票据的完整性和抗抵赖性能够得到保证，证书的使用确保了证书接收者能够对证书发送者的身份进行确认。以下对安全目标中通信主体的身份认证、票据新鲜性、机密性以及抗 DoS 能力进行分析。并为通信主体和共享密钥定义安全属性质疑（query）。最后，通过工具对安全属性质疑进行推导，得出安全性结论。

### 5.1 协议的 ProVerif 验证

在使用 ProVerif 进行安全性证明之前，首先要对新协议的关键事件进行描述，本节定义 4 个事件来说明协议执行时的关键点，分别为 V 发送票据请求事件（VsendRequest）、TTP 密钥生成事件（createKey）、V 接收票据事件（VacceptsKey）以及 DE 接收票据事件（DEacceptsKey）。

本节首先将关键事件添加到通信主体的形式化描述过程之中，以描述事件之间的对应性[11]，然后通过质疑语句来验证协议的安全属性。

#### 5.1.1 安全属性描述

本节描述 4 种安全属性，分别记为 Q1~Q4。其中，Q1 描述认证过程中诊断主体与 TTP 之间的身

份确认；Q2 描述诊断主体 V 对票据新鲜性的判断；Q3 描述诊断主体 DE 对票据的新鲜性以及对票据转发者 V 身份的判断；Q4 描述对票据机密性的保护。

Q1：满足 DE 和 V 对于 TTP 的认证。即在 DE 和 V 均执行了相应的接收事件之前，应满足 TTP 已经执行过密钥生成事件 createKey。其对应性可由质疑语句描述为

query
event(VacceptsKey(…))&&
event(DEacceptsKey(…))⇒
event(createKey(…))

由于 ProVerif 并不支持上述的对应性描述，故根据文献[10]的方法，引入辅助过程 ProcessQ、事件 termProto 以及表 Vmess、DEmess 来描述该安全属性，其中的 $k$ 和 $k'$表示两表中分别存储的密钥，操作 get T 表示读取表 $T$ 的内容。

event termProto(...)
query event(termProto(...))⇒ $k = k'$
let processQ = ! get DEmess(...) in
get Vmess(...) in
event termProto(...)

Q2：对于诊断主体 V，应保证接收到票据的新鲜性。亦即，在 V 执行事件 VacceptKey 之前，TTP 已执行过事件 createKey，且事件之间的对应性需满足单射（inj-event）关系

query
inj-event(VacceptsKey(...))⇒
inj-event(createKey(...))

Q3：对于诊断主体 DE，需保证与 Q2 描述一致的新鲜性同时需保证对 V 的身份认证。即 DE 在执行 DEacceptKey 之前，TTP 需执行事件 createKey，且满足单射关系

query
inj-event(DEacceptsKey(...))⇒
inj-event(createKey(...))

Q4：需要对共享密钥的机密性进行验证。在第 4.2.2 节中对 V 过程描述的最后，用 V 得到的共享密钥对预先定义的消息 $s$ 加密，并将其发送至信道。通过对 $s$ 进行机密性质疑描述（attacker），验证共享密钥的机密性

query attacker($s$)

#### 5.1.2　验证结果

ProVerif 工具对于安全属性的验证结果如表 3 所示。Q1 的结果表明 DE 和 V 能够对 TTP 的身份进行确认，即满足第 1 节的安全目标 1；Q2 的结果表明在 V 每次接收票据之前，TTP 能够进行唯一的票据生成，即存在着一对一的请求和响应关系，这保证了 V 所接收票据的新鲜性，即满足第 1 节的安全目标 2。由于 DE 接收的票据是由 TTP 生成经 V 转发给 DE，Q3 的验证结果表明 DE 和 TTP 之间能够进行一对一的请求和响应，亦保证了 DE 所接收票据的新鲜性以及对 V 的身份验证，满足第 1 节中的安全目标 1 和 2。Q4 的验证结果表明敌手无法获取经共享密钥加密后的明文信息，即满足第 1 节的安全目标 4。

**表 3　ProVerif 验证结果**

| 安全属性 | 工具内部描述 | 验证结果 |
|---|---|---|
| Q1 | Query event(termProto($h$_2114,V[],$k$_2115,$m$_2116, $h$_2114,V[],$k$'$m$_2116)⇒ $k$_2115=$k$' | true |
| Q2 | Query inj-event (VacceptsKey ($k$_11418, $v$_11419, $d$_11420, $p$_11421, $N$_11422))⇒ inj-event(creatKey ($k$_11418, $v$_11419, $d$_11420, $p$_11421, $N$_11422)) | true |
| Q3 | Query inj-event (DEacceptsKey ($k$_9569, $v$_9570, $d$_9571, Nde_9574, $ht$_9575))⇒ inj-event(createKey ($k$_9569, $v$_9570, $d$_9571, $p$_9572, $N$_9573)) | true |
| Q4 | Query not attacker_bitstring($s$[]) | true |

### 5.2　抵抗 DoS 攻击能力

DoS 攻击通常通过向服务提供方发出的大量请求信息耗尽服务资源，以达到阻止或延迟向授权用户提供服务的效果。出于 TTP 能力的多样化以及在 PVAUDS 协议中消息 2、3 之间计算资源不平衡的原因，本文在 PVAUDS+协议中引入了增加发起代价的解决机制，应对存在的 DoS 攻击。

PVAUDS+协议使用一种基于散列函数的 client-puzzle 问题来增加 V 发起票据请求的代价，TTP 可通过控制 client-puzzle 问题的难易程度以及设定可容忍的解答时间 $T$ 来应对不同强度的 DoS 攻击。client-puzzle 问题可描述为：TTP 生成一个长度为 $L$ 的值 $a$，记做 $a$<1, $L$>，并使用 2 次散列运算产生 $\theta$=hash($\lambda$)，其中 $\lambda$=hash(TTP, $a$<1,$L$>)。将 $\theta$ 和 $a$ 的后($L-k$)位，即 $a$<$k$+1, $L$>，发送给 V 作为 puzzle，V 得到问题后求解 $a'$<1, $k$>从而满足式(1)。

$$\text{hash}(\text{TTP}, a'\langle 1, k\rangle \| a\langle k+1, L\rangle)=\lambda \tag{1}$$

由于散列函数是单向的，所以对 puzzle 的求解只能通过暴力测试来解决，这大大增加了请求方的发起代价，使攻击者的攻击行为变得代价昂贵且低效，从而实现对 DoS 攻击的有效抵抗。因此新协议能够满足第 1 节的安全目标 3。

## 6 协议的性能分析

本节介绍 PVAUDS+协议中使用的具体 client-puzzle 方法以及建议的加密策略。分析了 client-puzzle 问题的计算代价以及新协议的计算开销。

### 6.1 client-puzzle 的代价分析

根据 5.2 节中提出的 client-puzzle 问题，对于求解 $a$<1, $k$>，该 client-puzzle 问题的搜索空间大小为 $2^k$，票据请求者平均需要进行 $2^{k-1}$ 次的计算，最多需要 $2^k$ 次的计算。假设车载计算机一次 hash 运算的时间为 $t$，则求解一个 client-puzzle 问题的总耗时平均为 $2^{k-1}t$。根据 Andreas 等在文献[12]中提供的实验环境，得到在 $k$ 变化的情况下，TTP 的验证和 V 的解答时间如表 4 所示。

**表 4 client-puzzle 计算开销**

| $k$ 所选长度/bit | TTP 验证时间/ms | V 解答时间/ms |
|---|---|---|
| 8 | 0.29 | 0.874 |
| 16 | 0.237 | 29.841 |
| 24 | 0.243 | 5 380.862 |

从表 4 中的数据可以看出随着 $k$ 值的增大，client-puzzle 问题的解答时间成指数倍增长。假设 $k$ 的值从 $a$ 增大至 $b$，在时间段 $T$ 内 TTP 接收的成功请求数为 $m$，则攻击者若想成功发动 $m$ 次请求则要求其计算能力需要平均增加 $2^{b-a}$ 倍，这使攻击者的攻击行为变得代价昂贵且低效，从而实现对 DoS 攻击的有效抵抗。

### 6.2 协议计算开销

根据协议的通信过程，表 5 列出了 PVAUDS 和 PVAUDS+协议中通信主体相对耗时操作的计算次数，而忽略散列、对称加密等计算开销较小的运算。本文建议协议使用椭圆曲线密码系统（ECC，elliptic curve cryptosystem），并选用 ECDSA-192 算法进行票据签名和验证，选用 ECDSA-256 算法进行主体证书的生成和验证。

由表 5 可知，通信主体 DE 的计算开销并没有变化，下面对票据发送方 TTP 的计算开销和 V 的计算开销分别进行分析。本文引入单位 MMs（modular multiplications）来表示 1 024 位模乘计算量，而 ECC 中点积运算的计算量约 29 MMs[13]。计算得签名操作需消耗 29 MMs；验证签名消耗 145 MMs；证书的验证消耗 203 MMs；加密操作为 58 MMs；解密操作为 29 MMs[14,15]。根据表 5 得出 PVAUDS+中 TTP 的总计算开销 493 MMs，在原 PVAUDS 协议中 TTP 的计算开销为 406 MMs；对于票据接收方 V 来说，新协议 PVAUDS+计算开销为 725 MMs+$T_{\text{puzzle}}$，其中 $T_{\text{puzzle}}$ 为解答 client-puzzle 问题的耗时，PVAUDS 协议中 V 的计算开销为 638 MMs。

由以上的计算数据得出，在 PVAUDS+协议中，可信第三方 TTP 的计算开销增加了 21.4%，这是由于本文对 PVAUDS 协议的安全属性进行了扩充，因此使协议的通信内容增加。相对于增加的安全性而言，21.4%的计算开销增长比例是可以接受的。同时在实际情况中，相对于车辆而言，可信第三方 TTP 的性能更为重要，因此 V 增加的开销并不会对车辆远程诊断授权过程的整体运行造成明显影响。

## 7 结束语

本文选取车辆远程诊断授权通信中的授权协议安全性作为研究对象，在对已有协议进行安全缺陷分析的基础上，提出新的车辆远程诊断授权协议 PVAUDS+。针对提出的安全目标使用工具 ProVerif 进行自动化证明并分析协议的抗 DoS 能力，说明了协议满足所提出的安全目标。对协议性能的定量分

**表 5 计算开销对比**

| 协议名称 | 通信主体 | 加密/解密 | 签名/验证 | 证书/验证 | Puzzle | 计算开销 |
|---|---|---|---|---|---|---|
| PVAUDS | TTP | 2/1 | 2/0 | 1 | 0 | 493 MMs |
| | V | 1/1 | 0/1 | 2 | 0 | 638 MMs |
| | DE | 0/1 | 0/1 | 0 | 0 | 174 MMs |
| PVAUDS+ | TTP | 3/2 | 2/0 | 1 | 0 | 406 MMs |
| | V | 2/2 | 0/1 | 2 | 1 | 725 MMs+$T_{\text{puzzle}}$ |
| | DE | 0/1 | 0/1 | 0 | 0 | 174 MMs |

析说明新协议在车辆远程诊断授权通信中是可行的。

随着被诊断车辆数的不断增加，在保障车辆远程诊断安全性的前提下，如何提高诊断授权的通信效率将成为今后研究的发展趋势。在此趋势下，针对本文提出的协议，未来工作包括使用公认标准的 ECC 加密算法对协议的计算和通信开销进行评价并优化；研究在 DoS 攻击抵御机制中，如何确定 client-puzzle 问题的合理难度以使通信双方获得最优效率；讨论车辆远程诊断授权中证书传递的必要性，进一步优化协议的通信开销。

## 参考文献：


[1] PIERRE K, TOMAS O. Protecting vehicles against unauthorized diagnostics sessions using trusted third parties[A]. SAFECOMP 2013[C]. 2013.70-81.

[2] JHENG S J, CHEN S H. The implementation of OBD-II vehicle diagnosis system integrated with cloud computation technology[A]. RVSP 2013[C]. 2013.9-12.

[3] CHEN S H, WANG J F, WEI Y R. The implementation of real-time on-line vehicle diagnostics and early fault estimation system[A]. The Fifth International Conference on Genetic and Evolutionary Computing[C]. 2011.13-16.

[4] ASHRAF T, AHMAD S, FOUAD J, *et al*. Android-based universal vehicle diagnostic and tracking system[A]. Consumer Electronics(ISCE)[C]. 2012.137-143.

[5] 何金儿, 朱守正, 张长伟. 一种新的车辆远程诊断系统的设计和实现[J]. 计算机应用与软件, 2012, 29(9): 95-97.
HE J E, ZHU S Z, ZHANG C W. Design and implementation of a new car remote diagnostic system[J]. Computer Applications and Software, 2012, 9(9): 95-97.

[6] MUHAMMAD S I, HENDRIK S, YVES R, *et al*. Secure automotive on-board protocols: a case of over-the-air firmware updates[J]. Nets4Trains/Nets4Cars, 2011, 6596: 224-238.

[7] DENNIS K. NILSSON, ULF E. LARSON: secure firmware updates over the air in intelligent vehicles[A]. IEEE International Conference on Communications Workshops (ICC Workshops)[C]. 2008.380-384.

[8] DANNY D, ANDREW C, YAO. On the security of public key protocols[A]. IEEE Transactions on Information Theory[C]. 1983.198-208.

[9] BRUNO B. An efficient cryptographic protocol verifier based on prolog rules[A]. Computer Security Foundations Workshop[C]. 2001. 82-96.

[10] BLANCHET B, SMYTH B, CHEVAL V. ProVerif 1.87: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial[M]. 2013.

[11] 冯登国. 安全协议: 理论与实践[M]. 北京:清华大学出版社, 2011.
FENG D G. The Theory and Practice of Security Protocol[M]. Beijing: Tsinghua University Press, 2011.

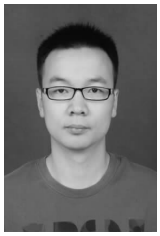
[12] ANDREAS G, SIMON O. Analysis of the client puzzles protocol[A]. KTH Computer Science and Communication[C]. 2012.

[13] ALEKSANDAR J, ALFRED J, MENEZES. Elliptic curves and cryptography[A]. Puhlic-key cryptography[C]. 2005.91-112.

[14] SCOTT M. Efficient implementation of cryptographic pairings [EB/OL]. http://ecryptss07.rhul.ac.uk/Slides/Thursday/ mscottsamos07.pdf, 2007.

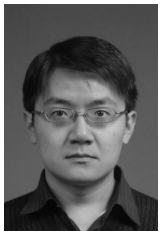
[15] CALANDRIELLO G, PAPADIMITRATOS P, HUBAUX J P, *et al*. Efficient and robust pseudonymous authentication in VANET[A]. Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET'07)[C]. 2007.19-28.


## 作者简介：

**焦政达**（1990-），男，河南洛阳人，西安电子科技大学硕士生，主要研究方向为网络与信息安全。

**马建峰**（1963-），男，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线和移动安全、系统可生存性等。



**孙聪**（1982-），男，陕西兴平人，博士，西安电子科技大学副教授，主要研究方向为信息流安全、程序分析与验证。

**姚青松**（1982-），男，湖北松滋人，博士，西安电子科技大学讲师，主要研究方向为网络安全、隐私保护。