# 车载软件安全更新智能小车

一. 成果完成人及所在单位： 胡秋燕，计算机与信息工程学院 指导教师：谢勇

## 二. 成果简介：

以智能小车为研究对象，将开源框架 Uptane 框架和国密 SM 系列算法相结合。在大量网联车辆适用平台进行调研的基础上，选择了搭载树莓派 4B 的智能小车平台。先后在计算机、智能小车平台实现基于 Uptane 框架的 OTA 更新基本功能，本平台嵌入国密 SM 系列算法，以及在车端和服务端都安装数字证书。保障车辆安全更新中车辆认证，文件加密传输，本都文件加密等条件。最后课题对嵌入国密算法后的框架，对安全性、内存资源消耗、计算效率等方面进行评估。得出了国密系列算法更加符合该框架，国密算法不仅安全性更高，在计算效率和内存资源占用上更优的结论。验证了在车端实现 OTA 安全更新的可行性。这项研究对提高 OTA 安全更新的安全性和计算效率做出一定贡献。

## 三. 主要研究内容及创新点：

针对搭载树莓派的智能小车（见图 1）为研究对象，建立了基于 Uptane 框架的车载软件安全更新框架；采用搭载了树莓派的智能小车平台，应用 Uptane 开源框架，在框架的基础上设计更新安全机制（见图 2），以及嵌入国密 SM 系列算法，对框架在安全性能、计算效率、内存资源占用等方面设计实验进行分析。得出了国密系列算法更加符合该框架，国密算法不仅安全性更高，在计算效率和内存资源占用上更优的结论；根据实验结果以及大量调查研究，研究结果指出，在车端是实现 OTA 安全更新切实可行，且推荐使用国密系列算法提高安全性。

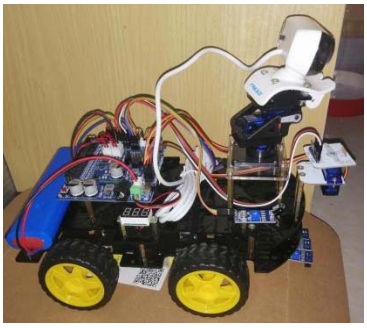


图 1 智能小车展示图

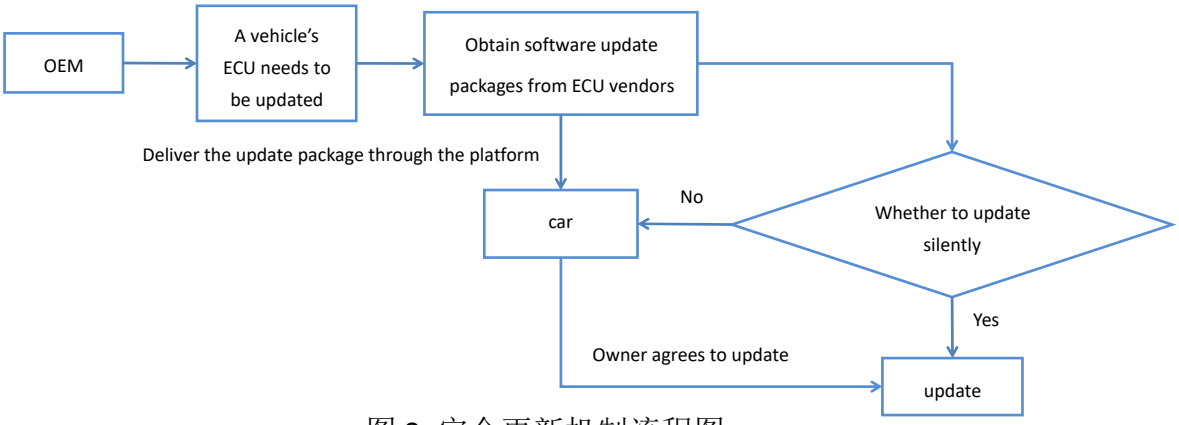



图 2 安全更新机制流程图

## 四. 主要研究成果及应用情况

网联车辆实验平台一个；待发表论文一篇

联系人：胡秋燕， 电 话：15058213632 Email:huqiuyan1996@163.com