基于国密技术的智能网联汽车软件升级模型设计*

黄俊隆 陈积常 朱雪平** 李建

南宁学院信息工程学院，南宁 530200

摘 要 深入分析智能网联汽车软件升级所面临的网络安全风险，评估风险可能带来的危害，构建一种基于国密技术的智能网联汽车软件升级模型，使用 SM2、SM3、SM4 等国家商用密码算法技术设计了软件升级安全通信协议。并对协议进行了安全性分析，分析结果表明协议能够有效地抵御黑客发动的主动攻击、被动攻击，以及在通信中间方（基站）被黑客控制的情况下，仍能实现软件升级信息安全传输的功能。实验结果验证了协议的有效性和可行性。

关键字 智能网联汽车；软件升级模型；商用密码算法；PKI 技术

Design of Software Upgrade Model for Intelligent Connected Vehicles Based on National Security Technology

Huang junlong Cheng Jichang Zhu Xue Ping Li Jian

School of Information Engineering of Nanning University
Nanning 530200, China

Abstract--A thorough analysis of the network security risks faced by intelligent connected vehicles during software upgrades was conducted, the potential harm caused by these risks was evaluated, and a software upgrade model for intelligent connected vehicles based on national encryption technology was constructed. The SM2, SM3, and SM4 national commercial encryption algorithms were used to design a secure communication protocol for software upgrades. The protocol was then subjected to a security analysis, which showed that the protocol could effectively defend against active and passive attacks launched by hackers, as well as ensure secure information transmission even if the communication intermediary (base station) was controlled. The experimental results validated the effectiveness and feasibility of the protocol.

Keywords--intelligent connected vehicles, software upgrade model, commercial cryptography algorithms, PKI technology

1 引 言

随着 5G 通信、人工智能、大数据、云计算等技术的高速发展，汽车不再局限于交通的功能，用户对于汽车有了更高要求，进而订阅更多服务，传统汽车逐步向智能网联汽车(Intelligent Connected Vehicle,ICV)转变。智能网联汽车时代，软件已逐步发展成为汽车的核心竞争力[1]。智能网联汽车软件关系着汽车乃至人民生命安全。网联汽车软件升级过程极易遭受黑客攻击，如何保障网联汽车软件升级安全，是急需研究的重要课题。

针对网联汽车软件升级过程中的传输效率与传输安全问题，文献[2]基于 POSIX 接口的软件升级管理器来实现 OTA 主节点无感化升级，减少了软件包升级传输所需的时间；文献[3]通过对汽车软件升级技术进行分析，提出 OTA 升级中的安全要求以及 OTA 能力建设建议。文献[4]使用 SM2、SM3、SM4 等商用算法，设计了车车、车路的通信方案，为后续研究者提供了参考。

国外方面，对于密码算法方面，在 70 年代，美国确立了国内的 DES 加密标准[5]。而后数年，国外分别产生了 AES、NESSIE 等密码算法，国外密码算法发展势头迅猛。而在远程升级（OTA）方面，日本先后出台和修订了相关文件，将其作为用车改装技术的应用[6]。在自动驾驶方面，美国众议院批准《自动驾驶法案（提案）》，赋予 NHTSA 专职负责自动驾驶网络安全的权利[7]。

本文基于研究现状，分析网联汽车软件升级风险，提出网联汽车软件升级模型功能需求，构建网联汽车软件安全升级模型，设计网联汽车软件安全升级协议，通过工程实现进一步表明协议的安全性与有效性。

*基金资助：本文得到南宁学院教学质量与教学改革工程项目《网络安全》核心课程（2022BKHXK09）和南宁学院一流专业培育项目（2020YLZYPY01）资助。

**通讯作者：朱雪平，125989168@qq.com 。

2 软件升级模型安全需求分析

2.1 安全风险分析

在信息化高速发展时代，汽车厂商为满足用户智能化需求，需要对网联汽车进行软件升级，而网联汽车软件升级过程中，也面临如下的安全风险：

（1）信息泄露：黑客通过攻击信息传输过程企图获得各方的相关数据，信息泄露会导致后续各种灾难；

（2）数据篡改：通过篡改信息流程中的信息来植入相关病毒，如软件升级包被篡改并植入病毒，进而获得汽车的控制权；

（3）数据重放：黑客在某方通信过程中截取信息，并向接收方发送老旧信息从而使接收方判断错误，进而达到相关目的；如黑客对发往汽车终端的升级包进行数据重放，发放更早版本的升级包来进行汽车软件“降级”，从而产生各种问题；

（4）通信业务否认：黑客对数据包进行破坏，并将已损数据包发往汽车终端，事后否认该数据来源于自身，从而规避法律追责；

（5）网络传输威胁：包括手机 APP 与 TSP(Telematics Service Provider,远程信息处理服务提供者)平台通信、TSP 平台与 T-BOX 通信、V2X 通信、汽车与充电桩通信过程中的信息监听和窃取、信息伪造等[8]；

（6）数据漏发、错发：在远程升级过程中，车联网平台的运营因功能众多而变得复杂，运维配置不当可能导致车辆信息报送漏发、错发数据等风险[9]。

2.2 模型安全性需求分析

（1）身份鉴别：在进行汽车软件升级包发送前，需进行总服务器、基站、汽车终端三方身份鉴别，确保身份真实、互相信任，能使通信得到进一步的安全保障；

（2）数据完整性和机密性：在信息的传输过程中，信息数据的完整和机密性是通信安全最基本的需求，保障传输的数据不被篡改和滥用；

（3）信息新鲜性和实时性：为了防止黑客在软件升级过程中实施重放攻击，需在通信中引入时间戳和随机数来确保信息的新鲜性。即通信三方也可根据时间戳或者随机数来判断信息是否处在一个正确的时间范围，以此来判断是否遭到重放攻击。

（4）信息传输不可否认性和可追溯性：为了防止软件升级过程中，收发双方否认信息传输，使用数字签名来保障信息传输不可否认；

3 智能网联汽车软件升级模型

3.1 软件升级流程架构

智能网联汽车软件升级模型由服务器、网络基站和车辆终端组成。其升级模型架构如图 1 所示。

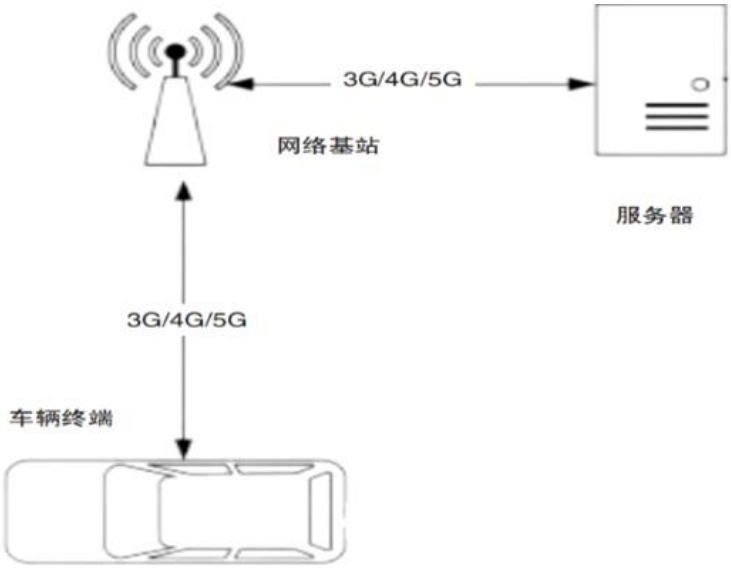

图 1 软件升级流程架构[10]

具体过程如下：

（1）构建数字证书机构（CA），为服务器、网络

基站、车辆终端三方通信端颁发数字证书，为三方通信提供信任基础；

（2）通信三方进行身份鉴别，达到三方互相信任；

（3）服务器将软件升级包发送至基站，由基站转发至车辆终端。

3.2 软件升级模型关键数据

（1）软件升级包数据是整个传输过程中最重要的数据之一，若软件升级包数据遭到窃取，黑客可通过植入病毒数据进升级包的方式来对汽车进行攻击，一旦汽车不慎安装含有病毒的升级包，黑客则可进一步控制汽车；

（2）身份信息、公私钥对等数据；

4 升级软件包传输流程

4.1 网联汽车软件升级流程协议

表 1 协议中所使用符号解释

符号	说明
IDi	服务器 i 的身份
IDj	网络基站 j 的身份
IDk	汽车终端 k 的身份
T	时间戳
H	杂凑值
||	拼接符号
Ex[Y]	用 x 对 Y 进行加密
Dx[Y]	用 x 对 Y 进行解密
PKi	服务器 i 用 SM2 算法的公钥
PKk	汽车终端 k 用 SM2 算法的公钥
Upgradepackages	软件升级包
sessionkey	SM4 密钥

根据软件升级流程架构，汽车软件远程升级过程涉及服务器 i、网络基站 j 及汽车终端 k 三家，基于国家商用密码算法、数字证书、数字签名、密钥管理技术设计汽车软件远程升级协议如图 2 所示，其中的符号如表 1 所示。

4.2 智能网联汽车软件远程升级协议解析

(1) $ID_i||ID_j||T_1||E_{SKi}[H(ID_i||ID_j||T_1)]||\{PK_i||ID_i||T_2||E_{SKCA}[H(PK_i||ID_i||T_2)]\}$

总服务器 i 向基站 j 发送身份信息 IDi、时间戳 T_1、数字签名 $E_{SKi}[H(ID_i||ID_j||T_1)]$以及 CA 签发的总服务器 i 的证书$\{PK_i||ID_i||T_2||E_{SKCA}[H(PK_i||ID_i||T_2)]$。

(2)网络基站 j 对总服务器 i 进行身份鉴别：

①基站 j 用 CA 的公钥值来鉴别服务器 i 证书的真实性：

$H_1=D_{PKCA}\{E_{SKCA}[H(PK_i||ID_i||T_2)]\}=H(PK_i||ID_i||T_2)$

基站 j 通过信息计算哈希值 H_2：

$H_2=H(PK_i||ID_i||T_2)$

判断 H_1 与 H_2 是否相等，若相等，则可确认该证书是 CA 签发的有效证书，若不等，则无法确认是 CA 签发的有效证书。

②基站 j 使用总服务器 i 的公钥来验证总服务器 i 的签名：

$H_3=D_{PKi}\{E_{SKi}[H(ID_i||ID_j||T_1)]\}=H(ID_i||ID_j||T_1)$

基站 j 通过信息计算哈希值 H_4：

$H_4=H(ID_i||ID_j||T_1)$

判断 H_3 与 H_4 是否相等，若相等，则可确认该消息是由总服务器 i 发送，若不等，则无法确认该消息是由总服务器 i 发送。

(3) $ID_j||ID_i||T_3||E_{SKj}[H(ID_j||ID_i||T_3)]||\{T_4||ID_j||PK_j||E_{SKCA}[H(T_4||ID_j||PK_j)]\}$

基站 j 向服务器 i 发送身份信息 IDj、时间戳 T_3、数字签名及服务器 i 的证书。

(4)同步骤（2），总服务器 i 先鉴别基站 j 的证书再验证其签名。

(5) $ID_i||ID_j||ID_jverifyID_k||T_5||E_{SKj}[H(ID_i||ID_j||ID_jverifyID_k||T_5)]$

服务器 i 向基站 j 发送身份信息 ID_i、时间戳 T_5、数字签名，要求基站 j 与汽车终端进行相互身份认证。

(6)基站 j 判断总服务器 i 的真伪：

③基站 j 使用服务器 i 的公钥来验证服务器 i 的签名：

$H_9=D_{PKi}\{E_{SKi}[H(ID_i||ID_j||ID_jverifyID_k||T_5)\}=H(ID_i||ID_j||ID_jverifyID_k||T_5)$

基站 j 通过信息计算哈希值 H_{10}：

$H_{10}=H(ID_i||ID_j||ID_jverifyID_k||T_5)$

判断 H_9 与 H_{10} 是否相等。

(7) $ID_j||ID_k||T_6||E_{SKj}[H(ID_j||ID_k||T_6)]||\{T_4||ID_j||PK_j||E_{SKCA}[H(T_4||ID_j||PK_j)]\}$

基站 j 向汽车终端 k 发送身份信息、时间戳、数字签名以及 CA 签发的基站 j 的证书。

(8)同（2）（4）步骤，汽车终端 k 先鉴别基站 j 的证书再验证签名。

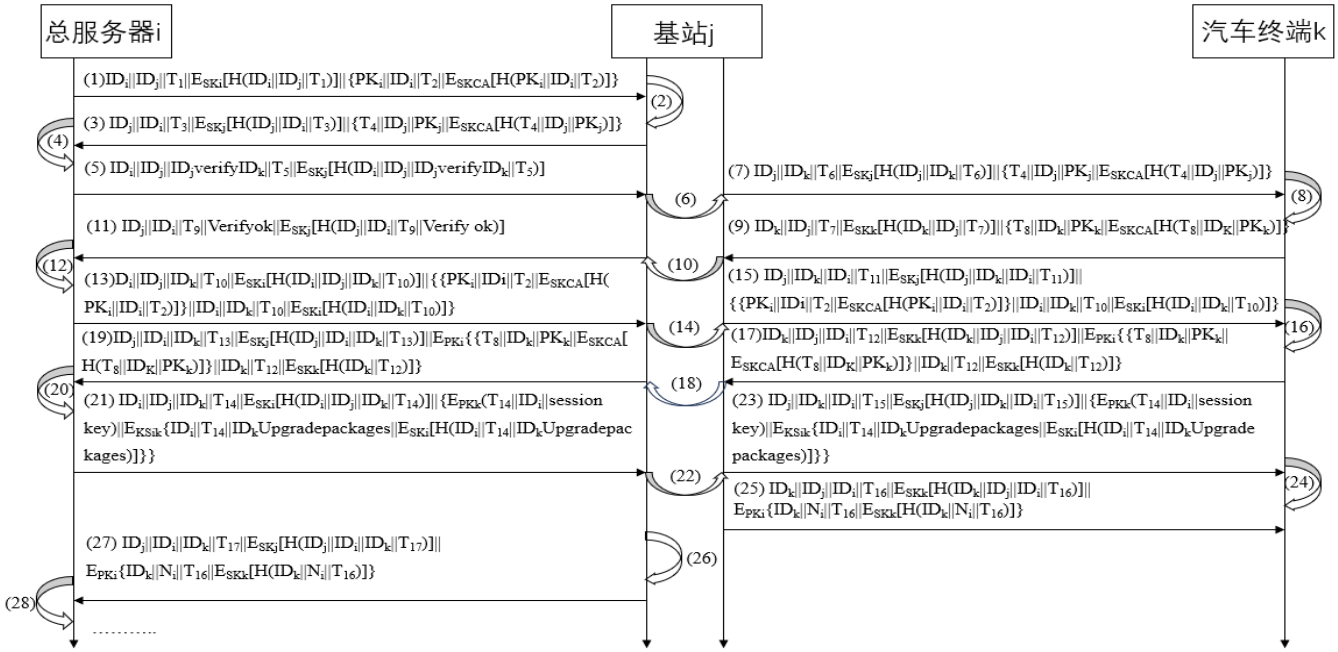

图 2　智能网联汽车软件升级安全协议

(9) $ID_k||ID_j||T_7||E_{SKk}[H(ID_k||ID_j||T_7)]||\{T_8||ID_k||PK_k||E_{SKCA}[H(T_8||ID_K||PK_k)]\}$

汽车终端 k 向基站 i 发送身份信息、时间戳、数字签名以及 CA 签发的汽车终端 k 的证书。

(10)同步骤（2）（4）（8），基站 j 先鉴别汽车终端 k 的证书再验证签名。

(11) $ID_j||ID_i||T_9||Verifyok||E_{SKj}[H(ID_j||ID_i||T_9||Verifyok)]$

基站 j 向服务器 i 发送身份信息、时间戳、数字签名及告知服务器 i 已完成与汽车终端 k 的相互验证。

(12)同步骤（6），服务器 i 验签基站 j，从而了解其已与汽车终端 k 完成身份鉴别；

(13) $ID_i||ID_j||ID_k||T_{10}||E_{SKi}[H(ID_i||ID_j||ID_k||T_{10})]||\{\{PK_i||IDi||T_2||E_{SKCA}[H(PK_i||ID_i||T_2)]\}||ID_i||ID_k||T_{10}||E_{SKi}[H(ID_i||ID_k||T_{10})]\}$

服务器 i 向基站 j 发送身份、时间戳、数字签名、压缩包以及告知基站 j 该消息发往汽车终端 k。

(14)基站 j 接收总服务器 i 发来的消息并判断消息的真伪及服务器 i 的意图：

④基站 j 使用服务器 i 的公钥验证签名：

$H_{21}=D_{PKi}\{E_{SKi}[H(ID_i||ID_j||ID_k||T_{10})]\}=H(ID_i||ID_j||ID_k||T_{10})$

基站 j 通过信息计算哈希值 H_{22}：

$H_{22}=H(ID_i||ID_j||ID_k||T_{10})$

判断 H_{21} 与 H_{22} 是否相等。

⑤基站 j 从信息 ID_k 中判断此信息中的压缩包要发往汽车终端 k。

(15) $ID_j||ID_k||ID_i||T_{11}||E_{SKj}[H(ID_j||ID_k||ID_i||T_{11})]||\{\{PK_i||IDi||T_2||E_{SKCA}[H(PK_i||ID_i||T_2)]\}||ID_i||ID_k||T_{10}||E_{SKi}[H(ID_i||ID_k||T_{10})]\}$

基站 j 向汽车终端 k 发送信息，信息包含身份信息、时间戳、数字签名及由总服务器 i 发来的压缩包。

(16)同步骤（2）（4）（8）（10），汽车终端 k 先验签基站，然后鉴别总服务器 i 的证书以及验证其签名。

(17) $ID_k||ID_j||ID_i||T_{12}||E_{SKk}[H(ID_k||ID_j||ID_i||T_{12})]||E_{PKi}\{\{T_8||ID_k||PK_k||E_{SKCA}[H(T_8||ID_K||PK_k)]\}||ID_k||T_{12}||E_{SKk}[H(ID_k||T_{12})]\}$

汽车终端 k 向基站 j 发送信息，包含身份信息、时间戳、数字签名及以总服务器 i 公钥加密的压缩包。

(18)同步骤（14），基站 j 在验签成功汽车终端 k 后，对其余信息进行转发；

(19) $ID_j||ID_i||ID_k||T_{13}||E_{SKj}[H(ID_j||ID_i||ID_k||T_{13})]||E_{PKi}\{\{T_8||ID_k||PK_k||E_{SKCA}[H(T_8||ID_K||PK_k)]\}||ID_k||T_{12}||E_{SKk}[H(ID_k||T_{12})]\}$

基站 j 向总服务器 i 发送信息。

(20)同步骤（16），服务器 i 先验签基站 j，再使用私钥解密，从而鉴别汽车终端 k 证书以及验证签名。

(21) $ID_i||ID_j||ID_k||T_{14}||E_{SKi}[H(ID_i||ID_j||ID_k||T_{14})]||\{E_{PKk}(T_{14}||ID_i||sessionkey)||E_{KSik}\{ID_i||T_{14}||ID_kUpgradepackages||E_{SKi}[H(ID_i||T_{14}||ID_kUpgradepackages)]\}\}$

服务器 i 向基站 j 发送信息。

(22)同步骤（14），基站 j 在验签总服务器 i 后进行数据的转发。

(23) $ID_j||ID_k||ID_i||T_{15}||E_{SKj}[H(ID_j||ID_k||ID_i||T_{15})]||\{E_{PKk}(T_{14}||ID_i||sessionkey)||E_{KSik}\{ID_i||T_{14}||ID_kUpgradepackages||E_{SKi}[H(ID_i||T_{14}||ID_kUpgradepackages)]\}\}$

基站 j 向终端 k 发送身份信息、数字签名等信息。

(24) ⑥同步骤（6），汽车终端 i 接收基站 j 发来的消息并判断消息的真伪；

⑦汽车终端 k 以自己的私钥解密压缩包：

$D_{SKk}\{E_{PKk}(T_{14}||ID_i||sessionkey)||E_{KSik}\{ID_i||T_{14}||ID_kUpgradepackages||E_{SKi}[H(ID_i||T_{14}||ID_kUpgradepackages)]\}\}=\{(T_{14}||ID_i||session\ key)||$

$E_{KSik}\{ID_i||T_{14}||ID_kUpgradepackages||$

$E_{SKi}[H(ID_i||T_{14}||ID_kUpgradepackages)]\}\}$

⑧汽车终端 k 使用会话密钥（session key）解密压缩包：

$D_{KSik}\{ID_i||T_{14}||ID_kUpgradepackages||E_{SKi}[H(ID_i||T_{14}||ID_kUpgradepackages)]\}$

$=\{ID_i||T_{14}||ID_kUpgradepackages||E_{SKi}[H(ID_i||$

$T_{14}||ID_kUpgradepackages)]\}$

⑩汽车终端 k 以总服务器 i 的公钥来验证升级包的签名：

$H_{41}=D_{PKi}\{E_{SKi}[H(ID_i||T_{14}||ID_kUpgradepackages)]\}$

$=H(ID_i||T_{14}||ID_kUpgradepackages)$

汽车终端 k 通过信息计算哈希值 H_{42}：

$H_{42}=H(ID_i||T_{14}||ID_k\ Upgrade\ packages)$

判断 H_{41} 与 H_{42} 是否相等，若相等，则可确认该软件升级包来自于服务器 i，可以进行安装，若不等，则无法确认该软件升级包来自与服务器 i，不能进行安装。

(25) $ID_k||ID_j||ID_i||T_{16}||E_{SKk}[H(ID_k||ID_j||ID_i||T_{16})]||PK_i\{ID_k||N_i||T_{16}||E_{SKk}[H(ID_k||N_i||T_{16})]\}$

汽车终端 k 向基站 j 发送信息。

(26)同步骤（14）（22），基站 j 在验证服务器 i 后进行相关的数据转发。

(27) $ID_j||ID_i||ID_k||T_{17}||E_{SKj}[H(ID_j||ID_i||ID_k||T_{17})]||E_{PKi}\{ID_k||N_i||T_{16}||E_{SKk}[H(ID_k||N_i||T_{16})]\}$

基站 j 向汽车终端发送信息。

(28)服务器 i 接收基站 j 发来的消息并判断消息真伪以及判断汽车终端 k 是否正常升级：

⑪同步骤（6）服务器 i 验签基站 j 的签名。

⑫服务器 i 用自己的私钥解密压缩包：

$D_{Ski}\{E_{Pki}\{ID_k||N_i||T_{16}||E_{SKk}[H(ID_k||N_i||T_{16})]\}\}=\{ID_k||N_i||T_{16}||E_{SKk}[H(ID_k||N_i||T_{16})]\}$

⑬服务器 i 以汽车终端 k 的公钥来验证汽车终端 k 的签名：

$H_{47}=D_{PKk}\{E_{SKk}[H(ID_k||N_i||T_{16})]\}=H(ID_k||N_i||T_{16})$

服务器 i 计算哈希值 H_{48}：$H_{48}=H(ID_k||N_i||T_{16})$

判断 H_{47} 与 H_{48} 是否相等，若相等，可确认该压缩包来源于汽车终端；若不等，无法确认压缩包发送者。

⑭服务器 i 通过计算对比 N_i 值来确认汽车终端 k 是否安装软件升级包：

$H_{49}=H(ID_kUpgradepackages)=H(N_i)$

服务器 i 通过信息计算哈希值 H_{50}：$H_{50}=H(N_i)$

判断 H_{49} 与 H_{50} 是否相等，若相等，确认汽车终端 k 正常接收安装包并安装，若不等，表明未正常安装。

4.3 软件升级协议安全性分析

（1） 抗主动攻击

主动攻击是一种由攻击者主动发起，对信息内容进行更改、假冒、重放。软件升级协议中分别对以下主动攻击进行了防范：

① 抗身份假冒、抵赖：协议中通信三方在通信前分别向 CA 证书机构进行证书的申请，在协议中，各方身份鉴别环节分别通过“$H_1=H(PK_i||ID_i||T_2)$、$H_4=H(IDi||IDj||T1)$”先鉴别 CA 证书，再鉴别通信方签名，通过比对数字签名从而能判断身份是否真实，

而数字签名旨在鉴别身份，保障数据完整，提供证据以无法抵赖[11]，进而达到抗身份假冒、抵赖的效果。如果黑客假冒身份，必须获得签名私钥，而由公钥得到私钥需求解椭圆曲线上离散对数，这是黑客办不到的。

② 抗数据篡改：协议中使用 SM3 哈希算法进行相关信息数据的摘要，黑客从摘要获取原文信息或伪造原文信息，是不可能的。对于非对称密钥体制下的密码算法，除非拥有对方的私钥，否则解密相当于求椭圆曲线上的离散对数问题，以现今的科技技术水平还未能做到，因此其有效防范了数据篡改的风险。

③ 防数据重放：数据重放多为通过转发“老旧信息”从而达到攻击的效果，在协议中，通信三方可以根据时间戳 T 或随机数 N 的值来判断消息的新鲜性、实时性。当时间戳 T 的值与系统时钟信号差距过大或随机数 N 不再新鲜，将视为重放攻击。

（④ 抗中间人攻击：由于软件升级过程中只能经由中间人（基站）转发，因此还需抗中间人攻击。在“ $E_{Pki}\{\{T_8||ID_k||PK_k||E_{SKCA}[H(T_8||ID_K||PK_k)]\}||ID_k||T_{12}||E_{SKk}[H(ID_k||T_{12})]\}$”中，汽车终端以收方公钥加密，能保障自己所传达信息安全。而收方以自己私钥解密获取信息跨中间方实现鉴别，即可实现握手，也可判断中间方目前处于比较安全的状态。即使中间人被劫持，仍不能破解获取其内容。而收方可通过“$H(ID_i||T_{14}||ID_k$ Upgrade packages)”来判断信息是否安全与是否新鲜。该协议很好的抵抗了中间人攻击。

（2） 抗被动攻击

相对于主动攻击，被动攻击不会更改消息内容一般多为数据监听等方式。协议中使用 SM2、SM4 密码算法对所需传达的信息进行加密。即便不对数据进行篡改，在没有解密的情况下，看到的数据皆为一串乱码，从而防范被动攻击（流量分析或数据监听）。

4.4 代码运行测试

为了验证设计协议的可行性，在工程实现方面，使用 Vmware Workstation Pro 模拟通信三方，基于 CentOS 7 操作系统，应用 Xshell 终端模拟软件和 GmSSL 工具箱，通过 shell 脚本实现网联汽车软件升级协议，身份鉴别与升级包发送传输部分截图如图 3~图 5 所示。从代码正确运行来看，该软件升级协议安全有效。

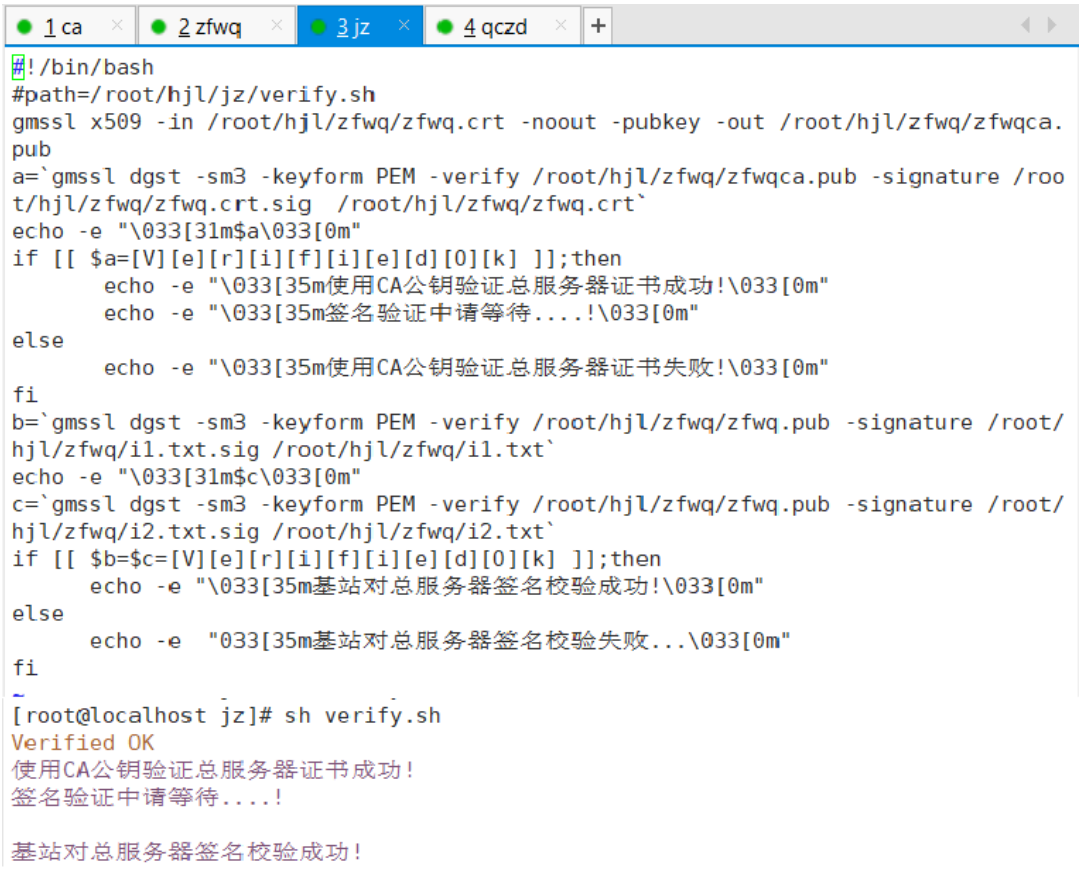

图 3 基站 j 对总服务器进行身份鉴别

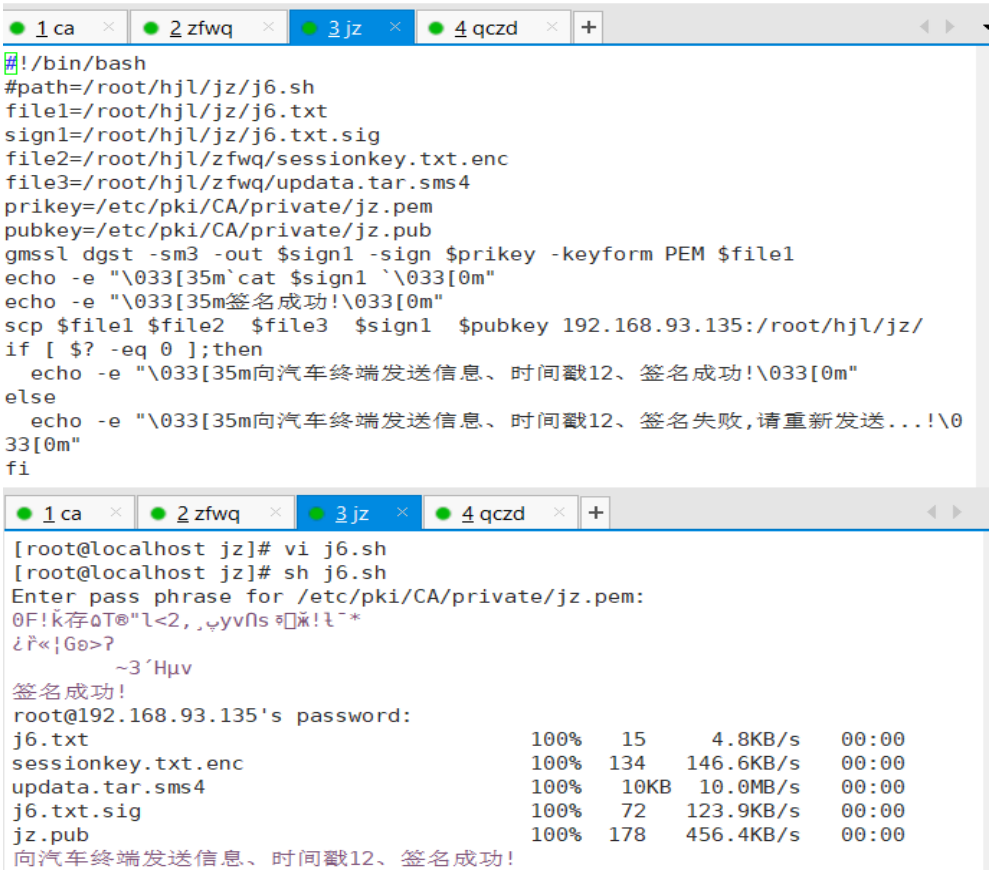

图 4 软件升级包中转发送

图 5 验签升级包完成升级

5 结束语

通过对网联汽车软件升级过程安全问题进行研究，分析其安全问题可能造成的危害，提出安全需求，根据需求构建基于国密技术的智能网联汽车软件升级模型与协议。智能网联汽车软件升级需在三方信任的前提下进行。但在 5G 通信过程中绕不开基站的传输，服务器方与汽车终端方需在保证信息安全的情况下相互鉴别认证。数据升级包体量较大，使用对称密钥来保证效率。本文使用非对称与对称密钥体制相结合的方式来实现远程升级，既保证了效率，又提高了安全性。

参 考 文 献

[1] 陈骏生.智能网联汽车网络安全分析[J].机电技术,2023,(04):90-92.

[2] 李占坤. 基于 SoC 平台的 OTA 主节点无感自升级系统研究 [J]. 上海汽车, 2024, (04): 38-42.

[3] 王婧璇,文海鸥,陈亚翔. 汽车软件在线升级关键技术及监管要求分析 [J]. 汽车文摘, 2024, (04): 19-27. DOI:10.19822/j.cnki.1671-6329.20230196.

[4] 鲍越. 智能网联汽车商用密码应用及验证分析[D]. 华东师范大学, 2023. DOI:10.27149/d.cnki.ghdsu.2023.003923.

[5] 孙孟海,聂岗,李明. 密码算法的标准化研究 [J]. 中国标准化, 2023, (08): 82-85.

[6] 付合东. 智能网联汽车 OTA 产品生产一致性风险分析及建议 [J]. 北京汽车, 2024, (02): 38-41. DOI:10.14175/j.issn.1002-4581.2024.02.010.

[7] 姚正宁. 智能网联汽车安全产业发展概况 [J]. 中国信息安全, 2024, (02): 37-40.

[8] 张海涛.智能网联汽车网络安全关键技术研究与应用[D].电子科技大学,2023.

[9] 李端,徐杰.智能网联汽车系统的网络安全风险分析[J].工业信息安全,2022,(04):73-80.

[10] 吴胜男,朱云尧,冀浩杰,等. 智能网联汽车软件在线升级安全风险分析及管理对策建议 汽车文摘, 2023, (03): 15-20. DOI:10.19822/j.cnki.1671-6329.20220191.

[11] 陈楠. 基于椭圆曲线的无证书 SM2 数字签名方案 [J]. 现代计算机, 2023, 29 (23): 53-57+63.