·安全技术· 文章编号：1000-3428(2018)06-0141-06 文献标志码：A 中图分类号：TP309

基于一次性密码本的车内网身份认证协议

万爱兰，韩 牟，马世典，王运文，华 蕾，冯晓林

（江苏大学 计算机科学与通信工程学院，江苏 镇江 212013）

摘 要： 针对车内网控制器局域网（CAN）总线中电子控制单元（ECU）易被篡改、假冒等安全问题，提出一种基于一次性密码本的身份认证协议。该协议利用网关 ECU（GECU）中的安全存储模块 TA 验证 ECU 的合法身份，根据车载电源电压变化得到随机数，生成会话密钥并且使 ECU 节点间共享会话密钥，简化 TA 对 ECU 的密钥管理，周期性地更新连接和释放外部设备时的会话密钥，以防止重放攻击。仿真结果表明，该协议可有效减少总线负载，提高通信效率。

关键词： 车内网；控制器局域网；一次性密码本；密钥更新；认证协议

中文引用格式： 万爱兰，韩 牟，马世典，等. 基于一次性密码本的车内网身份认证协议[J]. 计算机工程，2018，44(6)：141-146，161.

英文引用格式： WAN Ailan，HAN Mu，MA Shidian，et al. Identity authentication protocol for intra-vehicle network based on one-time pad[J]. Computer Engineering，2018，44(6)：141-146，161.

Identity Authentication Protocol for Intra-vehicle Network Based on One-time Pad

WAN Ailan，HAN Mu，MA Shidian，WANG Yunwen，HUA Lei，FENG Xiaolin

（School of Computer Science and Communication Engineering，Jiangsu University，Zhenjiang，Jiangsu 212013，China）

【Abstract】 To solve the problem of Electronic Control Unit（ECU） in the Controller Area Network（CAN） bus of intra-vehicle network，which is easy to be tampered and faked，this paper puts forward an authentication protocol based on one-time pad in the vehicle network. Firstly，it uses secure storage module TA in the Gateway ECU（GECU） to verify the legal identity of the ECU. Then according to the vehicle power supply voltage，it achieves the random number，generates the session key，and simplifies the key management of TA to ECU. At last，it periodically updates the session key when connecting and releasing external devices and effectively prevents the replay attack. The experimental result shows that this protocol can be applied to the vehicle environment efficiently，which significantly reduces the bus load and improves the communication efficiency.

【Key words】 intra-vehicle network；Controller Area Network（CAN）；one-time pad；key update；authentication protocol

DOI： 10.19678/j.issn.1000-3428.0047079

0 概述

近年来，随着计算机、互联网、通信、传感器及人工智能等高新技术与先进汽车技术的快速融合，智能网联汽车已经成为全球汽车、互联网等领域的研究热点和产业增长的新动力。车内网作为智能网联汽车的一部分，通过 WiFi、蓝牙或者 OBD 接口与外部设备连接，使敌手能够利用控制器局域网（Controller Area Network，CAN）总线的漏洞对车内的电子控制单元（Electronic Control Unit，ECU）执行远程无线攻击[1]。因此，为了保证车内 CAN 总线网络的安全，对智能网联环境下车内网认证协议的研究是必要的。

文献[2]证明现代车辆中的制动控制器通过无线方式连接到嵌入式控制网络，能对 MP3 播放器进行远程操纵。攻击者通过无线或者有线方式访问车内 CAN，以便在高速公路上行驶时控制汽车中的紧

基金项目： 国家自然科学基金（61300229）；中国博士后科学基金（2013M531283）；江苏省“六大人才高峰”项目（DZXX-012）；江苏省高校自然科学基金（12KJD580002）；江苏省研究生创新基金（KYLX_1057）；江苏省重点研发计划项目（BE2017035）。

作者简介： 万爱兰（1993—），女，硕士研究生，主研方向为密码学、车联网安全；韩 牟、马世典，副教授、博士；王运文、华 蕾、冯晓林，硕士研究生。

收稿日期： 2017-05-05 **修回日期：** 2017-06-30 **E-mail：** 1962130808@qq.com

急制动器,在夜间行驶时解锁车门并启动发动机或关闭前照灯,造成交通事故。通常的车内网络协议,如 CAN[3]、FlexRAY[4] 和时间触发协议(Time Triggered Protocol,TTP)[5],本身没有安全机制验证发送消息的节点的真实身份。因此,这些协议易受到伪造和重放攻击。为解决当前车内总线网络被恶意攻击的安全问题,文献[6]提出基于加密方法的安全机制,为现有车内网安全通信奠定了基础。文献[7]针对车内 CAN 局域网中 ECU 节点身份信息易被篡改的问题,提出基于时间戳的认证机制,其实现的底层标准化一次认证体制提高了安全性,但是不能有效地应用于车内网,增加了 CAN 总线负载。此外,针对 CAN 总线协议的安全问题,文献[8]提出轻量级车内 CAN 安全认证协议,能解决现有 CAN 以及其他传感器网络的隐私和安全漏洞,适用于资源有限的嵌入式系统,但是其消耗了车内的大量资源。文献[9]对当前 CAN 总线提出了后向兼容的广播认证协议,保证了密钥的后向安全,但是并未考虑前向安全。文献[10]提出了 CAN 中的轻量级广播认证协议,用 DES 算法加密一个数据帧,但该协议计算效率较低。

为解决上述问题,本文针对当前车辆环境提出一种基于一次性密码本的车内网身份认证协议。首先利用网关 ECU(Gateway ECU,GECU)中的安全存储模块 TA 验证 ECU 的合法身份,保证信息的机密性;然后利用智能 ECU 与车内电源系统之间产生的耦合作用,根据车载电源电压变化得到随机数,生成会话密钥;最后对车内 CAN 总线中的密钥分发协议进行优化,周期性地更新连接和释放外部设备时的会话密钥,从而防止重放攻击。

1 基于 CAN 协议的车内网系统

1.1 CAN 协议

车内网系统是典型的信息系统,其中信息通过车内网络总线(CAN、LIN 等)在内部各 ECU 之间进行交互,通过无线通信方式在车内 ECU 节点和外部接入设备间进行交互,其既有信息系统的通用特点,又存在嵌入式系统所特有的软硬件资源受限问题,因此,不可避免地面临更为严峻的信息安全威胁。车内网系统结构如图 1 所示。其中,MOST 为多媒体网络。

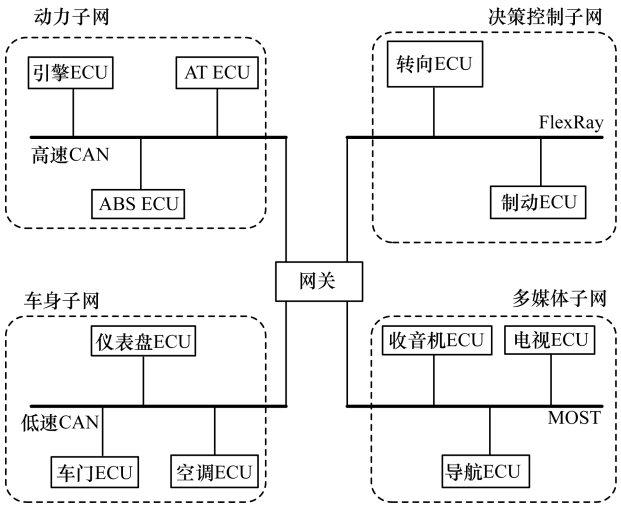

图 1 车内网系统结构

CAN 是目前最主要的车内通信网络,是一种允许汽车内多个 ECU 相互通信的总线协议,已在车内网通信系统中得到广泛应用[11]。通过 CAN 总线,短帧数据会发布到整个网络中[12]。由于车内的广播环境,连接到总线上的所有 ECU 均能接收数据帧。CAN 总线并联有多个 ECU,具有以下特点[13]:

1)可靠性高。CAN 总线能精确识别车内传输的数据帧的错误。

2)使用便捷。如果某个 ECU 停止工作,其他 ECU 还能正常工作,保持原先的功能状态,从而不影响信息传输。

3)数据密度大。在任意时刻 ECU 的信息状态均相同,这样 2 个 ECU 之间的通信没有数据偏差。如果 CAN 总线出现故障,连接到总线上的所有 ECU 都会收到通知。

4)实时性高。车内网中的各 ECU 之间的数据传输很快,不会发生延迟。

1.2 安全威胁

CAN 总线协议面临的安全威胁包括:

1)访问控制的脆弱性。ECU 使用车辆制造商分配的固定密钥,容易被攻击者截获,并且刷新 ECU 内部存储、开放车辆与外部设备通信的接口。这些对外接口在给车主带来功能性和舒适性的同时,也成为外部设备攻击 CAN 总线的入口[14]。

2)广播通信。CAN 是基于广播机制的网络协议[15],车内网中的任何 ECU 节点都能接收和发送数据帧。此外,恶意节点能对广播信道窃听,向 CAN 总线发送恶意数据帧,造成 ECU 故障,引发事故。

3)非加密的数据帧。车内网络 ECU 节点之间以明文通信,没有任何加密机制,不可避免地带来信息泄露问题。

4)多主机工作方式。连接到总线上的 ECU 是彼此独立的,直接向总线发送数据帧,使得恶意节点能通过窃取合法节点的身份(ID)来发送数据帧(如数据帧的修改和重放攻击)。

5)无认证机制。CAN 总线的数据结构中没有认证域,恶意节点能假冒合法节点发送数据帧,从而操纵 ECU 节点的行为。例如,恶意节点 X 假冒合法节点 Y 在 CAN 总线网络中注入包含恶意内容的欺骗消息,并且接收消息的节点 Z 不能区分消息是来自真实的节点 Y 还是恶意节点,因此需要广播认证机制。

2　车内网身份认证协议设计

当车辆启动或者更换 ECU 时,GECU 将认证密钥 k_i 和长期对称密钥 GK 加载到安全存储中,并记录安装在车辆上的 ECU 的数量 N。认证协议流程如图 2所示。本文中使用的符号及其定义如表 1 所示。

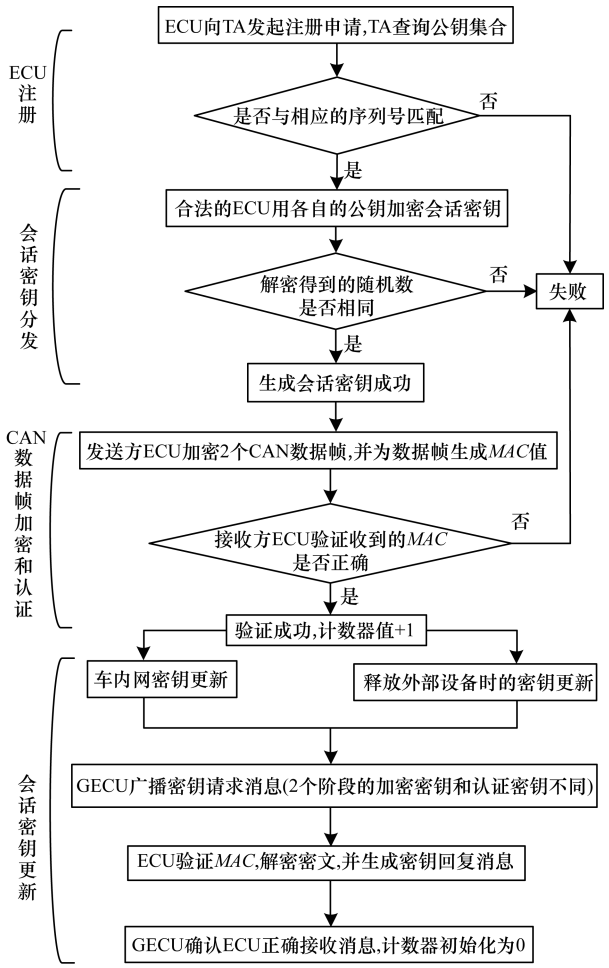

图 2　认证协议流程

表 1　符号定义

符号	定义
ECU_i	第 i 个 ECU
ID_{ECU_i}	ECU_i 的身份
$Number$	标识 ECU 的序列号
SK_{TA},SK_{ECU}	TA 的私钥,ECU 的私钥
CTR_{ECU_i}	ECU_i 的数据帧计数器
PK_{TA},PK_{ECU}	TA 的公钥,ECU 的公钥
$Rand_i$	随机值
EK_m	第 m 个会话的加密密钥
AK_m	第 m 个会话的认证密钥
Accept	确认信息
Refuse	拒绝信息
C	密文
M	明文
KEK_m	第 m 个会话密钥生成的加密密钥
KGK_m	第 m 个会话密钥生成的认证密钥
UK	释放外部设备的加密密钥
k_i	GECU 和 ECU 之间的认证密钥
GK	GECU 和 ECU 之间的对称密钥
$S()$	用于生成会话密钥的单向函数
$Hash_{ECU}$	对 ECU 进行哈希操作得到的散列值
$H_{1,x}$	用 x 表示带有密钥的哈希功能 $H_{1,x}:\{0,1\}^* \times S_m \rightarrow \{0,1\}^{64}$
$H_{2,x}$	用 x 表示带有密钥的哈希功能 $H_{2,x}:\{0,1\}^* \times S_m \rightarrow \{0,1\}^{32}$

2.1　ECU 注册

ECU 在进行密钥交换之前,在 GECU 的安全存储 TA 中注册信息,车辆点火时,ECU 在安全存储中加载公私密钥对,利用 ELGamal 算法产生该密钥对,ECU 隐藏私钥,而将公钥存放在 TA 的公钥集合中,使得需要通信的 ECU 能够查询。ECU 注册流程如图 3 所示。

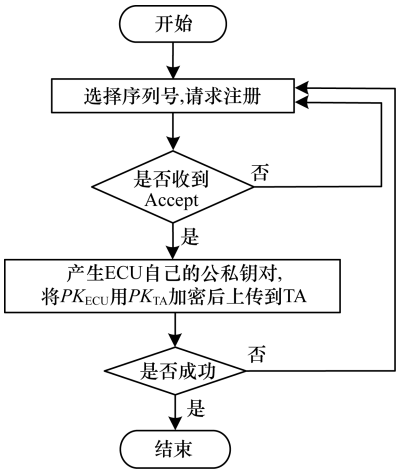

图 3　ECU 注册流程

具体步骤如下:

步骤 1　车辆启动时,ECU 向 GECU 的 TA 发起注册申请,利用 TA 的公钥 PK_{TA} 对车辆制造商在 ECU 上面标志的序列号 $Number$ 加密,然后作为公

钥 PK_{ECU} 上传到 TA 中并等待其确认。

步骤 2 TA 用自己的私钥 SK_{TA} 解密 ECU 的序列号,查询公钥集合,如果没找到相应的序列号,允许其注册,并返回给其确认信息 Accept;否则拒绝注册,返回第一步,TA 中的公钥集合不允许相同的序列号存在。

步骤 3 ECU 收到确认信息后,利用 ELGamal 算法生成一个公私密钥对,将私钥 SK_{ECU} 保存在安全存储中,将公钥 PK_{ECU} 用 TA 的公钥 PK_{TA} 加密发送给 TA。

步骤 4 TA 将序列号和公钥 PK_{ECU} 存储于其公钥集合中,用 ECU 的公钥 PK_{ECU} 加密后发送,保证信息的机密性。

步骤 5 ECU 收到消息后用 SK_{ECU} 解密,若解密得到的信息和自己发送的信息相同,则注册成功并结束。否则返回步骤 1。

2.2 会话密钥分发

以智能 ECU 对车辆的操控行为为媒介,与车内电源系统之间产生耦合作用,使得车内电源电压变化具有马尔科夫特性,生成随机数;假设通信的一方为 ECU_i,另一方为 ECU_j,会话密钥分发过程如图 4 所示。

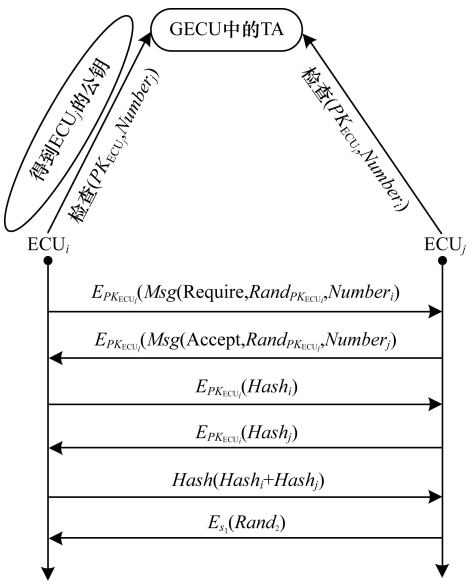

图 4 会话密钥分发过程

具体步骤如下:

步骤 1 通过交通环境和网络环境对车内环境感知单元 ECU、智能控制单元 ECU、智能驾驶决策单元 ECU 等的激励,随机控制车内电源系统,在断电的情况下补充蓄电池电能,作为随机波动能量作用于发电机,然后再作用于蓄电池,通过一个随机生成模块,采集不同情况下蓄电池的电压,作为随机数序列 $Rand_1, Rand_2, \cdots, Rand_n$;最后将对随机数 $Rand_1$ 进行 Hash 运算的结果作为密钥 S_1。

步骤 2 ECU_i 向 TA 发送与 ECU_j 通信的请求消息,并用 PK_{ECU_j} 加密后发送给 ECU_j。ECU_j 验证 PK_{ECU_i} 是否为 ECU_i 的公钥。如果 TA 验证成功,则发出确认信息 Accept 进行步骤 3,否则发出拒绝信息 Refuse,密钥交换结束。ECU_i 利用上述方法对 ECU_j 的公钥验证。

步骤 3 通信的 ECU 利用哈希函数产生散列值 $Hash_{\mathrm{ECU}_i}$ 和 $Hash_{\mathrm{ECU}_j}$,根据序列号、出厂时间等信息,然后用 PK_{ECU_j} 加密后发送给 ECU_j。

步骤 4 通信双方用各自的私钥解密收到的信息,对随机数 $Rand_2$ 进行 Hash 操作得到新的散列值 $Hash_{\mathrm{ECU}_{ij}}$,作为会话密钥 S_2。

步骤 5 ECU_i 和 ECU_j 验证随机数加密结果的一致性,分别用 S_2 加密 $Rand_2$ 后传送给对方,如果用 S_1 解密后得到的 $Rand_1$ 和先前的 $Rand_2$ 相同,表明双方的会话密钥生成成功;否则,只要任何一方生成会话密钥失败,就要回到步骤 1 重新进行会话密钥的生成过程。

2.3 CAN 数据帧加密与认证

在会话密钥分发过程完成后,GECU 对正在工作的 ECU 发送的数据帧进行认证,其中用 128 bit 的国际数据加密算法 IDEA 和带有密钥的消息认证码 MAC 进行认证。ECU_s 使用 IDEA 算法加密 2 个数据帧,并为数据帧生成 MAC 值,ECU_r 对 MAC 进行认证和解密,其过程如图 5 所示。

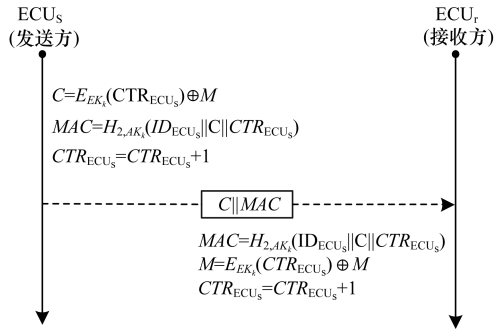

图 5 CAN 数据帧加密与认证过程

具体步骤如下:

步骤 1 发送方 ECU_S 管理其数据帧计数器值 CTR_{ECU_S},当传输数据帧时,ECU_S 用 CTR_{ECU_S} 生成密文 $C = E_{EK_k}(CTR_{\mathrm{ECU}_S}) \oplus M$;$E_{EK_k}(CTR_{\mathrm{ECU}_S})$ 的结果是 128 bit,由于 CAN 数据帧最大有效载荷为 64 bit,只有前 64 bit 是用来生成密文 C,因此用 128 bit 的 IDEA 算法来加密 2 个明文。

步骤 2 ECU_S 为 CAN 数据帧生成 MAC 值,包括明文 CTR_{ECU_S} 和密文 C,即:$MAC = H_{2,AK_k}(ID_{\mathrm{ECU}_S} \| C \| CTR_{\mathrm{ECU}_S})$。

步骤 3 ECU_r 接收发送方 ECU_S 的计数器值并用 CTR_{ECU_S}、AK_k 来验证所接收的 MAC 是否正确。

步骤 4 如果 MAC 验证成功,通过计算 $M = E_{EK_k}(CTR_{\mathrm{ECU}_S}) \oplus C$ 来解密并获得明文信息 M。

步骤 5 在认证和解密数据帧后,ECU_r 增加 ECU 的 CAN 数据帧计数器值 CTR_{ECU_S}。

2.4　会话密钥更新

由于车辆接入外部设备时可能泄露会话密钥,因此需要周期性地更新认证过程中的加密密钥和认证密钥。在第 m 个会话密钥中的会话密钥更新过程如图 6 所示。

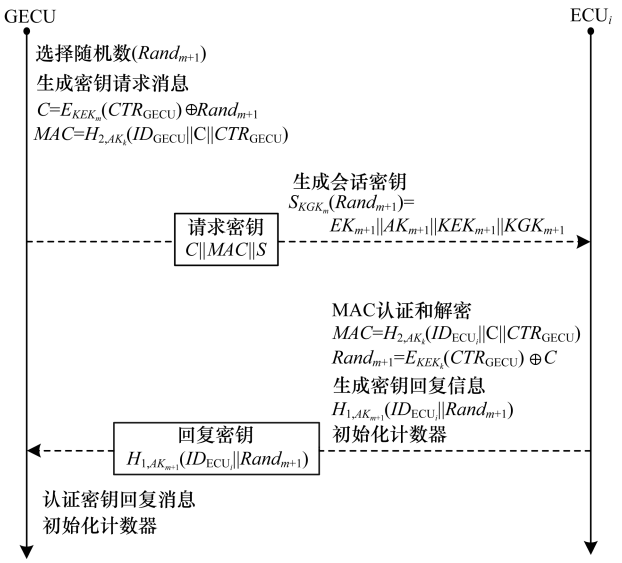

图 6　会话密钥更新过程

在车内 ECU 密钥更新阶段,GECU 按每个规定周期 T 更新密钥,具体步骤如下:

步骤 1　在随机序列中选择随机值 $Rand_{m+1}$,GECU 生成密钥请求消息并将其广播到车内网 CAN,此消息如下:

$$C = E_{KEK_K}(CTR_{GECU})\oplus Rand_{m+1}$$

$$MAC = H_{2,AK_k}(ID_{GECU}||C||CTR_{GECU})$$

步骤 2　接收密钥请求消息的每个 ECU$_i$ 使用 AK_k 验证 MAC 和 KEK_k 解密密文 C。然后,ECU$_i$ 使用密钥生成函数 S 得到在第 $m+1$ 个会话中使用的会话密钥。每个数据帧计数器值初始化为 0。

步骤 3　在执行步骤 2 后,每个 ECU_i 生成密钥回复消息,并将其发送到 GECU 以确定他们是否正确地接收到密钥请求消息:$H_{1,AK_{k+1}}(ID_{ECU_i}||Rand_{m+1})$。

步骤 4　在确认正确接收到密钥请求消息后,GECU 将 ECU$_i$ 的每个数据帧计数器初始化为 0,密钥更新阶段完成。

在释放外部设备时的密钥更新阶段,如果外部设备和车辆之间的连接被终止,则 GECU 按如下步骤执行会话密钥更新过程保证通信安全:

步骤 1　GECU 生成随机值 $Rand_{new}$,然后使用 UK 生成密钥请求消息:$C = E_{UK}(CTR_{GECU})\oplus Rand_{new}$,$MAC = H_{2,AK_k}(ID_{GECU}||C||CTR_{GECU})$,最后 GECU 将密钥请求消息广播到车载 CAN。

步骤 2　接收密钥请求消息的每个 ECU$_i$ 分别使用 AK_k 和 UK 执行 MAC 的验证和解密密文 C。其余步骤与车内 ECU 密钥更新阶段相同。

3　安全性及性能分析

3.1　安全性分析

对本文提出协议进行以下方面的分析:

1)机密性。注册过程中 GECU 的安全存储 TA 中存放了 ECU 的公钥、序列号等信息,在通信的过程中,ECU$_r$ 需要确认 ECU$_S$ 的合法身份,ECU$_r$ 向 GECU 发送待验证的 ECU$_S$ 的公钥、序列号等信息,GECU 收到信息后,TA 将信息与集合中的信息进行匹配,如果匹配成功,发送 Accept,说明 ECU$_S$ 合法;否则,认证失败,ECU$_r$ 就不会与 ECU$_S$ 通信,避免与非法节点截获信息,从而保证了机密性。

2)认证性。本文协议中生成 MAC 的认证密钥 AK_k 是安全的。对于攻击者而言猜测一个 32 bit 的 MAC 值是很困难的。虽然在一般的车内环境中,一个 32 bit 的 MAC 能在几秒的时间内伪造,但敌手要花费约 10 000 h 每秒传送 2^{32} 个数据帧。如果敌手在少于 10 s 的周期内在车内 CAN 中传输恶意的数据帧,车内网将会关闭 CAN 总线,提示通信失败。本文设计的会话密钥更新协议使用的是安全的 32 bit的 MAC。

3)前向和后向密钥安全。若外部设备和车载 CAN 之间的连接到期,则 GECU 广播包含 $Rand_{new}$ 的密钥请求消息。由于密钥请求消息由 UK 加密,因此外部设备不能获得前向会话密钥(由随机值 $Rand_{m-1}$ 生成的会话密钥),也很难获得后向会话密钥(由随机值 $Rand_{m+1}$ 生成的会话密钥)。尽管第 m 个会话密钥暴露,但是第 $m-1$ 个会话密钥不可能暴露,由于在 $Rand_{m-1}$ 和 $Rand_m$ 之间毫无关联。

4)密钥更新。在本文协议中,由车内电源电压变化的马尔科夫特性得到随机数,并据随机值生成会话密钥,因此会话密钥之间没有联系,即:$Rand_1$,$Rand_2$,…,$Rand_n$ 是不同的值。

5)重放攻击。发送方和接收方各自都有计数器,每次生成的都是不同的密钥,因此,本文协议抗重放攻击。

因此,针对 CAN 总线协议面临的安全威胁,协议安全性分析中提出的机密性、前向后向密钥安全确保了授权的 ECU 能够互相通信,进而防止非法设备通过接口访问车内网,解决了访问控制的脆弱性问题。认证性利用带有密钥的消息认证码 MAC 对 ECU 节点进行认证,规避了广播通信、多主机工作方式以及无认证机制的安全风险。针对总线数据帧非加密的问题,通过用国际数据加密算法 IDEA 加密数据帧的方法,达到保证车内 ECU 节点之间通信信息安全的目的。

3.2　性能评估

本文实现的仿真是将 ECU 与 CANoe 软件相连接,性能评估实验设置的通信负载比一般的车内 CAN 高。正如上文提到,一般的车内 CAN 被分为

3 类子网:动力子网,决策控制子网,多媒体子网。每个子网至少由 16 个 ECU 组成。特别的是,大型子网像车身控制子网,有 13 个 ECU 互相通信[16-17]。

实验将设计的协议与文献[7,9-10]中提出的协议进行比较。为了描述简单,将文献[9]中的协议记为 CANAuth,文献[10]中的协议记为 LiBrA-CAN,文献[7]中的协议记为 IDT&C。CANAuth 是在一个 CAN 数据帧中同时包含消息和 MAC 的模式。LiBrA-CAN 分别发送 2 个 CAN 数据帧,一个用于消息,另一个用于 MAC,IDT & C 生成与车内通信子网中的接收者一样多的 MAC 消息。若 N 作为通信中 ECU 的数量,额外生成的消息的数量是 N^2,以使子网内的每个 ECU 都能通信。

下文使用 1 MB/s 的 CAN 总线、32 bit 的 MAC 以及 20 ms 的 ECU 传输周期分析本文协议、CANAuth、LiBrA-CAN 和 IDT&C 协议所需的总线负载。

在一般情况下,总线负载必须保持在最大值的 50% 以下,以保持稳定的通信环境。从图 7 中可以看出,本文协议保持总线负载在 25% 以下,尽管有 40 个 ECU,由于 OURS 不需要额外的 CAN 数据帧,也不使用会话密钥分发用于消息认证。但是,CANAuth 由于额外的 CAN 数据帧和密钥分发,总线负载增加到 50% 以上,只有在少于4 个ECU 并且密钥分发延迟超过 4 ms 时才能保持 50% 以下的总线负载。IDT & C 协议也会快速增加总线负载,因为它还必须发送与接收方一样多的 MAC 消息,只有当通信组中有 4 个 ECU 时,才能维持 70% 左右的总线负载。

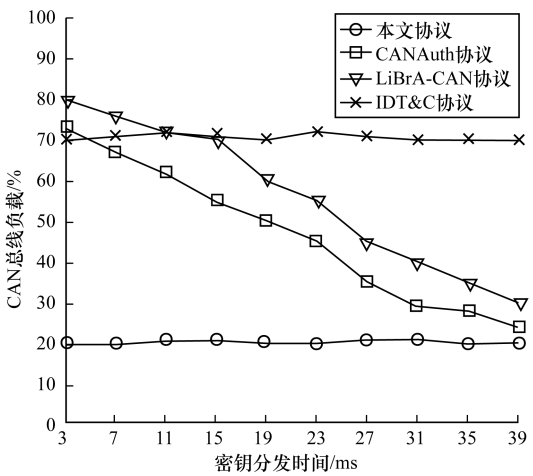

图 7 4 种协议的 CAN 总线负载对比

4 结束语

本文针对车内网中 CAN 的漏洞设计了一个安全协议,该协议具有以下特性:在注册阶段利用 GECU 中的安全存储 TA 验证 ECU 的合法身份,保证了信息的机密性;在密钥分发阶段根据车载电源电压变化得到随机数,生成会话密钥,简化了密钥管理,且会话密钥的生成满足一次一密的需求;在认证阶段通过 ECU 之间共享会话密钥,减少了认证次数,降低了 CAN 总线的负载;最后周期性地更新连接和释放外部设备时的会话密钥,有效地防止了重放攻击。

参考文献

[1] 马世典,江浩斌,韩 牟,等. 车联网环境下车载电控系统信息安全综述[J]. 江苏大学学报(自然科学版),2014,35(6):635-643.

[2] KOSCHER K, CZESKIS A, ROESNER F, et al. Experimental security analysis of a modern automobile[J]. IEEE Journal of Selected Topics in Quantum Electronics,2010,41(3):447-462.

[3] LING C,FENG D. An algorithm for detection of malicious messages on CAN buses[C]//Proceedings of International Conference on Information Technology and Computer Science. [S.l.]:Atlantis Press,2012:245-249.

[4] TANASA B, BORDOLOI U D, ELES P, et al. Scheduling for fault-tolerant communication on the static segment of FlexRay[C]//Proceedings of IEEE Real-time Systems Symposium. Washington D. C., USA: IEEE Press,2010:385-394.

[5] ALMEIDA J, FERREIRA J, OLIVEIRA A S R. Fault tolerant architecture for infrastructure based vehicular networks[M]//ALAM M, FERREIRA J, FONSECA J. Intelligent Transportation Systems. Berlin, Germany: Springer,2016:169-194.

[6] WOLF M, WEIMERSKIRCH A, PAAR C. Secure in-vehicle communication[M]//LEMKE K, RAAR C, WOLF M. Embedded Security in Cars: Securing Current and Future Automotive IT Applications. Berlin, Germany: Springer, 2006:95-109.

[7] LIN C W, SANGIOVANNIVINCENTELLI A. Cyber-security for the controller area network (CAN) communication protocol[C]//Proceedings of International Conference on Cyber Security. Washington D. C., USA: IEEE Press,2012: 1-7.

[8] XU M, XU W, WALKER J, et al. Lightweight secure communication protocols for in-vehicle sensor networks[C]// Proceedings of ACM Workshop on Security. New York, USA:ACM Press,2013.

[9] HERREWEGE A V, SINGELÉE D, VERBAUWHEDE I. CANAuth: a simple, backward compatible broadcast authentication protocol for CAN bus[C]//Proceedings of ECRYPT Workshop on Lightweight Cryptography. Louvain-la-Neuve, Belgium: [s. n.],2011:299-235.

[10] GROZA B, MURVAY S, HERREWEGE A V, et al. LiBrA-CAN: a lightweight broadcast authentication protocol for controller area networks[C]//Proceedings of International Conference on Cryptology and Network Security. Berlin, Germany: Springer,2012:185-200.

[11] 韩 鑫,鲍可进. CAN 总线网络层协议栈开发测试[J]. 计算机工程,2011,37(15):232-234.

[12] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive experimental analyses of automotive attack aurfaces[C]//Proceedings of the 20th USENIX Security Symposium. San Francisco, USA: USENIX,2011:6.

(下转第 161 页)

图 7 为改进皮尔森相似度计算方式下的 MAE 对比。可以看出,只加入单一因子的曲线相比较于传统的 MAE 曲线结果,在推荐的精确性上已经有了很好的提升,而加权融合后的相似度改进比起单一因子,在算法的精确度上很明显要小于前者的误差。相比较于传统的采用皮尔森相似度计算得出的 MAE 曲线,加入平衡因子的改进相似度计算得出的曲线 bf_pearson 和加入改进因子的曲线 wf_pearson 都表现出了更好的精确性。分析加权融合后的推荐结果可知,wb_pearson 在推荐算法的精确性上,偏差要小于以上三者,说明加权融合能够有效降低预测的评分误差,提高推荐的精度。

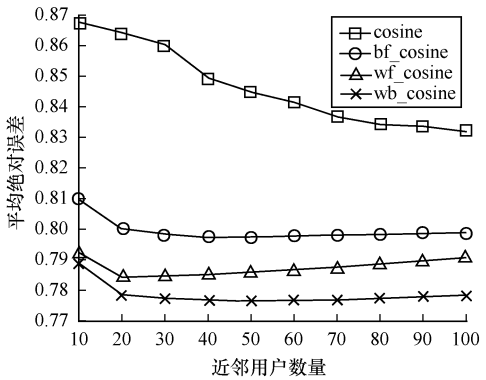

图 7　改进皮尔森相似度计算的 MAE 对比

4　结束语

用户的兴趣爱好会随着时间的增长发生迁移。为此,本文提出基于模糊时序分类模型的相似度加权推荐算法,在一定程度上解决了数据稀疏性和冷启动问题,从而更准确地找到最近邻居用户。实验结果表明,同时考虑用户属性标签和时间维度能够有效提升推荐算法的准确度。随着数据量的几何增长,异构信息网络替代传统同构网络是必然趋势,因此,如何将推荐算法融入异构网络将是下一步的研究方向。

参考文献

[1] ZHAO Z D, SHANG M S. User-based collaborative-filtering recommendation algorithms on Hadoop[C]// Proceedings of the 3rd International Conference on Knowledge Discovery and Data Mining. Washington D. C., USA:IEEE Press,2010:478-481.

[2] 文俊浩,袁培雷,曾　骏,等. 基于标签主题的协同过滤推荐算法研究[J]. 计算机工程,2017,43(1):247-252.

[3] ZHANG D,LEE W S. Question classification using support vector machines[C]//Proceedings of the 26th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York, USA: ACM Press,2003:26-32.

[4] 文　勖,张　宇,刘　挺,等. 基于句法结构分析的中文问题分类[J]. 中文信息学报,2006,20(2):33-39.

[5] 韩亚楠,曹　菡,刘亮亮,等. 基于评分矩阵填充与用户兴趣的协同过滤推荐算法[J]. 计算机工程,2016,42(1):36-40.

[6] 孙　辉,马　跃,杨梅波,等. 一种相似度改进的用户聚类协同过滤推荐算法[J]. 小型微型计算机系统,2014,35(9):1967-1970.

[7] 党　博,姜久雷. 基于评分差异度和用户偏好的协同过滤算法[J]. 计算机应用,2016,36(4):1050-1053.

[8] 王吉源,黎　晨,王婵娟. 用户属性加权活跃近邻的协同过滤算法[J]. 计算机应用研究,2016,33(12):3625-3629.

[9] 夏平平,帅建梅. 基于相似度拓展与兴趣度缩放的协同过滤算法[J]. 计算机工程,2016,42(1):199-202.

[10] 王　威,郑　骏. 基于用户相似度的协同过滤算法改进[J]. 华东师范大学学报(自然科学版),2016,2016(3):60-66.

[11] 荣辉佳,火生旭,胡春华,等. 基于用户相似度的协同过滤推荐算法[J]. 通信学报,2014,35(2):17-24.

[12] 赵　亮,刘建辉,崔彩峰. 互信息匹配的半朴素贝叶斯分类器[J]. 计算机工程与应用,2016,52(18):84-87.

[13] 孙光辉. 基于时间效应和用户兴趣变化的改进推荐算法研究[D]. 北京:北京邮电大学,2014.

[14] 周建伟,张　娟. 拉格朗日插值模型与统计数据检验及应用[J]. 统计与决策,2016(5):78-80.

[15] 孙光福,吴　乐,刘　淇,等. 基于时序行为的协同过滤推荐算法[J]. 软件学报,2013,24(11):2721-2733.

编辑　金胡考

(上接第 146 页)

[13] LIM H T,HERRSCHER D. Challenges in a future IP/Ethernet-based in-car network for real-time applications [C]// Proceedings of the 48th ACM/EDAC/IEEE Design Automation Conference. Washington D. C., USA: IEEE Press, 2011: 7-12.

[14] 于　赫. 网联汽车信息安全问题及 CAN 总线异常检测技术研究[D]. 长春:吉林大学,2016.

[15] 韩微辉. 互联网汽车总线安全模型与应用研究[D]. 上海:华东师范大学,2016.

[16] AKAMATSU M, GREEN P, BENGLER K. Automotive technology and human factors research: past, present, and future[J]. International Journal of Vehicular Technology, 2013(2013).

[17] HAN J,LIU Z,CUI S,et al. A study on the application of the controller area network communication protocol to hybrid electric vehicle [J]. Automotive Engineering, 2011,33(12):1062-982.

编辑　金胡考