

面向时延敏感的TRDP安全防护机制

崔玉龙¹, 吴学超¹, 程宥霖^{2,3}, 芦翔^{2,3}

(1. 中车青岛四方机车车辆股份有限公司, 山东 青岛 266111; 2. 中国科学院信息工程研究所, 北京 100085;
3. 中国科学院大学网络空间安全学院, 北京 100049)

摘要: 随着列车通信技术的发展, 列车控制网络的环境愈发复杂, 车载设备对网络带宽和网络拓扑复杂度的要求愈发严格, 列车互联网的物理层载体逐渐从串行通信总线网过渡到了以太网。为了保证以太网协议栈在列车互联网中的正常运行, 结合列车互联网的独特需求, 列车通信网络 (train communication network, TCN) 联盟提出了列车实时数据协议 (train real-time data protocol, TRDP), 现已成为车载设备数据传输中不可或缺的重要一环。然而, 在引入以太网架构的同时, 传统计算机网络面临的安全风险也被带入了列车通信网络中。架构在以太网之上的TRDP, 缺乏有效的安全防护机制, 面临着恶意攻击、数据泄露、拒绝服务等一系列风险。在TRDP的基础上, 分析了TRDP消息数据、过程数据两种协议模式的区别和安全需求, 结合列车互联网的实际情况, 选取合适的加密协议, 改进了协议细节, 设计了基于加密协议的安全防护机制。并在此基础上搭建了一个模型系统, 系统展示了如何将这些关键的密码技术组合起来, 构建一个安全的列车互联网信息系统, 并证明了系统在保证协议安全性的情况下, 能够满足列车互联网对TRDP的性能需求。

关键词: 列车通信网络; TRDP; 以太网; 网络安全; 安全协议设计

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025028

Security scheme for time-critical TRDP message

CUI Yulong¹, WU Xuechao¹, CHENG Youlin^{2,3}, LU Xiang^{2,3}

1. CRRC Qingdao Sifang Co., Ltd., Qingdao 266111, China
2. Institute of Information Engineering, CAS, Beijing 100085, China
3. School of Cyber Security, University of CAS, Beijing 100049, China

Abstract: As train communication technology advanced, the environment of train control networks became increasingly complex, with more network bandwidth being demanded by on-board devices and greater complexity emerging in network topology. Consequently, the physical layer carrier for train internet gradually transitioned from serial communication bus networks to Ethernet. To ensure the normal operation of the Ethernet protocol stack in the train

收稿日期: 2024-11-14; 修回日期: 2025-03-11

通信作者: 程宥霖, chengyoulin@iie.ac.cn

基金项目: 中车青岛四方机车车辆股份有限公司“列车网络信息安全”研究项目

Foundation Item: CRRC Qingdao Sifang Locomotive and Rolling Stock Co., Ltd. “Train Network Information Security” Research Project

引用格式: 崔玉龙, 吴学超, 程宥霖, 等. 面向时延敏感的TRDP安全防护机制[J]. 网络与信息安全学报, 2025, 11(3): 81-97.

Citation Format: CUI Y L, WU X H, CHENG Y L, et al. Security scheme for time-critical TRDP message[J]. Chinese Journal of Network and Information Security, 2025, 11(3): 81-97.

internet and meet the unique requirements of the train internet, the TRDP protocol was proposed by the TCN alliance and has now become an essential part of data transmission for on-board devices. However, with the introduction of the Ethernet architecture, traditional computer network security risks were also brought into the train communication network. The TRDP protocol, built upon Ethernet, lacked effective security protection mechanisms and faced a series of risks such as malicious attacks, data leakage, and denial of service. Based on the TRDP protocol, the differences and requirements of its two protocol modes, message data and process data, were analyzed. Suitable encryption protocols in line with the actual situation of the train internet were selected, protocol details were improved, and a security scheme based on encryption protocols was designed. Furthermore, a model system was constructed on this foundation. The system demonstrates how these key security technologies can be combined to build a secure TRDP train information system and proves that it can meet the performance requirements of the train internet for the TRDP protocol while ensuring the security of the protocol.

Keywords: train communication network, TRDP, ethernet, network security, cryptographic protocol design

0 引言

0.1 我国铁路信息化发展现状

如今,全球铁路信息化高速发展,国内外正经历着从传统串行通信总线到现代以太网技术,再到 5G 和智能化技术的转型。这一进程不仅标志着技术的演进,而且反映了对提高运输效率、安全性和乘客体验的不断追求。

在信息时代早期,铁路通信依赖于串行通信总线,如 LonWorks、控制器区域网络(controller area network, CAN)、ARCNET 和列车通信网络(train communication network, TCN)等协议,这些技术支持了车辆间的基本通信和信息共享。例如, LonWorks 网络在北美和亚洲得到应用,而控制器区域网络则在欧洲的轻轨和地铁中广泛使用。中国铁路^[1]也采纳了这些技术,如“神舟”和“新曙光”机车便是早期信息化的产物。

随着互联网时代的到来,以太网技术开始在铁路系统中得到应用。以太网技术的引入,使得列车通信网络能够处理更大的数据量,满足了旅客信息服务、远程维护和诊断等新兴需求。日本东芝公司提出的 T-Ethernet 体系结构和庞巴迪研制的以太网管理车辆控制信息的新型列车,标志着以太网技术在列车通信网络中的应用已经成熟。中国铁路采用列车通信网络标准^[2],并在 CRH 系列高速列车中实现了以太网技术的应用。

进入智能化时代,5G^[3]和智能化技术^[4]的融合预示着铁路信息化的新篇章。中国铁路作为全球铁路网络的领导者之一,正在积极推动智能高

铁的发展。无线技术,特别是其在列车控制与监控系统(train control and management system, TCMS)中的应用,正在推动从计算机网络到智能列车互联网的转变。这种转变将使得列车之间的通信更加无缝,提高了车辆间的兼容性,并降低了网络部署的复杂性。

在这一发展过程中,列车实时数据协议(train real-time data protocol, TRDP)作为 TCN 网络的一部分,是连接以太网和未来智能列车互联网的桥梁。它在确保列车通信的可靠性和安全性方面发挥着核心作用,建立在 TCP/UDP 之上,为应用层提供服务。这个位置使得 TRDP 能够高效地处理列车通信网络中的实时数据传输,对于列车的安全运行至关重要。它不仅确保了数据通信的实时性和可靠性,而且为未来的无线通信技术提供了坚实的基础。随着云计算、大数据、物联网和人工智能等新兴技术的应用^[5],铁路信息化正在向着更加智能、高效和环保的方向发展,TRDP 将起到越来越重要的关键作用。

0.2 列车互联网安全的研究现状

随着列车互联网技术的快速发展,网络安全已成为铁路系统信息化建设的重要组成部分。国际上,IEC 62443 系列标准为工业控制系统的网络与系统信息安全提供了全面的指导。这些标准涵盖了从安全策略与规程、系统安全要求到组件安全要求的各个层面,为资产所有者、系统集成商和组件供应商等所有利益相关方提供了可遵循的框架。IEC 62443 系列标准的制定是国际自动化协会(International Society of Automa-

tion, ISA) 和国际电工委员会 (International Electrotechnical Commission, IEC) 共同努力的成果, 反映了全球工控安全专家对网络安全重要性的共识。

中国在网络安全标准建设^[6]方面也不遗余力, 特别是在铁路行业。GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》等标准, 确立了网络安全等级保护的基本要求, 这些要求对工业控制系统, 包括列车互联网的安全性有着直接的指导意义。等级保护2.0标准体系进一步强化了网络安全等级保护制度, 提出了更为详细和严格的安全要求。《中华人民共和国网络安全法》和《关键信息基础设施安全保护条例》的实施, 为网络安全等级保护制度提供了法律支撑, 确保了关键信息基础设施, 包括轨道交通的网络安全。

然而, 以太网技术的引入给列车互联网带来了前所未有的挑战。以太网虽然提高了通信速率, 增强了开放性和兼容性, 但同时也为列车互联网打开了与外部环境的交互通道, 这破坏了传统总线式网络相对封闭的“安全壁垒”。这种开放性带来的直接后果是, 列车互联网面临着传统互联网所面临的安全风险^[7], 包括恶意软件攻击、数据泄露、拒绝服务等。威胁范围涉及隐私安全、列车安全、铁路安全、电气安全, 一旦发生事故, 直接危及铁路乘员的生命安全。

作为列车通信网络的核心组成部分, TRDP安全性对整个列车系统的稳定运行至关重要。TRDP面临的安全风险包括洪泛攻击、会话劫持和中间人攻击等。这些攻击手段可以严重影响列车控制系统的正常运行, 甚至可能导致列车运行故障, 威胁乘员安全。尽管TRDP的脆弱性防护至关重要, 且TRDP本身缺乏消息认证和安全传输机制, 但目前国内外在这一领域的研究成果并不丰富。其主要原因在于关键基础设施分析和迭代替换的成本过高, 以及国内外尚未形成一套完整的列车互联网安全研究体系。具体到TRDP的安全研究, 尤其是在实际应用中的安全性验证、风险评估和防护措施的研究, 数量还远远不够。这表明加强对列车互联网特别是TRDP安全性的研究, 已经成为一个迫切需要解决的问题。

0.3 本文的主要工作

针对TRDP缺乏有效安全机制的现状, 分析了TRDP不同传输模式所面临的安全风险与需求, 在此基础上, 提出了基于加密协议的消息源认证机制和改进的安全套接字层 (secure sockets layer, SSL) 安全协议保护TRDP安全, 设计了基于加密算法的TRDP安全方案; 基于哈希获取随机子集 (Hash to obtain random subset, HORS) 机制, 实现了协议过程数据的消息源认证机制, 保障了数据实时性、真实性和可靠性; 基于安全套接层机制, 实现了消息数据的安全传输信道。为了实现SSL对无状态TRDP的支持, 本文对SSL协议做了必要的改进, 并在此基础上设计了一个列车控制应用集成方案。此外, 基于国密算法套件, 本文搭建了一个原型系统, 这个系统展示了如何将这些关键的技术组合起来, 构建一个安全的列车关键基础设施通信系统; 并对系统进行了测试, 结果证明, 本文的防护机制在保障TRDP消息传输机密性、完整性和真实性的基础上, 引入了较小的性能开销; 针对面向不同场景的安全需求, 本文的防护机制均提供了有效保障。

1 TRDP概述

1.1 列车通信以太网协议层次模型

基于工业以太网的列车通信协议的层次模型如图1所示。其中, IEC 61375-2-4对列车控制和管理系统设备的应用层数据和业务行为进行了约定, 主要包括了牵引控制单元、车门控制、空调控制、制动控制等。与传统的WTB/MVB (wire train bus/multifunction vehicle bus) 模式不同, ETB/ECN (ethernet train backbone/ethernet consist network) 体制支持车载多媒体数据, 包括闭路电视监控系统 (closed circuit television, CCTV) 和乘客信息系统 (passenger information system, PIS) 等。车载视频监控系统和PIS的具体要求分别在IEC 62580-2和IEC 62580-4中进行了描述。IEC 61375-2-3明确了ETB/ECN架构下的通信协议架构, 包括列车实时数据协议、过程数据、消息数据、基于统一资源标识的寻址协议等。IEC 61375-2-5、IEC 61375-3-4对ETB、ECN的物理层、链路层、网络层、传输层和应用层分别做了约定。

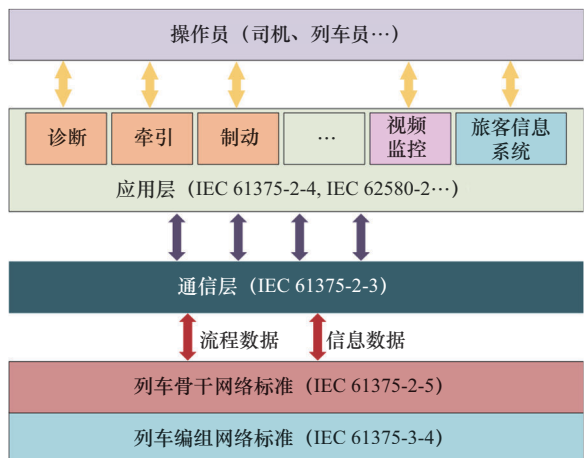


图1 基于工业以太网的列车通信协议的层次模型

Figure 1 Ethernet-based hierarchical model of train communication protocols

在国际标准 IEC 61375 中, 列车通信以太网的组成部分还包括 ETB 和 ECN, 分别针对列车级骨干以太网和车辆级编组以太网进行网络结构、通信格式和内容规约的描述。

国内列车通信以太网的应用发展经历了从早期测试到集中使用的 3 个阶段。随着 GB/T 28029 国家标准的制定, 国内铁路通信网络的建设和发展已经取得了显著进步, 列车通信以太网在多个实验和运行线路上进行了实车搭建测试和运行控制调试, 逐步取代了传统的 TCN 技术, 成为承载列车控制系统通信管理的主体。

1.2 TRDP 协议

列车通信以太网协议栈是现代铁路系统中不可或缺的一部分, 它确保了列车内部各种控制系统、监控设备和乘客服务系统之间的高效、可靠通信。在这一协议栈中, IEC 61375-2-3 标准和 TRDP^[8]起着核心作用。

IEC 61375-2-3 标准是由国际电工委员会和国际铁路联盟 (International Union of Railways, IEC) 共同制定的, 它定义了列车通信以太网的关键部分, 即列车实时数据通信协议。TRDP 是专为铁路通信设计的, 它在传统的以太网 TCP/IP 5 层模型的基础上, 在传输层与应用层之间增加了 TRDP 层, 以强化车内各类数据的传输机制, 实现规范化的车内数据通信。

如图 2 所示, TRDP 协议栈^[8]的技术规范包括物理层、数据链路层、网络层、传输层、会话

层、表示层和应用层。物理层基于 IEEE 802.3 标准, 负责提供物理介质, 如以太网连接线和光纤电缆, 以透明的方式传递比特流。数据链路层则基于 IEEE 802.3 和 IEEE 802.1D 标准, 确保数据帧在相邻节点间无差错传输。网络层采用 IP 协议 RFC 791 标准, 负责数据包的路由和实时传输。传输层则基于 TCP/UDP, 提供稳定的端到端服务和进程通信功能。

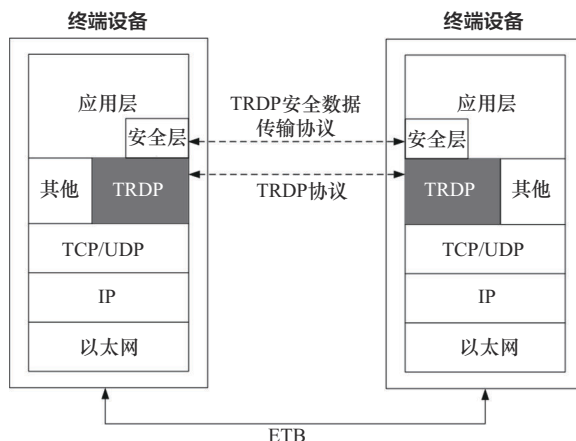


图2 TRDP 协议栈

Figure 2 TRDP protocol stack

在 TRDP 层, 定义了两种实时通信的数据类型: 过程数据 (process data, PD) 和消息数据 (message data, MD)。过程数据通常用于列车运行中的控制命令和状态信息传输, 其特点是数据长度短而实时性要求高。消息数据则用于传输故障报警信息和设备状态信息等。TRDP 层向上层提供过程数据通信服务、消息数据通信服务以及其他功能, 所有数据都遵循大端字节序和字节对齐的原则。

TRDP 层使用通信标识符 (communication identifier, ComID) 作为协议数据单元 (protocol data unit, PDU) 的标识符, 包含在 TRDP 报文头部中。该标识符和源地址 (或者目标地址) 共同作用, 表明了这个数据流的唯一身份。

TRDP 层需要传输层和网络层提供 Socket 服务。TRDP 使用的 Socket 分为 TCP 和 UDP 两种, 实时性要求高的过程数据采用 UDP 通信, 实时性要求低的消息数据采用 TCP/UDP 通信。TRDP 的 Socket 通信与传统 TCP/UDP 基本一致。

TRDP 由 MD 接口、PD 接口、精简 TRDP、使用程序以及虚拟操作系统 VOS 等构成。应用层

通过调用PD、MD接口，实现数据的实时传输；应用程序可以实现TRDP XML配置文件的读取、安全数据传输以及拓扑信息访问等功能；虚拟操作系统提供了不同操作系统的服务接口用于数据传输，其接口如图3所示。

目前TRDP通过行业团体TCNOpen实现了代码开源，为后续的安全性研究提供了良好的基础。

1.3 TRDP通信机制

TRDP的通信过程^[8]主要基于两种数据类型：过程数据和消息数据。过程数据用于周期性的实时控制任务，如速度控制和制动，而消息数据则用于非周期性的事件，如故障报告和系统日志。根据两种不同的数据类型，TRDP定义了特定的数据单元格式，即PD-PDU和MD-PDU，它们包含了必要的头部信息和数据负载。PD-PDU用于过程数据的传输，数据传输的最大等待时间在ETB上应小于20 ms，在ECN上应小于10 ms，而MD-PDU用于消息数据的传输，传输的最大等待时间在ETB、ECN上应小于100 ms。这些数据单

元的设计考虑了列车操作的实时性和数据完整性的需求，两种报文的时延要求见表1。

表1 PD和MD的时延要求

Table 1 Latency requirements of PD and MD

时延要求	过程数据	消息数据
最小循环时间	20 ms	不适用
数据长度	1 500 byte	1 500 byte
最大时延	10 ms	100 ms
最大抖动	10 ms	不适用

1.3.1 TRDP过程数据通信机制

在TRDP中，数据的发送和接收是通过发布者（publisher）-订阅者（subscriber）模型^[8]来实现的。发布者是数据的发送方，而订阅者是数据的接收方。此外，还有请求者（requester）角色，它在需要时向发布者请求数据。其主要通信模式分为：TRDP-PD-PUSH模式和TRDP-PD-PULL模式。

（1）TRDP-PD-PUSH模式

发布者周期性地发送数据，无须订阅者提请

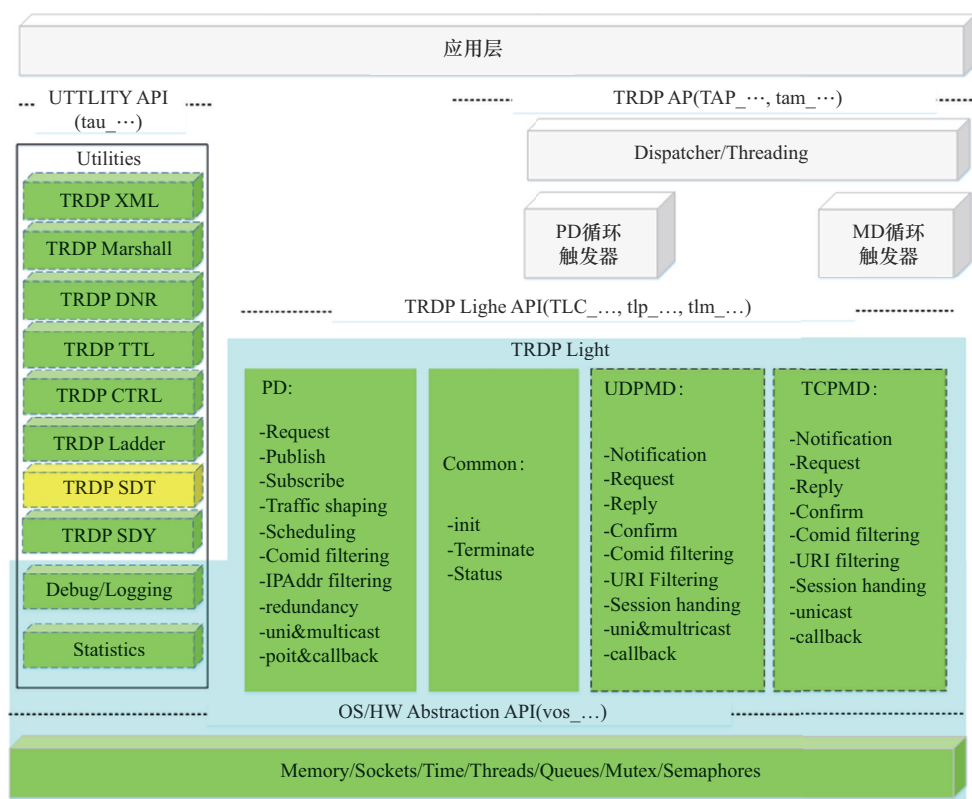


图3 TRDP接口

Figure 3 TRDP interface

求。这种模式适用于需要持续监控的数据,如传感器读数。

PUSH 模式可以分为点对点:数据从一个发布者发送到一个特定的订阅者;点对多点:数据从一个发布者发送到多个订阅者,通常通过多播实现。

(2) TRDP-PD-PULL 模式

在 PULL 模式下,订阅者向发布者发送数据请求,发布者收到请求后响应并发送数据。这种模式适用于按需请求的数据,如配置信息或大型数据集。

PULL 模式的通信方式有点对点:一个订阅者直接从一个发布者请求数据;多点对点:多个订阅者可以从一个发布者请求数据;点对多点:一个订阅者请求数据后,发布者将数据发送给多个订阅者;多点对多点:多个订阅者从多个发布者请求数据,发布者通过广播方式回应所有请求者。

1.3.2 TRDP 消息数据通信机制

消息数据通信模型中,参与通信的实体被划分为两种角色:呼叫者和应答者。呼叫者是发起通信请求的一方,而应答者则是响应这些请求的一方。这种模型支持高效且可靠的数据交换,适用于实时数据传输的需求。

在 TRDP 中,呼叫者负责发起消息传输。当呼叫者请求发送消息时,它会检查拓扑计数器以确保网络拓扑的一致性。发送通知消息时,会话标识符被设置为 0,而发送请求消息时,则会创建一个新的呼叫者会话,并使用基于时间的 UUID 确保会话的唯一性。呼叫者还负责定义应答消息的超时值,并在会话期间等待来自应答者的应答。如果应答者请求确认,呼叫者必须在指定的时间内提供确认,否则会话将被关闭。此外,如果应答超时或在等待确认时超时,呼叫者会被通知会话将结束。

应答者作为侦听者,对接收的消息进行处理。它必须注册为特定 URI 或 ComID 的 MD 的侦听者,并检查所有输入消息的拓扑计数器。如果接收到请求消息,应答者会打开一个新的会话,并启动超时定时器,等待侦听者的回复。应答者根据侦听者的回复发送确认或无确认的应答消息,并在必要时重启超时定时器。如果应答者收到的

确认消息与打开的会话不匹配,它将通知侦听者并关闭会话。应答者还负责在超时或其他异常情况下通知侦听者,并在会话结束时释放资源。

2 SSL 概述

SSL 协议是广泛使用的,同时支持消息机密性、完整性和可用性的安全协议。国内 SSL 通信^[10]依据 GM/T 0024--2014 SSL VPN 技术规范协议。在 SSL 协议中,客户端和服务端会根据优先级选择一个双方都支持的加密套件来进行后续的加密操作。SSL 协议族由握手协议、密码规格变更协议和报警协议组成,这里主要讨论握手协议。

在握手阶段,客户端和服务端建立连接并交换“hello”消息,协商协议版本、会话 ID、密码套件和随机数。客户端发送 ClientHello 消息,包括协议版本和密码套件。服务端回应 ServerHello,确认协议版本和加密方法。接着,服务端发送双证书模式下的两个证书(签名和加密证书),可能还会请求客户端证书以验证身份。ServerKeyExchange 消息包含密钥交换信息,ServerHelloDone 消息告知客户端所有必要信息已发送。

客户端响应包括发送自己的证书、进行密钥交换、可选地进行证书验证。完成这些步骤后,客户端发送 ChangeCipherSpec 消息,通知服务端将使用新的会话密钥进行通信。最后,客户端和服务端交换 Finished 消息,完成握手,建立加密通信。

3 HORS 概述

为了确保消息的完整性和真实性,一次性签名(one time signature, OTS)方案被提出作为一种高效的认证方法。然而,传统的 OTS 方案存在两个主要的局限性:较大的签名尺寸和一次性使用的限制。为了克服这些限制,哈希获取随机子集^[11]算法被开发出来,它不仅提高了计算效率,还允许在一定条件下重复使用密钥。

HORS 算法基于无陷门的单向函数,这意味着它可以在不牺牲安全性的前提下,提供快速的签名生成和验证。这一特性使得 HORS 特别适合需要快速消息认证的场景,如电力系统中的变电站自动化系统(substation automation system, SAS)。HORS 的一个显著优点是它生成的签名相

对较短，这对于需要传输和存储大量签名的系统来说是一个巨大的优势。

此外，HORS算法允许所谓的“多次性”使用，即使用同一个密钥签署多条消息。这一点在保持适当的安全级别的同时，为用户提供了更大的灵活性。然而，密钥的重复使用会导致安全级别的降低，因此需要仔细管理密钥的使用频率和周期，以确保系统的安全。

时间有效的HORS (TV-HORS) 方案是HORS算法的一个变种，它专门为工业互联网场景中的时效性消息设计。在TV-HORS中，一个HORS密钥可以在一个预定的时间周期内重复使用来生成多个签名。这种方法虽然会导致安全级别的快速下降，但如果管理得当，仍然可以保持足够的安全性，以抵御潜在的攻击。

HORS算法的工作原理可以概括为3个步骤：密钥生成、签名和验证。其主要算法流程如下。

(1) 密钥生成——输入：参数 l, k, t

1) 由密钥生成器随机生成 t 个随机的 l 位字符串 $s_1, s_2, \dots, s_t$ ；

2) 对每个满足 $1 \leq i \leq t$ 的情况，计算 $v_i = f(s_i)$ ，输出得出的公钥 $PK = (k, v_1, v_2, \dots, v_t)$ 和对应的私钥 $SK = (k, s_1, s_2, \dots, s_t)$ 。

(2) 签名过程——输入：待签名的消息 m 和私钥 $SK = (k, s_1, s_2, \dots, s_t)$

1) 计算散列值 $h = \text{Hash}(m)$ ；

2) 将上一步计算出的 h 分成 k 个子字符串

$h_1, h_2, \dots, h_k$ ，每个子字符串长度为 $\text{lb } t$ 位；

3) 将每个 h_j 解释为一个整数 i_j ，对每个满足 $1 \leq j \leq k$ 的情况，输出签名 $\sigma = (s_{i_1}, s_{i_2}, \dots, s_{i_k})$ 。

(3) 验证过程——输入：消息 m ，待验证的签名 $\sigma = (s_{i_1}, s_{i_2}, \dots, s_{i_k})$ 和被验证者的公钥 $PK = (k, v_1, v_2, \dots, v_t)$

1) 计算散列值 $h = \text{Hash}(m)$ ；

2) 与签名过程类似，将 h 分成 k 个子字符串 $h_1, h_2, \dots, h_k$ ，每个子字符串长度为 $\text{lb } t$ 位；

3) 将每个 h_j 解释为一个整数 i_j ，对每个满足 $1 \leq j \leq k$ 的情况，进行验证：如果对满足 $1 \leq j \leq k$ 的每个 j ，都满足 $f(s_{i_j}) = v_{i_j}$ ，则输出“接受”，否则输出“拒绝”。

在密钥生成阶段，会生成一组随机字符串作为私钥，并通过单向函数生成相应的公钥。签名阶段涉及对消息进行散列处理，并将散列值分割成多个子字符串，这些子字符串随后被转换成整数，用于从私钥中选择相应的字符串生成签名。在验证阶段，接收方通过执行类似的哈希处理和分割操作，然后使用公钥来验证签名的有效性。

4 改进的TRDP安全通信模型设计

4.1 模型设计

TRDP安全通信模型如图4所示，为了使本文的方案模块化、易扩展且不需要修改关键基础设施协议组件，对于过程数据，使用基于散列算

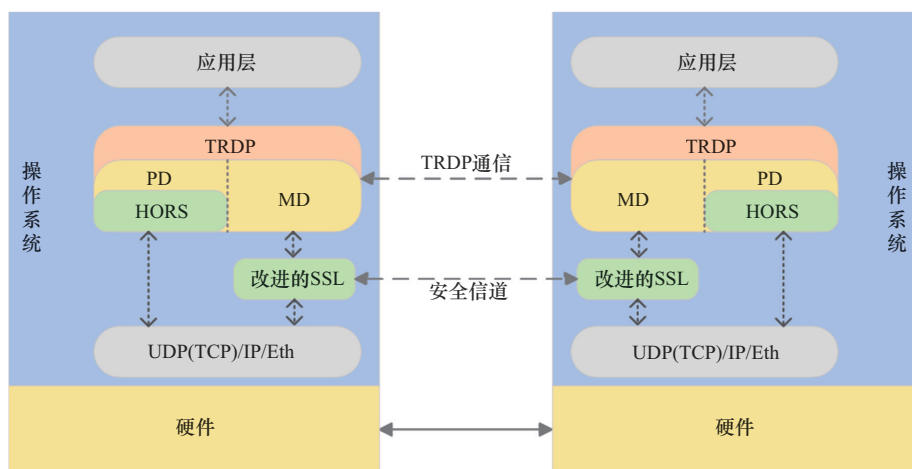


图4 TRDP安全通信模型

Figure 4 TRDP secure communication model

法的 HORS 来进行消息源验证, 并内嵌入 TRDP 的 PD 数据包中, 从而保证传输的可靠性和安全性。对于消息数据, 实体之间采用了改进的支持无状态的 SSL 协议来处理消息数据的密钥协商和隧道建立, 并通过这些认证的隧道传输, TRDP 数据包密钥协商的可靠性由重传计时器和超时重传机制实现。此外, 该组件还维护了一个基于 TRDP 的 ComID 生成的 Cookie 池, 以此抵御 DDoS 攻击和洪泛攻击。

4.2 针对过程数据的安全设计

4.2.1 安全性和性能需求

TRDP-PD 协议的安全性需求集中在确保数据的完整性和真实性上, 这对于列车控制和监控应用至关重要。结合 PD 协议的安全威胁, 根据 IEC 61375-1 和 IEC 61375-2-3 的要求, 总体来说, 过程数据的安全机制需要满足如下要求:

- 1) 保证通信的真实性和完整性;
- 2) 对消息时延的影响尽可能小;
- 3) 支持多播。

为了防止数据在传输过程中被篡改或伪造, 必须实施签名和认证机制。同时, 考虑到周期性数据的特点, 一个高效的密钥管理系统对于定期更新密钥以防止密钥泄露是必不可少的。此外, PD 协议的安全机制必须具备抵御重放攻击、拒绝服务攻击和密钥耗尽攻击等多种网络威胁的能力。这要求需要使用支持密钥更新的安全机制来验证消息的新鲜度, 以及确保系统有足够的资源来处理大量的安全验证操作, 从而维持通信的安全性和稳定性。

PD 协议的性能需求强调了极低的时延和高效的数据处理能力。具体来说, 数据传输的最大等待时间在 ETB 上应小于 20 ms, 在 ECN 上应小于 10 ms, 这对安全机制提出了严苛的时延要求, 以便在不影响数据传输实时性的前提下完成认证操作。考虑到数据可能需要通过多播方式发送到多个设备, 安全方案还必须支持多播消息认证机制。此外, 安全机制的实施不应过度消耗系统资源, 特别是在资源受限的嵌入式系统环境中。因此, 安全方案必须在保障安全性的同时, 最小化对系统资源的占用, 确保在不牺牲性能且不影响协议正常工作的情况下实现所需的安全保护。

基于以上安全需求, 本文使用改进的 HORS

协议, 在保障数据安全性的同时, 满足 PD 协议对实时性和多播的要求。

4.2.2 安全设计

在密钥管理方面, 基于 HORS 设计了一个轻量级的密钥生成和分发系统。由于 TRDP 要求过程数据的传输时延在 10 ms 以内, 密钥生成过程必须迅速, 以避免造成额外的时延。因此使用预生成密钥的策略, 在系统空闲时生成一批密钥, 将它们统一存储并分发给所有节点, 并在需要时启用。此外, 密钥的分发应该保证安全性, 这里使用改进的 SSL 隧道进行密钥交换, 并通过预先建立好的安全通道来更新密钥。为了减少管理开销, 采用 ETB 分层密钥管理架构, 将密钥分配给不同的 ECN 区域, 每个区域内部建立相对独立的密钥更新和分发机制, 不同 ECN 之间由密钥管理服务器使用定期握手和猝发方式同步时序和证书。

签名生成过程需要在不牺牲安全性的前提下尽可能保持高效。考虑到 HORS 方案的计算效率, 允许密钥的缓存和重用, 以加快签名过程。为了进一步减少处理时间, 签名在数据包即将发送前的最后一刻生成, 确保签名的实时性。此外, 为了避免重复计算, 对于周期性发送的 PD, 采用缓存机制, 对相同内容的数据包只进行一次签名, 直到下次密钥更新时发送新签名。

签名验证是保证数据完整性和认证的关键步骤。订阅者在接收到 PD-PDU 后, 必须迅速验证签名的有效性。为了满足 10 ms 的严格时延要求, 验证算法需要高度优化。采用缓存队列验证周期性签名, 减少对相同内容的重复验证; 同时, 采用快速失效机制, 在检测到签名无效时立即丢弃队列中数据包, 以避免对系统造成更大的影响。

密钥更新机制必须既要保证系统的安全性, 又不能影响实时数据传输。采用动态密钥更新策略, 根据网络负载和数据传输频率来调整密钥更新的频率。为了防止密钥耗尽攻击, 本文为密钥设计了生命周期, 在使用后或达到预设的时间阈值后扣除, 并在达到预设的使用阈值之前自动触发更新过程。此外, 密钥更新过程并不基于过程数据, 不影响正在进行的数据传输。

时延管理要求系统能够在保证安全性的同时, 满足 PD-PDU 的实时传输需求。这需要对网络进行

精细的时间同步和调度优化。利用现有的时间同步协议来同步网络中所有设备的时钟。此外，网络协议需要配置优先级队列，确保PD-PDU可以优先传输。采用基于滑动窗口的时延预测模型，动态调整数据包发送和处理的数目，以适应不同的网络条件。

4.2.3 数据包设计

如图5所示，为了使PD-PDU数据包原生支持HORS算法的数据元认证，本文提出以下改进方案，以便在PD-PDU载荷中携带公钥和数据源认证信息的哈希值。根据TRDP文档，PD-PDU提供的‘reserved01’字段，原本用于功能扩展，可用于标记公钥信息和数据源认证信息载荷的起始地址。具体改进措施包括如下内容。



图5 改进的PD-PDU

Figure 5 PD-PDU improvements

(1) 调整 reserved01 字段

1) 利用 reserved01 字段的前 8 位存储公钥信息的地址；

2) 使用 reserved01 字段的后 8 位记录签名信息的地址。

此调整既充分利用现有字段，又为新增加的认证机制提供必要的地址信息。

(2) 填充 dataset 字段

1) 在 dataset 字段末端附加公钥信息和签名信息；

2) 公钥信息负责签名的真实性验证；

3) 签名信息由 HORS 算法生成，覆盖数据包包含的 PD-PDU 其他字段内容。

(3) 数据包结构优化

1) 对数据包结构进行适当调整，以适应公钥和签名信息的加入，通过增加 datasetLength 字段的值来反映额外数据的长度；

2) 确保新加入的信息不影响数据包的其他内容。

(4) 验证过程优化

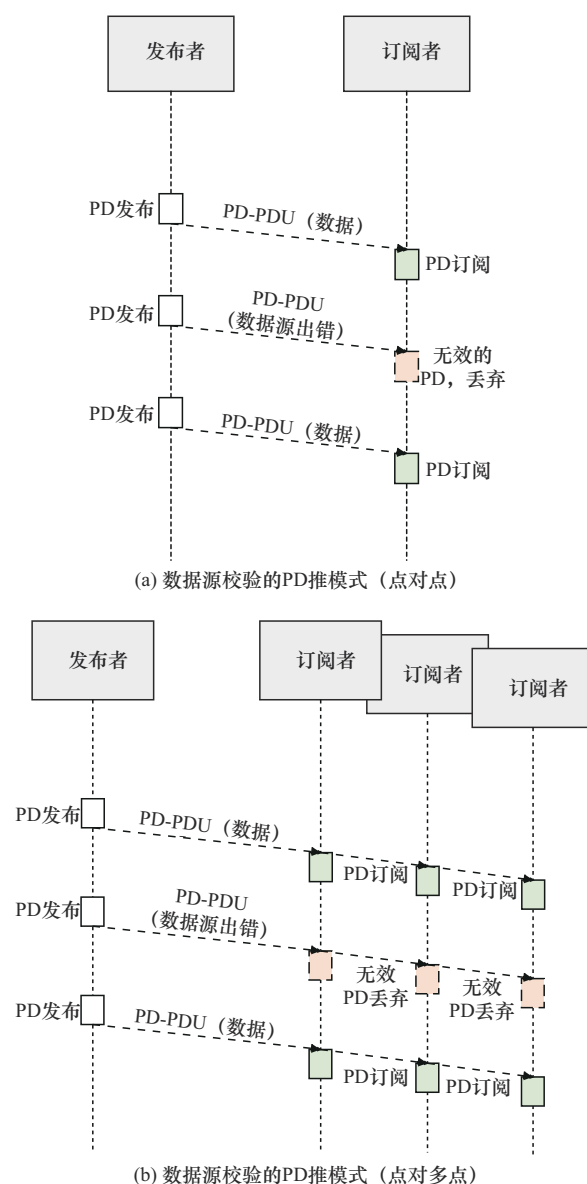
1) 接收方根据 reserved01 字段中记录的地址提取公钥和签名信息；

2) 利用提取的公钥验证签名，确保数据包的真实性和完整性。

通过以上设计，PD-PDU 数据包不仅能传输原有信息，还可以在支持多播的场景下，利用 HORS 算法确保数据的真实性和完整性。

4.2.4 改进的通信模式

如图6和图7所示，结合 TRDP 和 HORS 算法，本文针对 TRDP-PD 的不同通信模式，设计支持数据源校验的改进通信模式。



(b) 数据源校验的PD推模式（点对多点）

图6 改进的PD-PUSH模式

Figure 6 Improved PD-PUSH mode

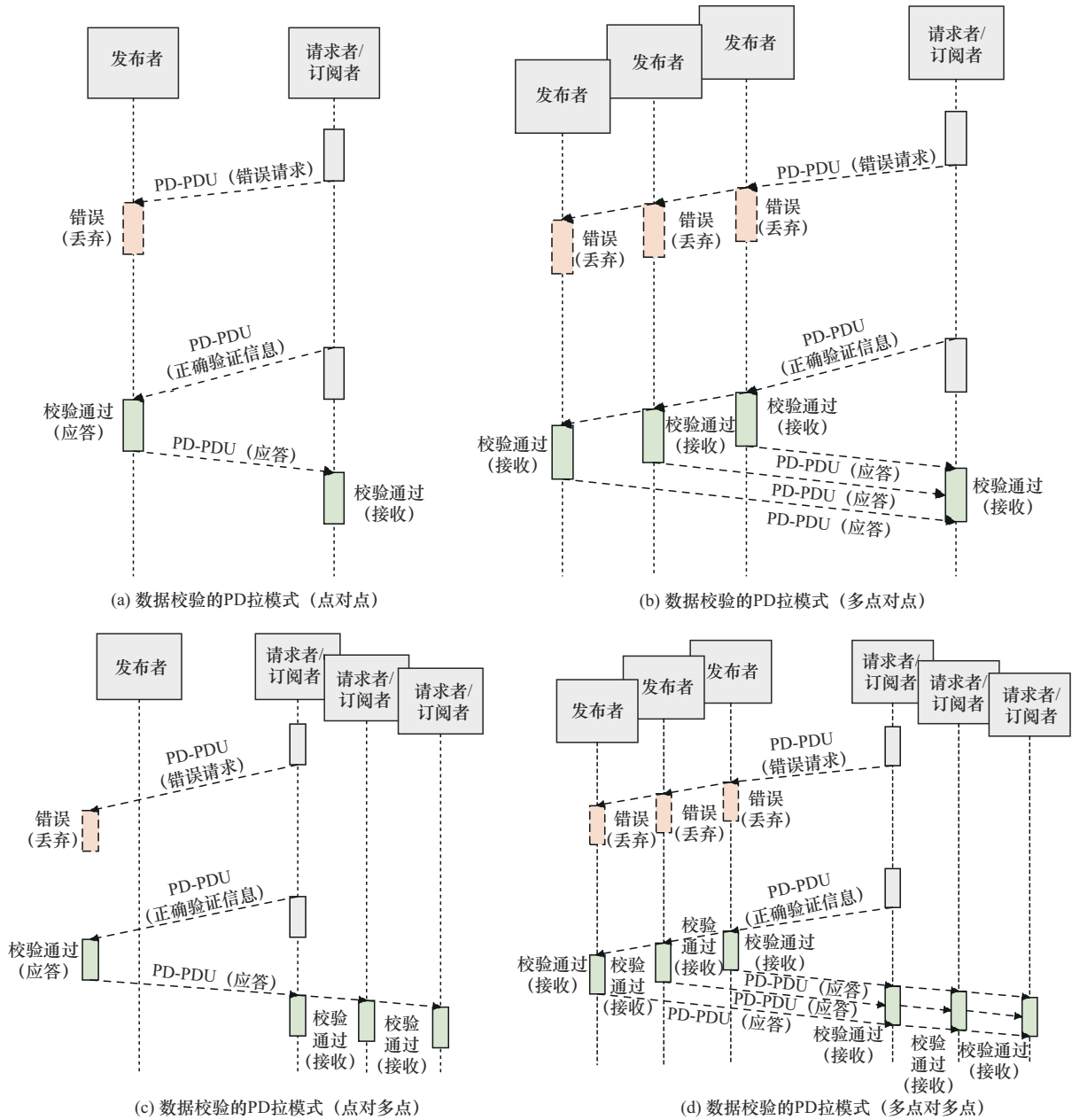


图7 改进的PD-PULL模式

Figure 7 Improved PD-PULL mode

(1) TRDP-PD-PUSH模式

1) 点对点: 发布者对数据进行HORS算法签名, 然后将带有签名的数据包发送给特定的订阅者。订阅者接收数据后, 使用预先共享的公钥验证签名的真实性和完整性, 用以确认是否接收。

2) 点对多点: 发布者对数据进行一次使用散列函数的签名, 并通过多播将带有签名的数据包发送给多个订阅者。每个订阅者使用相同的公钥

验证数据。

(2) TRDP-PD-PULL模式

1) 点对点: 订阅者向发布者发送含有自身签名的数据请求。发布者验证通过后响应请求, 对数据进行HORS签名再发送给订阅者。订阅者接收后使用公钥验证签名。

2) 多点对点: 多个订阅者可以向同一个发布者发送签名后的数据请求。发布者对每个请求单独进行验证和群体响应, 发送经过HORS签名的

数据。每个订阅者使用公钥独立验证签名。

3) 点对多点: 单个订阅者发送签名的数据请求后, 由发布者验证, 成功后对响应数据进行一次HORS签名, 然后将签名数据发送给多个订阅者。各订阅者使用公钥验证签名。

4) 多点对多点: 多个订阅者向多个发布者请求数据, 每个发布者验证请求后, 对数据进行HORS签名, 通过广播方式回应所有请求者。每个订阅者使用公钥验证其接收到的数据。

在所有情况下, 使用HORS签名的目的是确保数据的真实性和完整性。为了实现这一点, 需要在发布者和订阅者之间安全地共享公钥。为了保证不影响PD数据的传输, PD协议的密钥交换使用下面提到的SSL安全信道完成。此外, 对于多播或广播的情况, 确保所有订阅者都有正确的公钥来验证签名至关重要, 需要配合分层公钥基础设施(public key infrastructure, PKI)架构来实现密钥同步。这样的设计方案在保证TRDP-PD通信效率的同时, 通过引入面向时延敏感的验证协议, 满足了过程数据对真实性和完整性的安全需求。

4.3 针对消息数据的安全设计

4.3.1 安全性和功能需求

TRDP-MD消息数据在处理如故障报告、系统日志和关键数据传输等非周期性事件时尤为关键。根据IEC 61375-2-3的内容和消息数据的安全威胁场景, 总体安全性需求如下:

- 1) 确保消息的机密性、完整性和真实性;
- 2) 确保消息的按时到达;
- 3) 支持无状态协议。

TRDP默认设置的消息数据使用明文传输且缺乏身份认证机制, 这导致TRDP-MD面临着众多安全威胁, 包括信息劫持、数据篡改和中间人攻击。攻击者能够轻松渗透到ETB系统的ECB中, 利用嗅探、劫持等技术拦截并篡改通信数据, 从而可能导致列车设备的故障及其他严重后果。因此, 不同于PD协议, 针对MD协议, 需要设计强大的加密和身份认证机制, 以确保数据的机密性、完整性和真实性, 有效阻止网络攻击和信息泄露。

相较于PD协议, MD协议的时延要求虽然

相对宽松, 但其应用场景对实时性仍有一定的需求。考虑到车载设备的计算能力通常有限, MD协议对安全机制的性能优化需求至关重要。即使MD的最大时延要求为100 ms, 安全机制的设计仍然需要具备高效性, 以保证在低算力条件下也能实现实时数据传输。这意味着握手和加解密操作必须迅速且不影响数据传输的实时性。鉴于列车互联网设备通常资源有限, 安全方案的实现同样需要尽可能轻量, 以最小化对系统资源的占用, 尤其针对资源受限的环境, 如嵌入式控制系统或车载设备。因此, 方案设计时应平衡安全性需求和资源需求, 保证在不牺牲通信效果的情况下实现安全保护。

此外, TRDP的PD协议要求同时支持TCP和无状态的UDP, 数据包传输层安全性^[12](datagram transport layer security, DTLS)协议是在SSL协议的基础上, 一个支持无状态协议的改进版本, 但DTLS协议的实现和机制设计较为臃肿, 无法满足低时延和轻量化的要求。本文参照DTLS的设计原则, 对SSL协议稍加改进, 使其在保留SSL的性能和安全性情况下, 支持使用无状态协议交换握手信息、收发密钥和加解密信息。

基于这些安全性和性能需求, 选择了对SSL协议做无状态改进, 作为安全解决方案。通过采用非对称加密算法来分发、更新和交换信道密钥, 使用对称加密来完成通信, 这种方案既保障了数据的机密性、完整性和真实性, 又满足了车载互联网对性能的需求。

4.3.2 安全设计

基于PKI体系, 本文设计了一种改进的SSL密钥交换和信道安全机制。在这个设计中, 首先利用PKI体系下的认证中心来分发和管理基于非对称算法生成的数字证书, 确保每个通信实体(呼叫者和应答者)都拥有经过验证的身份凭证。当呼叫者发起安全通信请求时, 它会发送包含随机数和所选用加密套件的连接请求。应答者响应这一请求, 提供自己的随机数、选择的加密套件和数字证书, 还需要呼叫者的证书以实现双向认证。在证书被验证后, 呼叫者生成一个预主密钥并用应答者的公钥加密发送。

接着, 双方通过各自的随机数和预主密钥生成会话密钥。此过程涉及密钥派生函数, 基于散列算法来保证密钥的安全性和独立性。之后, 双方利用派生的会话密钥 (基于对称算法) 对数据进行加密和解密, 以确保数据传输的机密性。整个 SSL 通信流程不仅在身份认证阶段提供了强大的安全保障, 而且在数据传输过程中通过加密保护了数据的安全。

在性能优化方面, 主要考虑了 MD 协议的实时性和性能需求。为了满足这一需求, 采取了几项关键的性能优化措施。首先, 改进的 SSL 支持无状态的 UDP, 这使得可以使用 UDP 维持加密信道, 从而省去了每次发送数据所需的烦琐握手流程。这一改进对于提升数据传输的速度和效率至关重要。其次, TRDP 消息机制的请求包被封装进预共享密钥的数据包中。这种设计使得在 SSL 握手完成后, MD 应答和确认过程可以立即执行, 从而减少了整体通信的时延。最后, 为了进一步提高通信效率, 首次握手建立的安全信道被设计为可以被后续通信复用。这意味着一旦安全信道建立, 它将持续有效, 直到信道关闭或证书失效。这种机制不仅提高了通信的效率, 也减轻了频繁建立和取消安全信道所带来的性能负担, 更适合 TRDP 的应用场景。

通过这种设计, 本文有效地结合了 PKI 体系的可靠证书管理机制和 SSL 算法的安全特性, 实现了一种既安全又高效的密钥交换和信道建立机制。利用这些优化措施, 改进的 SSL 协议能够更好地适应实时性强、资源受限的通信环境, 特别是在列车互联网系统等关键应用场景。

4.3.3 数据包的设计

为了保障通信的 TRDP 的实时性要求, 下层协议栈同时采用了 TCP 和 UDP 协议, 要实现通过安全隧道对 TRDP 的保护, 势必要实现 SSL 对无状态连接协议的支持。为了实现改进 SSL 对无状态 MD 数据的支持, 需要在协议附加字段上对 SSL 数据包加以改进。

如图 8 所示, 本文基于 TRDP 的部分字段对 SSL 协议机制做了如下增改。

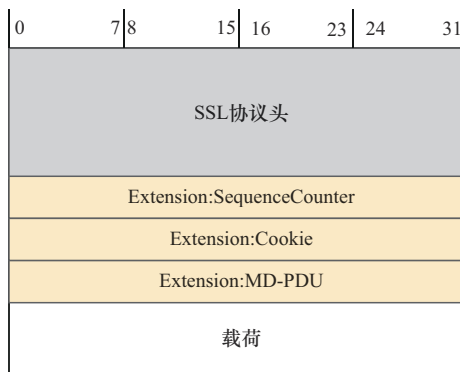


图8 改进的 SSL 数据包
Figure 8 Improved SSL packets

1) 增设消息丢失容忍机制: SSL 协议不会在记录之间保留加密上下文, 为了解决记录间的依赖问题, DTLS 通过增加显式序列号来解决这个问题。而 TRDP 采用的 SequenceCounter 字段可以很好地替代计数器来提供数据包时序信息, 在修改的 SSL 协议数据包的扩展字段处, 定义了 SequenceCounter 字段, 直接同步 MD 数据包的时序。使接收方能快速确定是否为下一个预期消息, 使用位图窗口进行接收记录的重放检测, 支持重排序和丢失处理。同时通过手动维护一个缓存和超时重传机制来确保握手过程的可靠性, 即使在数据包丢失的情况下也能完成握手。

2) 增设会话保持和防伪机制: DTLS 使用 Cookie 保持无状态握手建立的可用性, 同时防止洪泛和重放攻击。TRDP 消息数据的 ComID 标识了使用消息数据的用户程序身份, 可用于标识请求者的唯一性, 在改进的 SSL 协议中, 每个通信实体维护一个 Cookie 池, Cookie 由应答者使用呼叫者的 ComID, 结合应答者收到第一个握手包的时间戳生成。

3) 在 ChangeCipherSpec 数据包中封装 MD 请求: 为了提高 TRDP 消息数据的传递效率, 在 SSL 握手消息中封装消息数据的请求发送通知 (Mn) 或请求消息 (Mr), 在握手的过程中实现数据的准备, 并在握手结束后发送接下来的 MD 数据。

4.3.4 安全隧道协商流程设计

经过对数据包的修改, SSL 的协商机制也需要做出针对无状态协议的适配, 如图 9 所示, 改进后的无状态协商机制如下。

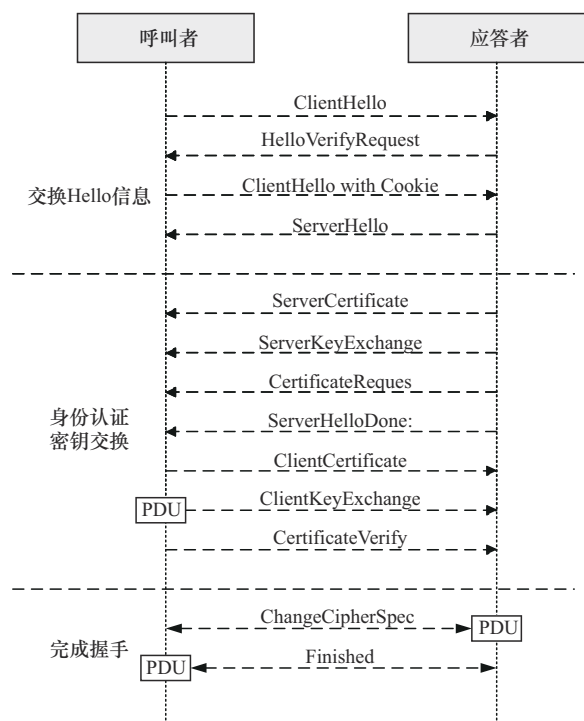


图9 改进的SSL握手流程

Figure 9 Improved SSL handshake process

(1) 交换Hello信息阶段

1) **ClientHello**: 呼叫者发送第一个 ClientHello 消息, 包括协议版本、支持的密码套件、压缩算法、会话 ID 以及呼叫者随机数。此时, Cookie 字段为空。

2) **HelloVerifyRequest**: 应答者接收到 ClientHello 后, 不立即进入状态保持模式, 而是发送一个 HelloVerifyRequest 消息给呼叫者, 该消息包含应答者生成的 Cookie 值。

3) **ClientHello with Cookie**: 呼叫者收到 HelloVerifyRequest 后, 重新发送 ClientHello 消息, 这次包含应答者提供的 Cookie 值。这一步验证了呼叫者的可达性, 防止了 DoS 攻击。

4) **ServerHello**: 应答者验证 Cookie 后, 发送 ServerHello 消息, 包含协议版本、选择的密码套件、压缩算法以及应答者随机数。

(2) 身份认证和密钥交换阶段

1) **ServerCertificate**: 应答者发送 ServerCertificate 消息, 包含其公钥证书 (签名证书和加密证书)。

2) **ServerKeyExchange**: 应答者发送 ServerKeyExchange 消息, 提供密钥交换所需的额外

信息, 如临时公钥或其他参数。

3) **CertificateRequest**: 应答者需要呼叫者认证, 发送 CertificateRequest 消息。

4) **ServerHelloDone**: 应答者发送 ServerHelloDone 消息, 表示应答者已经发送了所有握手消息。

5) **ClientCertificate**: 呼叫者发送 ClientCertificate 消息, 提供其公钥证书。

6) **ClientKeyExchange**: 呼叫者发送 ClientKeyExchange 消息, 包含加密的预主密钥或生成预主密钥所需的信息, 载荷中包含使用预主密钥加密的 MD 请求包。

7) **CertificateVerify**: 呼叫者发送 CertificateVerify 消息, 包含所有握手消息的签名, 以验证呼叫者的身份。

(3) 完成握手阶段

1) **ChangeCipherSpec** (呼叫者和应答者): 呼叫者和应答者都发送 ChangeCipherSpec 消息, 通知对方将开始使用协商的密码算法进行加密通信, 载荷中包含使用预主密钥加密的 MD 应答包。

2) **Finished** (呼叫者和应答者): 呼叫者和应答者交换 Finished 消息, 包含之前所有握手消息的 MAC 值, 确保握手过程未被篡改, 载荷中包含使用会话密钥加密的后续 MD 应答包或确认包。

在整个过程中, 应答者不保持任何握手状态, 直到它接收到包含有效 Cookie 的 ClientHello 消息。这种无状态的握手减少了应答者的资源消耗, 并提高了对 DoS 攻击的抵抗力。同时, 由于 UDP 的不可靠性, 所有消息都需要包含足够的会话信息以允许独立处理, 并且必须实现消息的重传机制以处理丢包情况。

5 原型系统与性能分析

5.1 模型设计

为了评估上文设计的安全机制在满足协议安全性需求的同时, 对协议正常运行的影响, 需要搭建一个列车互联网仿真系统。

列车仿真实验平台以半实物的方式构建, 硬件系统主要包括平台主控端和被控端, 硬件系统结构框架如图 10 所示, 简化后搭建模拟硬件系统, 平台采用实时以太网, ETB&ECN 网络结构, 简化后的列车包含 3 节车厢, 包含主控模块

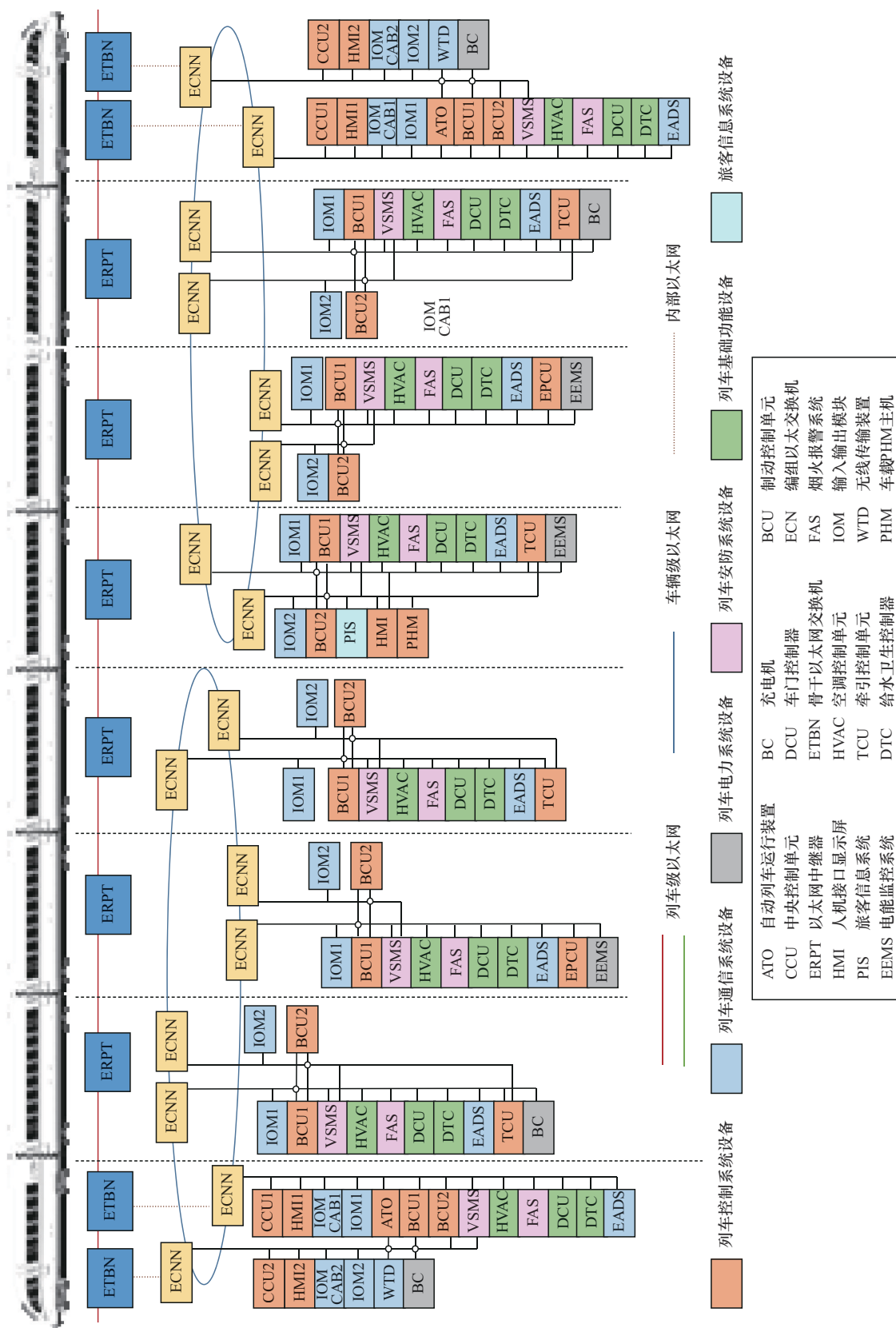


图 10 硬件系统结构框架

Figure 10 Hardware system architecture framework

EGWM×1、自动控制系统ATC×1、乘客信息系统PIS×1、门控系统EDCU×6、空调系统HVAC×3、制动系统BCU×3、牵引系统DCU×1、辅助逆变器SIV×2,全部采用树莓派4B型号模拟设备。

仿真平台软件系统是一个简化的CBTC应用,模拟了列车运行所需的一系列交互,包括联锁系统、移动授权、移动监控、人机交互和列车控制模拟。联锁系统控制物理开关,使用改进后的PD协议传达轨道信息和火车相对位置信息。车载设备计算安全速度限制,并使用改进的MD协议反馈给联锁控制系统。实际ETCS应用中,移动授权和轨道信息通过应答器和RBC接收,而在仿真系统中,火车只接收包含开关设置和火车位置的轨道图,由车载应用生成数据以确保火车安全运行。

改进的安全协议基于TCNOpen提供的TRDP组件,结合国密套件开发,HORS使用SM3实现散列功能,改进的无状态SSL使用SM2套件交换证书和密钥,使用SM4套件完成加密隧道的通信,PKI使用存有预共享证书的XML配置文件模拟实现。通过这种软硬件结合的方式,实现了一个简单的列车互联网测试系统,用以评估本文安全方案是否在保障TRDP不同场景安全需求的情况下,能够满足列车互联网时延敏感的要求。

5.2 性能度量与参数设置

在评估TRDP协议的PD和MD消息以及相应的安全方案时,采用了消息验证比率(message verification ratio, MVR)作为性能度量,这是因为传统的网络度量如时延、吞吐量和数据包丢失率并不能完全揭示安全方案是否满足TRDP的严格时间要求。在度量改进的SSL协议时,达成通信的最关键因素在于隧道的协商,因此主要以握手成功率作为消息验证率,用来度量改进的SSL协议性能。

在本文的测试中,对于HORS,采用了一个160字节的签名,由从1 024个随机字符串中选择的16个10字节的字符串组成。对于改进的SSL协议,采用了国密SSL套件推荐的安全参数设置,在确保足够的安全级别的同时提高计算效率。

5.3 实验结果

本文对TRDP中的PD和MD进行了性能测

试,以评估使用HORS和改进的无状态SSL方案后,对TRDP的影响。

1) SSL签名消息。第一个实验是在以太网总线上传递SSL签名的MD消息。图11显示了验证比率在不同TRDP消息长度下,随通信双方CPU频率的变化,以20 ms作为时延阈值。结果如图11所示,与消息长度相比,SSL握手的消息验证比率更易受CPU频率的影响,在提高握手双方的CPU频率时,MVR显著上升,从400 MHz时MVR不到40%增加到1.6 GHz时MVR超过85%。这个结果再次确认SSL性能主要受车载设备的处理器性能影响。即当非对称算法认证应用于列车互联网设备时,设备性能是需要首要考虑的关键因素。

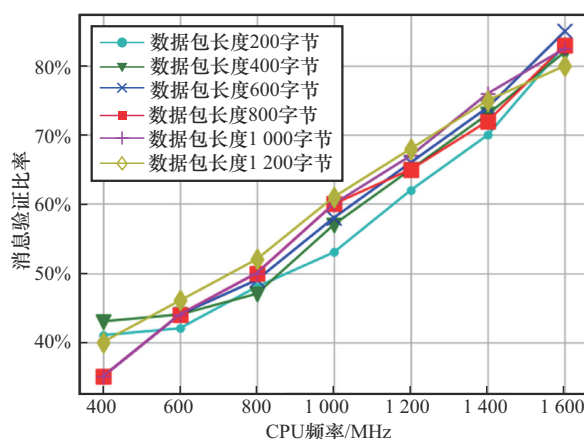


图11 不同数据包长度下,SSL签名消息的消息验证比率

Figure 11 In the case of different data packet lengths, the data packet verification ratio for SSL signature messages

在第二个实验中,测试了不同方案分别在PD和MD协议上的性能,将时延约束从10 ms放宽到20 ms(如图12所示),SSL隧道消息的性能将显著赶上没有数字签名的原始消息。在这种情况下,SSL成为列车互联网安全应用的合适选择。对于MD数据,使用改进的SSL的方案在以太网总线上的表现同样相当出色。尽管MD数据的实时性要求不如PD数据严格,但该方案仍然保证了较高的消息验证率,显示出其在保证安全性的同时,对性能的影响较小。

2) HORS签名消息与MAC机制比较。在图12的实验中,测试了不同方案在PD协议上的性能,大多数情况下,原始消息、MAC附加消息和HORS签名消息的消息验证比率几乎相同。唯一

的例外是当 CPU 频率设置为 600 MHz 时, MAC 附加和 HORS 签名消息的消息验证比率比原始消息低约 5%。尽管如此, 它们仍然接近 90%。因此, MAC 和 HORS 可以说是以太网中满足低时延完整性校验需求的理想验证方式。对于 PD, HORS 方案在以太网总线上的实现显示出了极低的时延, 在测试中, PD 消息的 MVR 接近 100%, 这意味着几乎所有的 PD 消息都在规定的时延阈值内成功验证并传递, 满足了 PD 协议对实时性的要求。

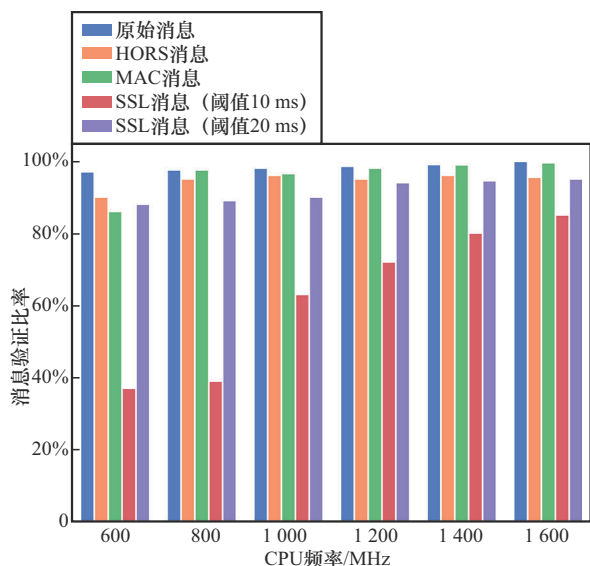


图 12 不同安全方案的性能比较

Figure 12 Performance comparison of different security solutions

6 结束语

本文研究了基于 TRDP 不同消息类型的安全性需求, 并结合 SSL 隧道和 HORS 机制, 设计了 TRDP 在列车通信网络中的安全解决方案, 特别介绍了针对 PD 协议验证机制的重新设计以及对 SSL 安全协议的无状态改进。并通过在一个模拟列车控制系统原型上开展的实验, 验证了方案的可行性。

在 TRDP 安全通信机制的方案中, 主要挑战是基于两种不同的消息类型, 在确保消息安全的同时, 充分利用有限的算力, 满足其不同的安全性和时效性要求。本文对 TRDP 的安全性需求进行分析, 并对不同的实现做了深入研究, 基于本文设计的安全机制, 观察到了几个有趣的现象。尽管以太网现有的安全机制为保障信息安全提供

了强有力的技术保障, 但在高速移动的列车环境中, 对于那些时延敏感的消息, 传统的安全算法可能不适用。研究结果揭示了列车控制系统的多样化应用环境 (如车载设备的计算能力以及时效性要求), 对安全通信方案的性能有直接和显著的影响。这直接影响了安全机制在列车互联网系统中实现的可行性。更重要的是, 安全协议设计的限制, 包括复杂的计算过程、额外的等待时延和密钥有效期, 可能会在实际应用到列车通信网络时, 将算法的优势转变为可靠性漏洞。因此, 需要针对列车互联网的安全需求, 为列车通信网络提供一个既高效又完善的通信系统安全解决方案。

未来的工作将集中在进一步优化安全协议的实现, 通过引入密钥调度和算法加速技术, 减少计算开销和交互时延对系统性能的影响。同时, 还需要进一步完善列车互联网密钥管理机制, 保持其在安全性方面的优势, 并适应列车控制网络中对时效性和安全性的双重要求。

参考文献:

- [1] 王麟书. 中国铁路信息化事业的发展[J]. 铁路计算机应用, 2002, (6):2-5.
WANG L S. Development of the information technology industry in chinese railways [J]. Railway Computer Application, 2002, (6):2-5.
- [2] GB/T 28029.12-2020, 轨道交通电子设备 列车通信网络(TCN) 第 3-4 部分: 以太网编组网(ECN) [S]. 2020.
GB/T 28029.12-2020, Urban rail transit electronic equipment - train communication network (TCN) - Part 3-4: Ethernet Consist Network (ECN) [S]. 2020.
- [3] 王同军. 铁路 5G 关键技术分析和路线[J]. 中国铁路, 2020, (11): 1-9.
WANG T J. Analysis of key 5G technologies for railways and development roadmap [J]. China Railway, 2020, (11):1-9.
- [4] 李平, 邵赛, 薛蕊等. 国外铁路数字化与智能化发展趋势研究[J]. 中国铁路, 2019, (2): 25-31.
LI P, SHAO S, XUE R, et al. Research on the development trend of digitalization and intellectualization of railways abroad[J]. China Railway, 2019, (2):25-31.
- [5] 史天运. 中国高速铁路信息化现状及智能化发展[J]. 科技导报, 2019, 37(6):53-59.
SHI T Y. The current status of information technology and the development of intelligence in China's high-speed railways [J]. Science & Technology Review, 2019, 37(6):53-59.

- [6] 邹智荣, 陈超群, 陈勃等. 列车通信网络安全现状分析及应对方案研究[J]. 机车电传动, 2023, (1): 78-85.
ZOU Z R, CHEN C Q, CHEN B, et al. Analysis of the current status of train communication network security and research on counter-measures[J]. Electric Drive for Locomotives, 2023, (1):78-85.
- [7] 岳川, 王立德, 申萍等. 基于以太网的列车通信网络安全脆弱性定性分析[J]. 机车电传动, 2022,(4):44-54.
YUE C, WANG L D, SHEN P, et al. Qualitative analysis of security vulnerabilities in train communication networks based on ethernet [J]. Electric Drive for Locomotives, 2022, (4):44-54.
- [8] IEC 61375-2-3: 电子铁路设备-列车通信网络(TCN)- 第2-3部分: TCN通信概要[S]. 2015.
IEC 61375-2-3: Electronic railway equipment - train communication network (TCN) - Part 2-3: TCN communication profile[S]. 2015.
- [9] 姚健. 国产商用密码算法研究及性能分析[J]. 计算机应用与软件, 2019, 36(6): 327-333.
YAO J. Research and performance analysis of domestic commercial cryptographic algorithms [J]. Computer Applications and Software, 2019, 36(6): 327-333.
- [10] 吴永强. 国密SSL安全通信协议的研究与实现[D]. 西安: 西安电子科技大学, 2014.
WU Y Q. Research and implementation of the national secret SSL security communication protocol[D]. Xi'an: Xidian University, 2014.
- [11] REYZIN L, REYZIN N. Better than BiBa: short one-time signatures with fast signing and verifying[J]. Algorithm, 2002, 32(1): 1-9.
- [12] 赵华, 周利华. 一种基于DTLS协议的VPN方案设计[J]. 电子科技, 2006, (7): 32-35.
ZHAO H, ZHOU L H. A VPN scheme based on the DTLS protocol design[J]. Electronic Technology, 2006, (7):32-35.

[作者简介]



崔玉龙 (1983-), 男, 山东日照人, 中车青岛四方机车车辆股份有限公司正高级工程师, 主要研究方向为列车网络控制。



吴学超 (1990-), 男, 山东临沂人, 中车青岛四方机车车辆股份有限公司工程师, 主要研究方向为列车网络安全、数据安全。



程宥霖 (1998-), 男, 山西晋中人, 中国科学院大学硕士生, 主要研究方向为网络安全、密码工程。



芦翔 (1982-), 男, 河南许昌人, 中国科学院信息工程研究所副教授, 主要研究方向为计算机与网络安全、信息物理系统安全、密码工程。