

RSSP-II的安全分析及安全增强新方案

冯涛, 铁小平, 吴毅, 石建明
(兰州理工大学计算机与通信学院, 甘肃 兰州 730000)

摘要: 铁路信号安全协议-II (railway signal safety protocol-II, RSSP-II) 是我国列车控制系统 CTCS-3 的核心安全通信协议, 在保障列车通信安全性与可靠性方面发挥着关键作用。然而, 现有研究表明, RSSP-II 的消息鉴定安全层存在密钥恢复与伪造等安全漏洞, 可能危及列车控制系统的稳定运行。针对上述安全问题, 使用着色 Petri 网 (colored Petri nets, CPN) 形式化建模方法对 RSSP-II 进行了分析, 验证了 RSSP-II 中存在安全漏洞, 并提出了一种改进协议 EN-RSSP (enhanced railway signal safety protocol)。该改进协议主要包含 3 个方面的增强措施。首先, 通过可信第三方在安全信道中动态构建通信双方设备的临时密钥对; 其次, 基于椭圆曲线双线性对的离散对数困难特性, 结合哈希函数实现会话密钥协商; 最后, 采用由会话密钥和通信双方设备的预共享密钥构成的双密钥加密体系对消息进行加密传输。此外, 还在信息交互过程中引入了时间戳和 CMAC (cipher-based message authentication code) 消息认证码, 以确保通信双方消息的保密性和完整性。通过 CPN 形式化分析工具对 EN-RSSP (enhance-RSSP) 和 RSSP-II 进行安全评估, 结果表明, 改进后的协议不仅能有效抵御密钥恢复与伪造攻击, 还可防范重放攻击, 显著提升了系统的安全性。

关键词: RSSP-II; 着色 Petri 网; 形式化分析; 安全评估

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025038

Security analysis of the RSSP-II protocol and a novel security enhancement approach

FENG Tao, TIE Xiaoping, WU Yi, SHI Jianming

School of Computer and Communication Lanzhou University of Technology, Lanzhou 730000, China

Abstract: The railway signal safety protocol-II (RSSP-II), as the core security communication protocol of China's train control system (CTCS-3), played a crucial role in ensuring the security and reliability of train communication. However, existing research revealed that RSSP-II's message authentication security layer (MASL) had security vulnerabilities like key recovery and forgery, which might endanger the train control system's stable operation.

收稿日期: 2025-01-15; **修回日期:** 2025-05-26

通信作者: 冯涛, fengt@lut.edu.cn

基金项目: 国家自然科学基金 (61762060); 甘肃省重点研发计划基金 (23YFGA0060); 甘肃省优秀博士生基金 (23JRRA837)

Foundation Items: The National Natural Science Foundation of China (61762060), Key Research and Development Projects of Gansu Province (23YFGA0060), Gansu Province Excellent Doctoral Student Foundation (23JRRA837)

引用格式: 冯涛, 铁小平, 吴毅, 等. RSSP-II 的安全分析及安全增强新方案[J]. 网络与信息安全学报, 2025, 11(3): 45-66.

Citation Format: FENG T, TIE X P, WU Y, et al. Security analysis of the RSSP-II protocol and a novel security enhancement approach[J]. Chinese Journal of Network and Information Security, 2025, 11(3): 45-66.

tion. To address these security issues, the formal modeling method of colored Petri nets (CPN) was employed to analyze RSSP-II, and the existence of security vulnerabilities in it was verified. Consequently, an improved protocol, EN - RSSP (enhanced railway signal safety protocol), was proposed. The improvement primarily comprised three aspects. First, a temporary key pair for the communication devices of both parties was dynamically constructed through a trusted third party in a secure channel. Next, session key negotiation was achieved based on the difficulty of the discrete logarithm problem in elliptic curve bilinear pairing combined with a hash function. Finally, a dual-key encryption system made up of the session key and the pre-shared key of the communication devices of both parties was adopted to encrypt and transmit messages. Moreover, timestamps and CMAC (cipher-based message authentication code) were incorporated into the information exchange process to ensure the confidentiality and integrity of messages between devices. Security assessment of EN-RSSP and RSSP-II was conducted using the CPN formal analysis tool. The results show that the improved protocol could not only effectively resist key recovery and forgery attacks, but also prevent replay attacks, thereby significantly enhancing the system's security.

Keywords: RSSP-II, coloured petri nets, formal analysis, security assessment

0 引言

近年来,随着铁路运输业的迅猛发展及铁路网络的不断拓展,列车控制系统的安全问题日益凸显。作为保障列车安全高效运行的核心系统,列车控制系统的可靠性与安全性直接关系到铁路运输的整体运营安全^[1]。我国参考欧洲列车控制系统(European train control system, ETCS)系列规范,制定了中国列车控制系统(Chinese train control system, CTCS)标准,并通过不断地实践与改进,成功将CTCS-3应用于我国的铁路运营。CTCS-3利用GSM-R(global system for mobile communications-railway)网络实现车地双向信息传输,同时,在传输网络中部署了铁路信号安全协议-II(railway signal safety protocol-II, RSSP-II),以保障列车控制系统通信的安全,防止铁路信号通信设备遭受数据丢失、插入、篡改等各种威胁^[2]。RSSP-II专为列车控制系统间通信而设计,以确保信号安全设备之间关键信息的安全交换^[3]。该协议的制定参照了欧洲保护开放式网络系统标准EN50159-2^[4]与欧洲协议标准Subset-098^[5],并经过多次修订^[6]。RSSP-II在有效保护我国铁路列车控制系统免受潜在攻击和干扰的同时,还提供了安全可靠的通信服务。

虽然RSSP-II在设计之初已经综合考虑多种安全因素,但是现有研究者发现,该协议中的消息鉴定安全层(message authentication safety

layer, MASL)的消息验证码(message authentication code, MAC)存在安全漏洞,攻击者可基于生日攻击原理实施密钥恢复、伪造攻击^[7],这类攻击不仅会威胁列车控制系统的稳定运行,严重时甚至可能导致整个系统瘫痪。针对该协议的安全性问题,国内外学者已开展多项研究。英国学者Tom Chothia针对ER安全层协议中的MAC实施密钥恢复攻击,成功伪造了未授权信息并被列车接收^[4]。该研究仅针对消息验证码的现有漏洞提出了简单的改进措施,在一定程度上提升了协议的安全性,但并未引入新的加密或认证机制,因此无法提供更高级别的安全保障。徐倩等^[8]创新性地采用着色Petri网(coloured Petri nets, CPN)对RSSP-II中的消息认证层进行建模,为协议后续的安全性研究提供了新的思路。然而,该研究未针对密钥恢复、伪造等关键安全问题开展深入的形式化分析与验证。

为解决RSSP-II存在的密钥恢复、伪造攻击等安全问题,本文运用CPN形式化建模方法对RSSP-II的MASL开展安全性评估分析,在此基础上设计出一种EN-RSSP(enhance-railway signal safety protocol)。该协议融合可信第三方、椭圆曲线双线性对和哈希函数等技术。与原协议相比,EN-RSSP的优势在于:借助可信第三方实现系统临时密钥对的动态分配,且能在通信双方建立安全连接时动态生成会话密钥,这一机制提高了协议的安全性。此外,在RSSP-II的基础上,

构建预共享密钥与会话密钥的双重加密体系,对传输消息进行加密保护,进一步强化协议的安全防护能力。

本文的主要贡献如下。

1) 使用 CPN 形式化建模方法对 RSSP-II 进行安全性评估,通过形式化验证明确该协议存在密钥恢复、伪造攻击风险,为后续改进提供理论依据。

2) 针对 RSSP-II 中存在的密钥恢复、伪造攻击问题,提出 EN-RSSP。该协议通过如下机制提升安全性:①引入可信第三方动态生成通信双方设备的临时密钥,并通过安全信道将其发送给双方设备,同时定期更新临时密钥对;②基于椭圆曲线双线性对实现密钥协商,并将协商生成的会话密钥进行哈希处理,从而有效抵御密钥恢复攻击、伪造攻击及重放攻击;③构建双密钥加密体系(预共享密钥与会话密钥),配合时间戳和 CMAC 消息验证码机制,强化数据传输的机密性与完整性。

3) 通过 CPN 形式化安全验证方法对比评估 RSSP-II 与 EN-RSSP,结果表明 EN-RSSP 不仅能抵御密钥恢复、伪造攻击,还具备防御重放攻击能力,安全性能显著优于 RSSP-II。

1 相关工作

随着列车控制系统的快速发展, RSSP-II 作为确保铁路通信安全的重要协议,已成为学术研究的焦点。现有研究主要围绕协议安全性提升展开,学者通过增强加密算法、引入新型安全机制及采用形式化建模等手段进行优化。本节将分别从协议的应用研究、安全性优化及形式化分析 3 个维度梳理相关研究工作。

(1) 协议应用研究

RSSP-II 作为列车控制系统的重要协议,已得到了广泛应用。王海龙^[9]针对无线闭塞中心与计算机联锁接口场景,提出 RSSP-II 的部署规范与使用方法。刘国靖等^[10]对 RSSP-II 的通信过程进行了软件自动测试,为相关领域研究人员提供了可靠的参考。乐超等^[11]基于 RSSP-II 设计了临时限速服务器(temporary speed restriction server, TSRS)与调度集中控制(centralized traffic control, CTC)间的安全通信接口,并成功应用于

CTCS-3 级列车控制系统,实现线上运营的安全通信保障。刘振玉等^[12]提出 RSSP-II 软件自动化测试框架,并成功进行了多轮自动化测试,助力将专项测试工具推广应用于半实物软硬件集成测试。

(2) 协议安全性优化

为了增强协议的安全性,研究人员提出了一系列优化方案。左林等^[13]提出用国家标准 SM4 算法替换 RSSP-II 原有的 3DES (data encryption standard) 算法,通过仿真与实物测试验证了新算法在安全性上的优势。张淼等^[14]设计了 AES (advanced encryption standard) 与 SM4 混合加密方案,通过半物理仿真实验证明该方案具有更高的实时性。郭伟等^[15]对 RSSP-II 中的 MASL-MAC 开展了安全分析,发现由于采用 64 位 DES 分组密码,该协议存在密钥恢复、伪造攻击风险。为此,该团队建议将现有的 64 位分组密码 DES 替换为国际或国内标准化的 128 位分组密码(如 AES 或 SM4),以进一步提高 RSSP-II 的整体安全性。张元玲等^[16]对 RSSP-II 中的消息验证码算法以 AES 作为 MAC 的核心算法,利用密文分组链接方式对报文进行加解密处理,成功解决了原算法存在的弱密钥和半弱密钥等安全隐患问题,显著提高了安全性和实时性。Wu 等^[7]将 MAC 的核心算法替换为 AES-128,采用密文对报文链路的消息进行加解密,并对 RSSP-II 中的安全相关密钥服务过程进行了改进,进一步增强了协议的安全性。Liang 等^[17]提出一种改进的椭圆曲线 Diffie-Hellman (ECDH) 密钥协商算法,旨在解决原先采用的密钥分配方式所存在的安全威胁,以进一步提高协议的安全性^[18]。然而,该方案在身份认证阶段可能面临重放攻击的威胁。张凯等^[5]提出将 AES-128 算法集成到 RSSP-II 的 MAC 生成模块中,并通过 FPGA 硬件加速实现,从而进一步提高 RSSP-II 的安全性。代新月^[6]引入认证加密机制和 Deoxys-II 算法,解决了 RSSP-II 核心消息鉴定算法的安全问题,为未来列车控制通信系统提供了端到端的安全保护机制,但是密钥的分配方式仍存在潜在的安全威胁。

(3) 协议形式化分析

为深入了解 RSSP-II, 学术界已开展一系列形式化分析研究。Xu 等^[19]针对 RSSP-II 中的 SAI 连接管理过程和时间戳初始化过程进行形式化建模和分析, 使用 UPPAAL 工具进行协议仿真, 验证了模型的活性、安全性和可达性, 并证明 RSSP-II 在 MAC 的生成与处理方面的安全性完全符合铁路信号安全相关设备间进行通信的安全性要求。和晟姣^[20]使用模型检测工具 Casper-FDR 对 RSSP-II 中的密钥服务流程和对等实体认证这两个关键点进行建模分析, 以验证其保密性和认证性。徐倩等^[8]基于 CPN 建立了 RSSP-II 中 MASL 的形式化模型。该研究不仅对会话密钥生成、对等实体认证和消息源认证等核心安全流程进行了形式化描述, 还通过计算树逻辑语句验证了协议的保密性和认证性等特定安全属性。这些研究成果为协议工程的后续实现和一致性检验奠定了重要的理论基础。

综上所述, 现有研究主要集中于 RSSP-II 的对称加密算法优化及协议的建模与仿真工作, 这些研究在一定程度上提高了协议的安全性。然而, 目前基于 CPN 对 RSSP-II 进行安全性形式化分析与改进的研究仍显不足, 针对非对称加密机制的改进研究也较匮乏。此外, 尽管已有研究通过增加密钥长度和采用复杂算法设计来强化安全性, 但在已知部分明文-密文对的情况下, 协议仍面临密钥恢复、伪造攻击的风险, 其安全强度有待进一步提高。

为此, 本文在现有研究基础上, 基于 CPN 的形式化建模方法^[21], 对 RSSP-II 的安全性进行评估与验证, 并提出一种增强型铁路信号安全协议 (enhance-railway signal safety protocol, EN-RSSP)。该协议的核心改进包括: ①基于椭圆曲线双线性对和哈希函数的密钥协商机制, 通过可信第三方动态生成通信双方设备的临时密钥, 并定期更新系统临时密钥对, 提升密钥管理的安全性; ②结合原协议的预共享密钥 (KMAC) 和会话密钥对消息进行双重加密。相较于现有研究成果, EN-RSSP 在密钥协商、动态更新及加密强度等方面均有所优化, 能够更有效地抵御密钥恢复、伪造攻击, 从而为铁路信号安全通信提供更高的安全保障。

2 背景知识

2.1 RSSP-II

RSSP-II 中定义的消息结构如图 1 所示, 其安全服务功能主要由 MASL 与安全应用中间子层共同提供。

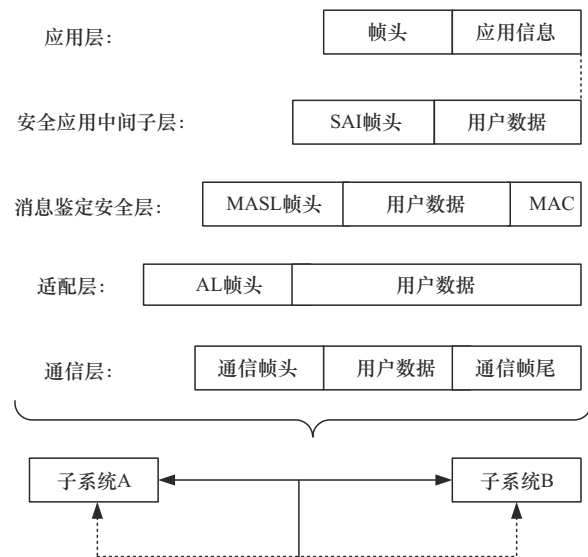


图 1 RSSP-II 中定义的消息结构
Figure 1 Message structure defined in the RSSP-II

本文的研究聚焦于安全功能模块中的 MASL^[3,6]。该层作为协议安全体系的核心组件, 主要实现以下安全功能: ①防御篡改和损坏消息, 确保数据的完整性; ②防止伪装攻击, 提供身份认证机制; ③抵御非法消息插入, 保障通信链路的合法性。MASL 通过上述安全机制, 为铁路信号系统中的安全设备间通信提供了可靠的链路。

MASL 的安全功能依托于 RSSP-II 定义的 3 层对称密钥体系实现。RSSP-II 构建了传输密钥 (TRANS)、认证预共享密钥 (KMAC) 和会话密钥 (KSMAC) 的分级密钥架构, 并将其应用于 3DES 对称加密算法, 形成数据安全交互的基础保障。需特别说明的是, 本文研究范畴限定于安全相关设备在密钥管理域内的密钥传输机制。

RSSP-II 在 MASL 执行对等实体认证过程。对等实体认证通过 3 次握手消息交互 (AU1SaPDU、AU2SaPDU 和 AU3SaPDU) 实现, 其传输的数据单元称为安全协议数据单元 (safety protocol data unit, SaPDU)。协议中通过 “Text” 字段规

范各 SaPDU 的格式, 采用“P”字段将消息长度填充至 64 位整数倍 (该填充数据仅在加密前处理, 不参与实际传输)。

对等实体认证过程如图 2 所示, 其具体实现流程如下。

1) 安全连接初始化: 设备 A 向设备 B 发起安全连接建立请求; 密钥管理中心 (KMC) 已预先为通信双方设备 A 和 B 分配验证密钥 KMAC, 该密钥以安全方式预置并存储在设备的受保护存储区域中。

2) 认证信息交换阶段: ①设备 A 生成符合密码学安全要求的 64 位随机数 R_A (在消息发送前, 设备 A 将 R_A 存入链路专用缓存, 用于后续响应验证), 将 R_A 与设备 ID、时间戳 T_A 封装在首个认证消息 (AU1SaPDU) 中, 将 AU1SaPDU 消息发送给设备 B; ②设备 B 接收到此消息后, 随后生成一个长度为 64 位的随机数 R_B , 接着基于三方参数 (R_A 、 R_B 、KMAC) 通过密钥派生函数

生成会话密钥 K_s , 采用 CBC-MAC 算法对文本字段 Text3、 R_A 、 R_B 、设备 A 的身份 (即 A 的 CTCS ID) 和填充位 P 进行计算, 生成 MAC 值。将上述信息封装在 AU2SaPDU 消息中发送给设备 A; ③设备 A 接收 AU2SaPDU 消息后, 首先根据会话密钥生成方式生成会话密钥 K_s , 然后进行消息源验证 (通过对比接收到的 MAC 值与本地生成的 MAC 值, 验证是否一致), 以检查接收到的 AU2SaPDU 消息的正确性。若 MAC 值验证通过, 则设备 A 采用 CBC-MAC 算法对文本字段 Text5、 R_A 、 R_B 和填充位 P 进行计算, 生成新的 MAC 值, 将上述信息封装在 AU3SaPDU 中并发送给设备 B; ④设备 B 接收 AU3SaPDU 消息后, 使用密钥 K_s 验证 AU3SaPDU 消息的正确性, 完成整个认证流程。

图 2 中 Text1~Text5 的内容分别如下。

1) Text1 = "ETY|MTI|DF|SA|SaF", 其中 SA=主叫列车控制设备号 (CTCS ID)。

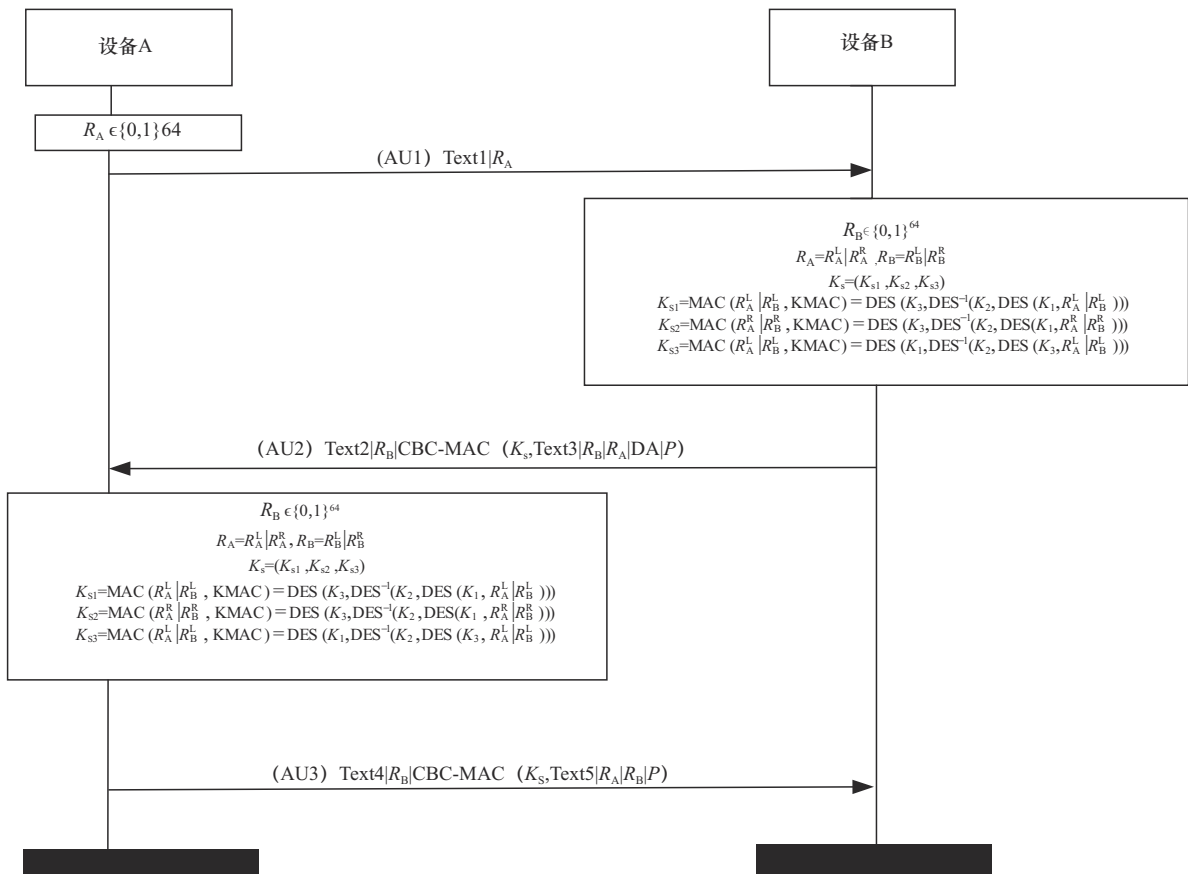


图2 对等实体认证过程

Figure 2 Peer entity authentication process

2) Text2 = "ETY|MTI|DF|SA|SaF", 其中 SA=响应 CTCS ID。

3) Text3 = "l|DA|ETY|MTI|DF|SA|SaF", 其中 DA=主叫 CTCS ID, SA=响应 CTCS ID。

4) Text4 = "'000'|MTI|DF|SA|SaF"。

5) Text5 = "l|DA|'000'|MTI|DF", 其中 DA=响应 CTCS ID。

上述说明表明, 铁路安全相关设备 A 和 B 通过对等实体的认证, 将生成相同的会话密钥 K_s 和认证密钥 KMAC 以完成认证过程。表 1 列出了 RSSP-II 对等实体认证机制涉及的消息流术语及其含义。

表 1 消息流术语及其含义
Table 1 Definitions and meanings of message flow terminology

术语	含义
K_s	会话密钥
AU1	第 1 个认证消息单元
AU2	第 2 个认证消息单元
AU3	第 3 个认证消息单元
SaPDU	安全协议数据单元
ETY	设备类型
MTI	消息类型标志 (AU1、AU2、AU3)
DF	方向标志
SA	源地址
DA	目的地址
'000'	保留
SaF	安全特征: 3DES
l	长度为 2 个字节的字符串
P	填充数据
R_A 、 R_B	随机数, 用于产生会话密钥
A、B	设备发起方、设备接收方

2.2 CPN 建模工具

CPN 是一种基于 Petri 网的建模方法, 它通过引入有色令牌扩展了传统 Petri 网的能力, 使其能够更有效地描述并发系统、分布式系统、通信协议, 以及其他交互和并行系统的行为^[22]。

与传统 Petri 网^[23]相比, CPN 不仅保留了 Petri 网形式化、可视化的优点, 还通过令牌着色机制增强了模型的表达能力。CPN 在安全协议分析领域具有显著优势。

1) 灵活建模: 通过形式化的语义和语法对协议进行精确描述, 并逐步观察协议消息流的执行过程。

2) 自动化检测和识别漏洞: 利用 CPN 工具提供的状态空间分析和 SML (Standard ML) 编程功能, 对协议交互过程进行自动化检测, 识别协议中可能存在的安全漏洞^[24]。

近年来, 形式化安全协议验证领域涌现了多种先进工具, 如 ProVerif、Scyther、BAN 逻辑和 Tamarin Prover 等^[25]。ProVerif 采用基于逻辑编程的方法, 虽然能够自动验证协议的安全性, 但其攻击路径受限, 通常仅适用于小规模协议验证, 在协议处理能力上远不及 CPN 工具^[26]。Scyther 基于模型检测和符号执行技术, 提供了常见的攻击模型, 但其攻击方式较为单一, 难以模拟特定场景下的定制化攻击手段^[27]。BAN 逻辑侧重于定理证明的形式化验证, 虽然逻辑严谨, 但缺乏直观的可视化分析能力, 且无法对协议的形式语义进行动态分析, 与 CPN 工具相比适用性较差。Tamarin Prover 支持状态空间的穷尽搜索, 具备较强的自动化验证能力, 但与 Scyther 类似, 其攻击模式相对固定, 难以灵活引入特定攻击方法^[28]。相比之下, CPN 工具凭借其强大的协议建模能力、灵活的攻击场景定制和丰富的状态空间分析功能, 能够有效弥补上述工具的不足。

3 RSSP-II 的 CPN 建模

3.1 RSSP-II 的颜色集定义

在建模时对设备 A 与设备 B 交互的 3 条信息进行颜色集的建立。交互信息由 AU1、AU2、AU3 这 3 个消息构成。Text1、Text2、Text3、Text4、Text5 表示设备信息, RA、RB 表示随机数, KS 表示会话密钥。AU1 表示设备 A 给设备 B 发送安全协议单元信息。AU2 表示设备 B 给设备 A 发送身份验证信息。AU3 表示设备 A 将身份验证结果发送给设备 B 来进行对等实体认证。RSSP-II 的颜色集定义见表 2。

表2 RSSP-II的颜色集定义

Table 2 Definition of color sets for the RSSP-II

关键元素	颜色集定义
Text1	Colset Text1=string;
Text2	Colset Text2=string;
Text3	Colset Text3=string;
Text4	Colset Text4=string;
Text5	Colset Text5=string;
RA	Colset RA=string;
RB	Colset RB=string;
KS	Colset KS=product RA*RB*KMAC;
AU1	Colset AU1=product Text1*KMAC;
AU2	Colset AU2=product Text2*RB*MACB;
AU3	Colset AU2=product Text4*MACA;

3.2 RSSP-II的安全性形式化分析

RSSP-II的安全性形式化分析基于CPN工具,采用自顶向下的建模方法,依次构建协议的顶层模型和内部模型。

图3所示的顶层CPN模型清晰地绘制了设备A与设备B之间的完整认证会话流程。顶层模型由3个替代变迁和6个库构成。其中椭圆形表示消息库所,用于存储通信过程中的消息;矩形表示变迁;双线矩形表示替代变迁,包含协议更详细的子模型;箭头标识通信双方之间的消息传输。

替代变迁NET的内部CPN模型如图4所示。变迁Trans_AU1表示设备A给设备B发送AU1消息。变迁Trans_AU2表示设备B给设备A发送身份认证请求信息。变迁Trans_AU3表示设备A给设备B发送认证结果信息。

替代变迁EntityA的内部CPN模型如图5所示。库所RA与变迁random_number交互获取随机数,将其存入库所getRA。变迁AU1基于库所Text1和库所getRA的信息生成AU1SaPDU,将其存储在库所AU1SaPDU中,通过变迁S_AU1将消息发送到库所Send_AU1SaPDU。接着库所Rec_AU2SaPDU将接收到的数据通过变迁T2提取信息rB与macb后,分别存储在库所RB和库

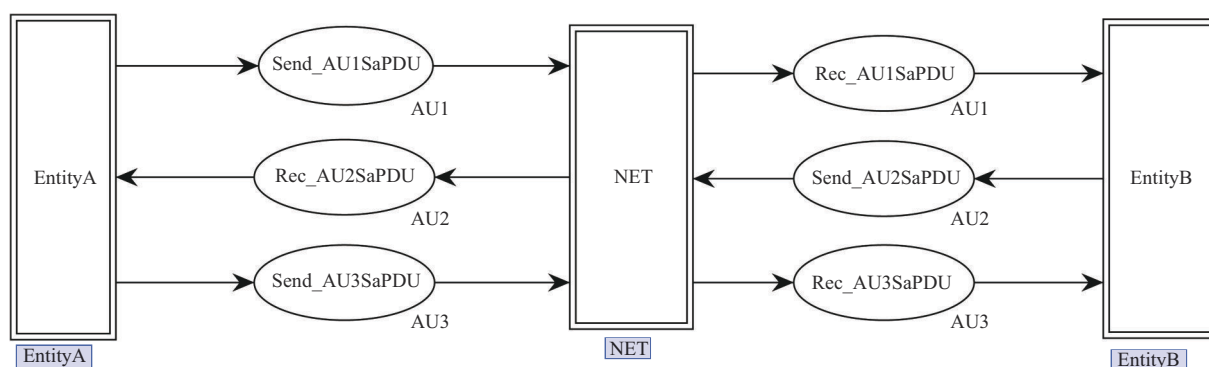


图3 RSSP-II的顶层CPN模型

Figure 3 Top-level CPN model of the RSSP-II

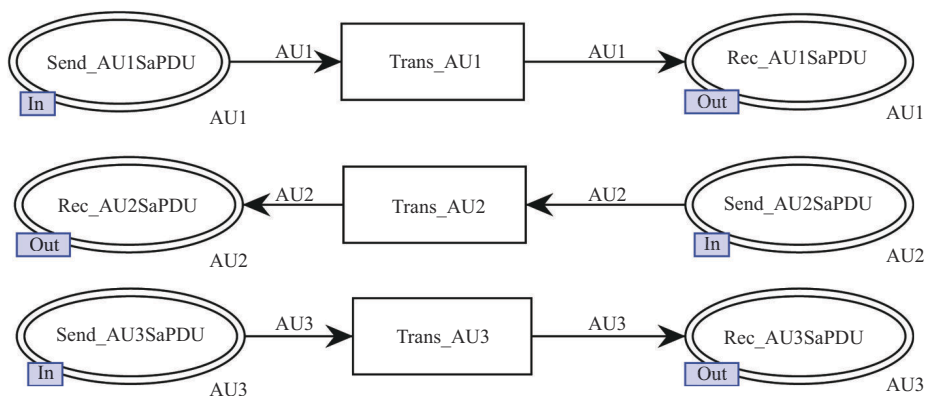


图4 替代变迁NET的内部CPN模型

Figure 4 Internal CPN model of the substitution transition NET

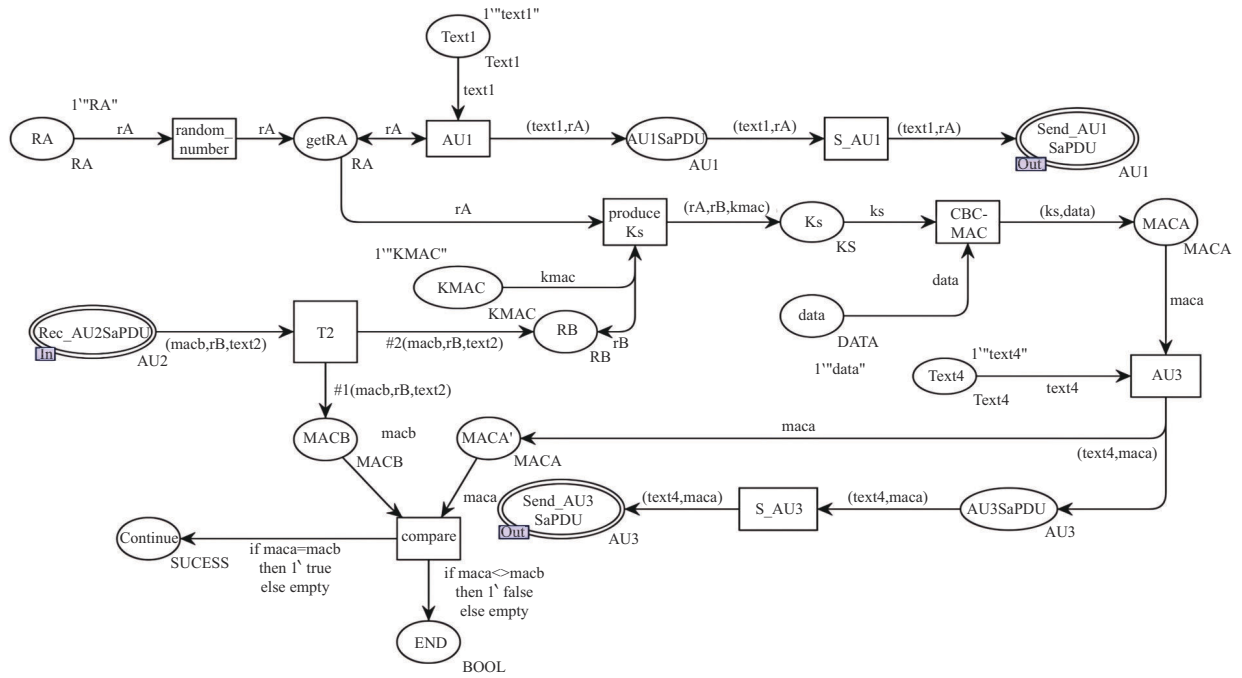


图5 替代变迁EntityA的内部CPN模型

Figure 5 Internal CPN model of the substitution transition EntityA

所MACB中。变迁compare对接收到的消息认证码macb和变迁AU3产生的消息认证码maca进行验证,若验证失败则通过库所END进行重置,若验证成功则到达库所Continue中。接着,变迁produce_Ks基于rA、rB和kmac生成会话密钥KS,将其存储到库所Ks中,再通过变迁CBC_MAC对数据data和ks进行加密生成maca,变迁AU3基于库所MACA和库所Text4的信

息生成AU3SaPDU消息,将其存储到库所AU3SaPDU中,再通过变迁S_AU3将信息发送给库所Send_AU3SaPDU。

替代变迁EntityB的内部CPN模型如图6所示。变迁take out RA从库所Rec_AU1SaPDU接收到的消息AU1中提取出信息rA,并将其存储到库所RA中。与此过程同时进行的是,用与rA相同的方式获取随机数rB,将其存储在库所

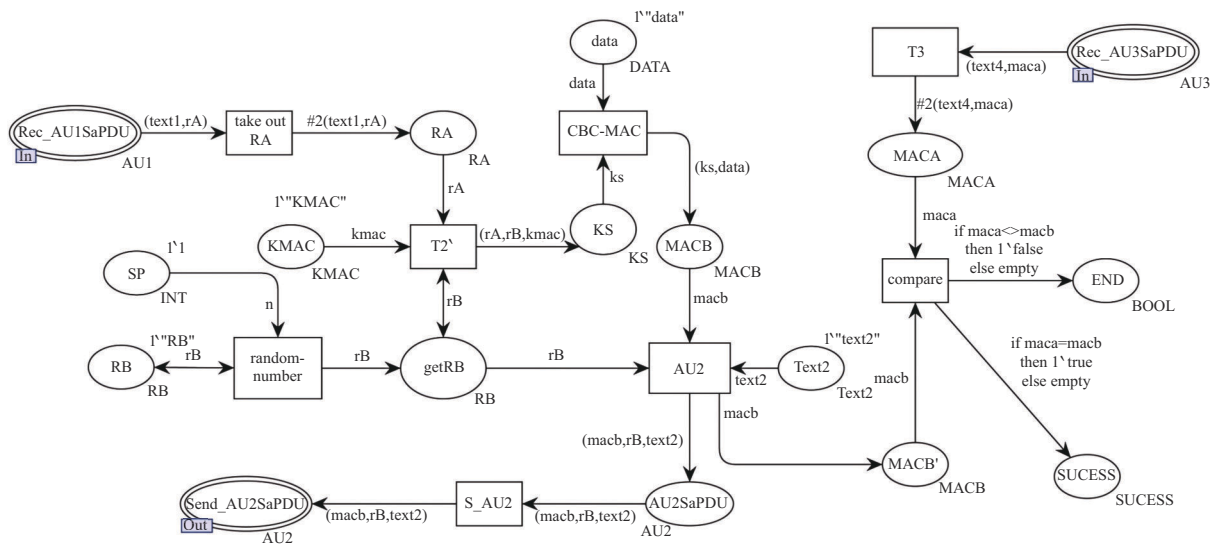


图6 替代变迁EntityB的内部CPN模型

Figure 6 Internal CPN model of the substitution transition EntityB

getRB 中。变迁 T2' 基于 rA、rB 和 kmac 生成会话密钥 KS, 并将其存储在库所 KS 中。通过变迁 CBC-MAC 加密数据信息得到消息认证码 macb, 将其存储在库所 MACB 中。变迁 AU2 将库所 MACB、库所 Text2 和库所 getRB 中的消息结合起来发送给库所 AU2SaPDU, 再将其通过变迁 S_AU2 发送给库所 send_AU2SaPDU。库所 Rec_AU3SaPDU 收到消息之后, 通过变迁 T3 提取消息 maca 并将其存储到库所 MACA。变迁 compare 通过对比收到的 maca 与本地生成的 macb 进行验证。若验证成功, 则设备之间对等实体认证成功, 若验证失败, 则通过库所 END 终止该操作。

3.3 RSSP-II 的一致性分析

RSSP-II 的 CPN 模型的状态空间分析报告汇总在表 3 中。

表 3 RSSP-II 的 CPN 模型的状态空间分析报告
Table 3 State space analysis report of the CPN model of RSSP-II

状态空间信息	数量
状态空间节点/个	30
状态空间有向弧/条	38
强连通节点/个	30
强连通弧/条	38
死节点/个	1
死变迁/个	0

从表 3 可以看出, 该协议的状态空间节点与强连通节点的数量相等, 状态空间有向弧与强连通弧的数量也相等^[29]。这表明 RSSP-II 的 CPN 模型中的所有状态节点都是可达的。在构建的 CPN 模型中, 只存在一个死节点, 其对应的终止标记同样位于第 30 个节点。因此, RSSP-II 的 CPN 模型能够正常终止, 不存在任何意外中断和死锁情况。在无攻击的情况下, 模型将按照协议流程执行交互, 且所有的交互均不会触发模型中建立的两个重置库所。此外, 死变迁数量为 0, 说明不存在无法触发的变迁, 这与预期结果一致。

3.4 基于 Dolev-Yao 攻击者模型的 RSSP-II 的安全性评估

在密码学安全协议的形式化分析中, Dolev-Yao 攻击者模型发挥着重要作用。该模型假设攻

击者具备强大能力, 能够模拟合法通信方和完全控制通信信道(可拦截、篡改、删除或重放任意传输中的消息), 甚至解密截获的密文^[30]。基于 Dolev-Yao 模型, 攻击者可构造复杂的主动攻击, 对安全协议的正确性和保密性构成严峻挑战。为更精确地刻画现有网络环境下的实际威胁, 本文提出具有网络传输层密钥恢复攻击和伪造攻击特征的 RSSP-II 模型。RSSP-II 攻击者模型如图 7 所示。

攻击者可以根据 MAC 碰撞恢复出会话密钥, 可以对设备间的第二次传输信息进行 MAC 伪造。其中, 红色标注的表达式和变迁库所模拟的是伪造攻击, 包括传输过程中的变迁 Trans_AU1、Trans_AU2 和 Trans_AU3, 并且攻击者 mattack 通过变迁 ATTACK 发起攻击; 蓝色标注的库所和变迁模拟了密钥恢复攻击的过程。攻击者通过变迁 t0' 截获 RSSP-II 在第一轮传输的消息后, 将这些消息分解并存储到库所 distri'、p1、p2、p3、p11 和 p22 中。变迁 TA 和 TC' 负责分解攻击者截获的信息, 库所 p111、p222、p333、p22 和 p6 则用于存储分解后的原子信息。接下来, 攻击者通过变迁 t11 发起攻击, 利用过渡规则将无法解密的消息保存到库所 atom1 和 atom2 中。攻击者随后将原子信息重新组合, 并通过变迁 TD' 利用合成规则存储到库所 p4 中。这一过程受限于并发控制库所 sp, 初始状态允许合成操作, 而合成操作在有新的分解消息后被重新触发。变迁 TE 表示攻击者已成功恢复出会话密钥。库所 p5、p7 和 p8 用于存储合成和待合成的消息。变迁 TG、TH 和 TF 表示将分解后的消息重新组合。最后, 通过变迁 ATTACK 将攻击者的合成信息发送到被攻击的信道库所中。

3.5 RSSP-II 的安全属性验证分析

RSSP-II 攻击者模型的状态空间分析报告汇总在表 4 中, 从表中数据来看, 状态空间节点和强连通节点的数量相等、状态空间有向弧和强连通弧的数量也是相等的。这表明在 RSSP-II 攻击者模型中, 所有状态节点均可达, 且未出现状态空间过大或爆炸问题。这不仅确保了攻击模型的可信度, 还在保证攻击者能力的前提下验证了引入攻击者模型的有效性。

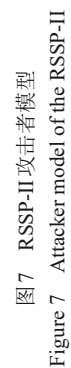


图7 RSSP-II攻击者模型

Figure 7 Attacker model of the RSSP-II

表4 RSSP-II攻击者模型的状态空间分析报告
Table 4 Analysis report on the state space of the
RSSP-II attack model

状态空间信息	密钥恢复攻击	伪造攻击
状态空间节点/个	1 802	484
状态空间有向弧/条	6 087	1 055
强连通节点/个	1 802	484
强连通弧/条	6 087	1 055
死节点/个	8	12
死变迁/个	0	0

攻击者对 RSSP-II 的传输层 AU2 成功实施了密钥恢复攻击, 恢复了会话密钥。利用该会话密钥, 攻击者能够伪造 MAC, 从而介入后续的通信过程。RSSP-II 采用 CBC-MAC 算法, 发送端和接收端分别使用各自的随机数及共享密钥来计算 MAC 值。若计算出的 MAC 值与本地生成的 MAC 值不一致, 则接收操作失败。通过查询语句比较接收端和发送端的库所信息, 发现攻击者在恢复密钥后伪造了另一条消息, 而接收端正常执行 MAC 认证, 具体情况如图 8 所示。通过对变迁和库所响应状态的进一步分析, 发现死节点数由原来的 1 个变成了 20 个。其中 8 个死节点是因为引入密钥恢复攻击后, 攻击者利用 MAC 碰撞恢复出会话密钥, 缺乏向后保密性。其余的 12 个死节点是因为引入了伪造攻击, 攻击者对 MAC 值进行伪造 (通过查询语句得知攻击者将消息中的 RA 篡改为 rA), 便可冒充设备合法身份进行对等实体认证, 具体情况如图 8 所示。

```
val it =
  [
    (["RA","RB","KMAC"],"Text3[R8|RA|DA|P"]),(["RA","RB","KMAC"],"TEXT,RA,RB"),
    (["RA","RB","KMAC"],"Text3[R8|RA|DA|P"])] : MACB ms
```

UpperMulbSet(Mark.EntityA'MACB 1)

```
val it = (((("RA","RB","KMAC"),'Text3|RB|RA|DA|P')) : MACB ms
```

UpperMultiSet(Mark.EntityB'MACB' 1)

```
val it = [("RA","RB","KMAC")]: KS ms
```

UpperMultiSet(Mark.EntityB'KS 1)

```
val it = [("text1","RA")] : AU1 ms
```

UpperMultiSet(Mark.EntityA'Send_AU1SaPDU 1)

```
val it = [("text1","RA"),("text1","rA"),("text1","RA")] : AU1 ms
```

UpperMultiSet(Mark.EntityB'Rec_AU1SaPDU 1)

图8 基于攻击者的RSSP-II查询结果

Figure 8 Based on the attacker's RSSP-II query results

综上所述, 基于 SML 的形式化分析与状态空间验证, 发现 RSSP-II 无法抵御密钥恢复、伪装攻击。攻击者在获取会话密钥后, 可以伪造设备的合法身份和伪造通信过程使用的 MAC, 成功通过对等实体认证。

4 本文方案

针对 RSSP-II 存在的密钥恢复、伪造攻击问题, 本文提出了 EN-RSSP。该协议首先通过可信第三方在安全信道中动态构建设备的临时密钥对; 然后, 通信双方设备基于椭圆曲线双线性对的离散对数困难特性, 结合哈希函数进行会话密钥的协商; 最后, 通过会话密钥和通信双方设备的预共享密钥构建的双密钥加密体系, 对消息进行加密传输。

EN-RSSP涉及的符号及其定义见表5。

表5 EN-RSSP 涉及的符号及其定义
Table 5 Symbols involved in EN-RSSP and their definitions

符号	含义	符号	含义
TA	可信第三方	$\parallel, $	连接符
U_A, U_B	设备A、B的公钥	K_s	会话密钥
r_A, r_B, s	随机数	$k_{A \rightarrow B}$	设备A生成的密钥
$H(\cdot)$	哈希函数	$T(\cdot)$	时间戳
y_A, y_B	系统临时私钥	$\text{Enc}(\cdot)$	加密
P_{pub}	系统临时公钥	$k_{B \rightarrow A}$	设备B生成的密钥

EN-RSSP 的通信过程包括系统初始化^[31]、设备注册^[32]、认证密钥协商^[33]和数据传输共 4 个阶段。其中, 系统初始化和设备注册是基于安全信道的, 认证密钥协商和数据传输是基于公开信道的。下面对这 4 个阶段展开详细描述。

4.1 系统初始化阶段

假设 q 是一个大素数, q 阶加法循环群 G_1 的生成元为点 P , G_2 是同阶的乘法循环群。

步骤 1 选取哈希函数 $H_1: \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow G_1$, $H_2: \{0,1\}^* \times G_2 \rightarrow G_2$ 。其中 $e: G_1 \times G_2 \rightarrow G_2$ 是一双线性映射关系。在设备系统内部发布参数 $\text{params} = \{q, G_1, G_2, P_{\text{pub}}, H_1, H_2, e\}$ 。

步骤 2 由可信第三方生成随机数 $s \in Z_q^*$, 计算系统临时公钥 $P_{\text{pub}} = sP \in Z_q^*$, 并通过安全信道发送给通信双方设备 (设备 A 和设备 B)。同时, 定期更新临时系统密钥对。

4.2 设备注册阶段

步骤 1 通信双方设备 (设备 A 和设备 B) 分别根据各自的身份信息, 生成设备公钥 $U_A = H_1(\text{ETY}|\text{MTI}|\text{DF}|\text{SA}|\text{SaF})$ 和 $U_B = H_1(\text{ETY}|\text{MTI}|\text{DF}|\text{DA}|\text{SaF})$, U_A 和 U_B 均为 G_1 中的元素。接着, 通信双方设备将 U_A 和 U_B 通过安全信道发送给可信第三方 TA。

步骤 2 可信第三方计算设备 A 和设备 B 对应的临时私钥 $y_A = sU_A$ 和 $y_B = sU_B$, 并通过安全信道发送给通信双方设备。之后, 通信双方设备将会对临时公私钥对进行自动销毁。

4.3 认证密钥协商阶段

步骤 1 设备 A 生成随机数 $r_A \in Z_q^*$ 和秘密值 RND, 并计算 $R_A = r_A P$ 。然后, 将消息 $\{U_A, R_A, \text{RND}\}$ 发送给设备 B。

步骤 2 设备 B 收到来自设备 A 的消息后, 设备 B 生成随机数 $r_B \in Z_q^*$, 分别计算 $R_B = r_B P$, $M_2 = \text{RND} \oplus r_B U_A$, $k_{B \rightarrow A} = e(r_B U_A, P_{\text{pub}}) e(y_B, R_A)$, $M_1 = H_2(\text{RND}, k_{B \rightarrow A})$ 的值。接着, 将消息 $\{U_B, R_B, M_1, M_2\}$ 发送给设备 A。

步骤 3 设备 A 在本地分别计算出 $k_{A \rightarrow B} = e(r_A U_B, P_{\text{pub}}) e(y_A, R_B)$, $r_B U_A \oplus M_2 = \text{RND}$, $M'_1 = H_2(\text{RND}, k_{A \rightarrow B})$ 的值。接着, 判断 $M_1 = M'_1$ 等式是否成立。若成立, 则认证成功。接着, 计算 $K_s = H_2(\text{RND}, k_{A \rightarrow B})$ 作为会话密钥。

步骤 4 设备 A 计算 $M_3 = H_2(\text{RND})$ 并将消息 $\{M_3\}$ 发送给设备 B。

步骤 5 设备 B 计算 $M'_3 = H_2(\text{RND})$ 。如果 $M_3 = M'_3$, 那么设备双方认证成功。接着计算 $K_s = H_2(\text{RND}, k_{B \rightarrow A})$ 作为会话密钥。最后, 由设备 A 生成的秘密值 RND 在原来的基础上进行加一操作, 这在一定程度上保证了会话密钥的前后向安全性。

表 6 展示了认证密钥协商阶段的流程。

表 6 认证密钥协商阶段流程

Table 6 Authentication key agreement phase process

设备 A	设备 B
生成随机数 $r_A \in Z_q^*$	
产生秘密值 RND	
计算 $R_A = r_A P$	
$\{U_A, R_A, \text{RND}\}$	
	生成随机数 $r_B \in Z_q^*$
	计算 $R_B = r_B P$
	$M_2 = \text{RND} \oplus r_B U_A$
$k_{B \rightarrow A} = e(r_B U_A, P_{\text{pub}}) e(y_B, R_A)$	
$M_1 = H_2(\text{RND}, k_{B \rightarrow A})$	
$\{U_B, R_B, M_1, M_2\}$	
验证 $r_B U_A \oplus M_2 = \text{RND}$	
计算 $M_3 = H_2(\text{RND})$	
$k_{A \rightarrow B} = e(r_A U_B, P_{\text{pub}}) e(y_A, R_B)$	
$M'_1 = H_2(\text{RND}, k_{A \rightarrow B})$	
$K_s = H_2(\text{RND}, k_{A \rightarrow B})$	
$\{M_3\}$	
	验证 $M'_3 = H_2(\text{RND})$
	$K_s = H_2(\text{RND}, k_{B \rightarrow A})$

4.4 数据传输阶段

步骤 1 设备 B 生成时间戳 T_1 , 通过预共享密钥 KMAC 加密 Text3、 R_A 、 R_B 、DA、 P 的消息, 并使用 CMAC 算法进行消息的验证, 计算 $\text{CMAC} = (\text{KMAC}, \text{Text3} | R_B | R_A | \text{DA} | P)$ 。其中 P 是填充位, 不参与消息的传输。接着利用协商后的会话密钥 K_s 加密整个 AU2 消息。

步骤 2 设备 A 收到消息后, 检查时间戳 T_1 , 生成时间戳 T_2 , 通过协商后的密钥来解密此消息, 并计算 $\text{CMAC}' = (\text{KMAC}, \text{Text3} | R_B | R_A | \text{DA} | P)$, 若 $\text{CMAC} = \text{CMAC}'$, 则确认数据完整, 即验证成功。

步骤 3 设备 A 验证成功, 通过预共享密钥 KMAC 加密 Text5、 R_A 、 R_B 、 P 的消息, 并使用 CMAC 算法进行消息的验证, 计算 $\text{CMAC} = (\text{KMAC}, \text{Text5} | R_B | R_A | P)$ 。其中 P 是填充位, 不参与消息的传输。接着利用协商后的会话密钥 K_s 加

密整个 AU3 消息。

步骤4 设备B收到消息后, 检查时间戳 T_2 , 解密此消息, 并计算 $CMAC'_1 = (KMAC, \text{Text5} | R_A | R_B | P)$, 若 $CMAC_1 = CMAC'_1$, 则确认数据完整, 即验证成功。至此, EN-RSSP 的消息流结束。

表7展示了数据传输阶段的流程。

表7 数据传输阶段流程

Table 7 Data transmission phase process

设备A	设备B
	生成时间戳 T_1
计算 $CMAC = (KMAC, \text{Text3} R_B R_A DA P)$	
$E_n \{ K_s, \text{Text2} R_B CMAC(KMAC, \text{Text3} R_B R_A DA P) T_1 \}$	
检查时间戳 T_1	
生成时间戳 T_2	
验证 $CMAC' = (KMAC, \text{Text3} R_B R_A DA P)$	
计算 $CMAC = (KMAC, \text{Text5} R_B R_A P)$	
$E_n \{ K_s, \text{Text4} CMAC(KMAC, \text{Text5} R_B R_A DA P) T_2 \}$	
检查时间戳 T_2	
验证 $CMAC'_1 = (KMAC, \text{Text5} R_A R_B P)$	

5 EN-RSSP 的安全性形式化分析

5.1 EN-RSSP 的 CPN 模型

采用 CPN 工具对 EN-RSSP 进行安全性形式化分析。EN-RSSP 顶层模型由 14 个库所和 4 个替代变迁组成, 其架构和会话流程如图9所示。其

中, 椭圆形表示消息库所, 用于存储通信流程中的消息; 双层矩形表示替代变迁, 模型中包含通信设备 (A 与 B)、通信网络 (NET) 和可信第三方 (TA) 4 个替代变迁。箭头表示消息流向, 用于模拟通信双方之间的消息传输。

设备A内部CPN模型如图10所示, 其主要包括以下3个环节。

1) 设备A和TA进行动态交互, 生成临时公私钥对。设备信息分别存储在 ETY、MTI、DF、SA、SaF 这5个库所中, 通过变迁 combineA 进行哈希处理, 生成设备A的公钥并将其存储在库所 UA 中, 并通过变迁 send_to_TA 发送给库所 send UA。可信第三方将计算出的临时私钥 yA 发送给库所 Receive yA, Receive yA 通过变迁 receiveya 将收到的临时私钥 yA 发送给库所 yA。

2) 设备A与设备B进行会话密钥协商。库所 UA 和库所 RA 通过变迁 MUL 将信息发送给库所 S1。库所 S2 收到信息之后将信息传输给变迁 REC-Div, REC-Div 将信息拆分后分别存储在 RB、M1、UB 这3个库所中。通过变迁 MUL1 生成 RA, 并存储在库所 RA 中。设备A将计算的密钥过程值存储在库所 e1 和 e2 中, 通过变迁 MULK 生成密钥 Kab, 将其存储在库所 Kab 中。变迁 COMM1' 通过库所 Kab、RANDOM、HASH 进行哈希处理后生成信息 M1', 并将 M1' 信息存储在库所 M1' 中。变迁 compare 对库所 M1、M1' 中的信息进行比较。两者若相同, 则认证成功, 接着进行下一步的密钥协商; 反之, 认证失败。

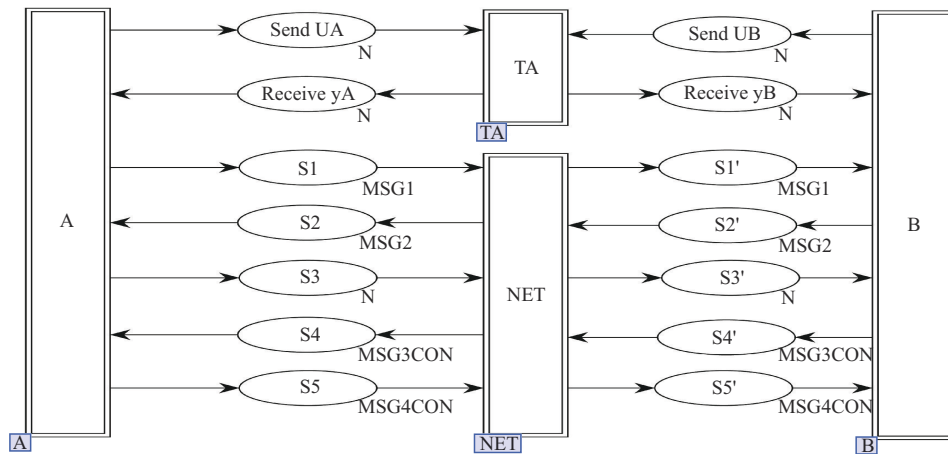


图9 EN-RSSP 顶层模型

Figure 9 Top-level model of the EN-RSSP

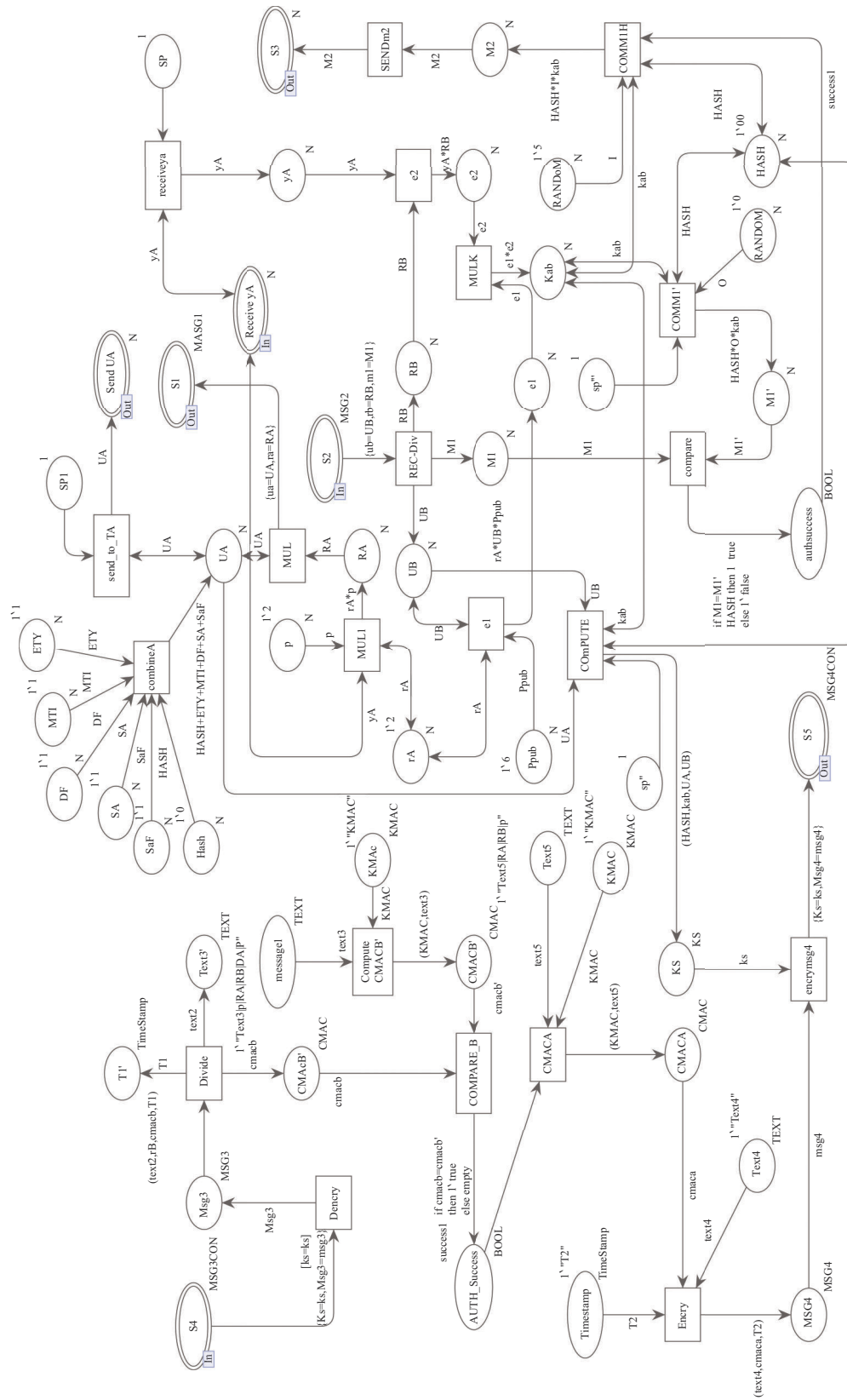


图 10 设备 A 内部 CPN 模型

Figure 10 Internal CPN model of device A

库所UA、UB、Kab、HASH通过变迁COMPUTE协商出会话密钥KS将其存储在库所KS中。

3) 设备A通过会话密钥和预共享密钥KMAC对信息进行双重加密后传输设备B。库所S4接收设备B传输过来的信息,将其解密后存储在库所Msg3中。通过变迁Divide将消息分解并分别存在T1'、Text3'、CMACB'这3个库所中。变迁COMPARE_B将信息cmacb与cmacb'进行比较。两者若相同,则认证成功,保证了消息的完整性;反之,则中断数据传输过程。变迁ComputeCMACB'使用密钥KMAC对所传输的消息进行加密后,将其存储在库所CMACB'中。最后变迁encrymsg4利用协商好的会话密钥对AU2信息进行整体加密,这样就形成双重加密体系,之后将加密后的信息传输给库所S5。

替代变迁NET的内部CPN模型如图11所示。变迁Trans1模拟A向B发送公钥,变迁Trans2模拟B向A发送公钥以及身份认证请求,变迁

Trans3模拟A向B发送身份认证请求。变迁Trans4和变迁Trans5模拟设备A、B使用协商的会话密钥进行数据的传输。

替代变迁TA的内部CPN模型如图12所示。变迁multiple利用库所S和库所Send UA中的信息计算出设备A的临时私钥,将该私钥存储在库所yA中,并将设备A的临时私钥信息通过变迁send to ya发送给库所Receive yA。与此同时,库所Send UB接收到设备B发来的消息后,变迁Multiple利用库所S和库所Send UB中的信息计算出设备B的临时私钥,将该私钥存储在库所yB中,并将设备B的临时私钥信息通过变迁send to yb发送到库所Receive yB中。同时可信第三方将自己计算好的临时公钥发送给设备双方,并定期更新临时密钥对。

设备B内部CPN模型如图13所示。此替代变迁主要包含以下3个环节。

1) 设备B和可信第三方TA进行交互,生成

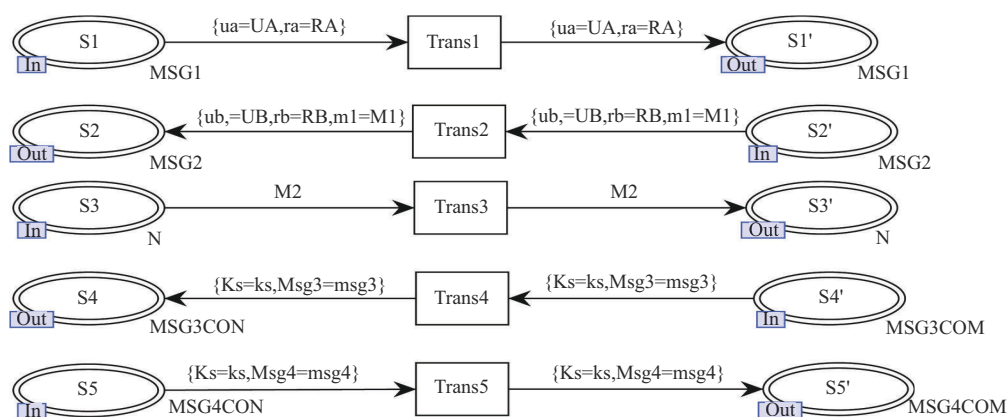


图11 替代变迁NET的内部CPN模型

Figure 11 Internal CPN model of substitution transition NET

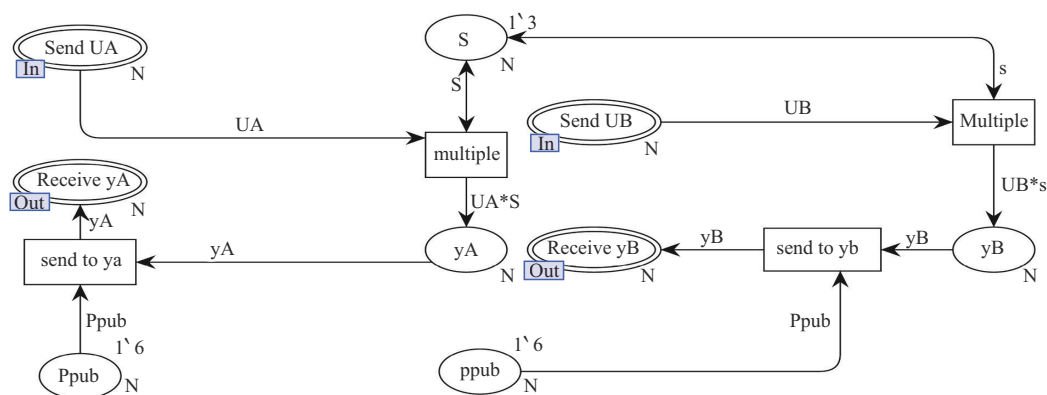
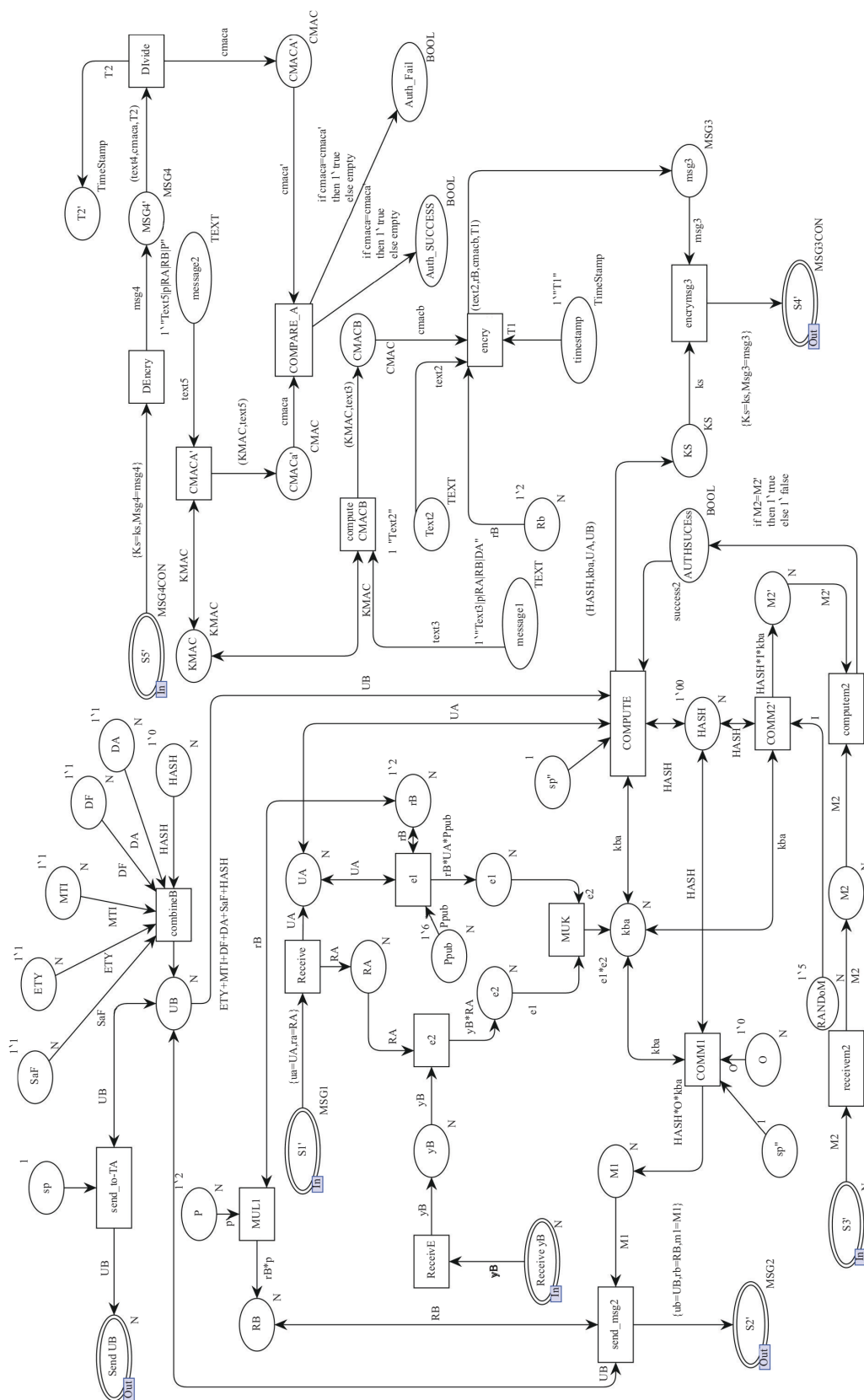


图12 替代变迁TA的内部CPN模型

Figure 12 Internal CPN model of substitution transition TA



临时公私钥对。设备信息分别存储在 ETY、MTI、DF、DA、SaF 这 5 个库所中, 通过变迁 combineB 进行哈希处理, 生成设备 B 的公钥, 将其存储在库所 UB 中, 并通过变迁 send_to_TA 发送给库所 send UB 中。可信第三方计算出私钥 yB 并将其发送给库所 Receive yB, Receive yB 收到私钥 yB 后通过变迁 ReceivE 发送给库所 yB。

2) 设备 B 与设备 A 进行会话密钥的协商。库所 S1' 收到信息之后通过变迁 Receive 将信息分解后分别存储在库所 RA 和 UA 中。通过变迁 MUL1 生成设备 B 的公钥并将其存储在库所 RB 中。设备 B 将计算出的密钥过程值存储在库所 e1 和 e2 中, 通过变迁 MUK 生成密钥 kba, 将密钥 kba 存储在库所 kba 中。变迁 COMM2' 通过库所 Kab、RANDoM、HASH 哈希化生成信息 M2', 将其信息存储在库所 M2' 中。库所 S3' 将接收到的信息 M2 通过变迁 receivem2 存储到库所 M2 中。变迁 computem2 将库所 M2、M2' 中的信息进行比较。两者若相同, 则认证成功, 接着进行下一步的密钥协商; 反之, 则认证失败。变迁 send_msg2 将库所 UB、RB、M1 中存储的信息发送给库所 S2'。库所 UA、UB、kba、HASH 通过变迁 COMPUTE 协商出会话密钥 KS, 将其存储在库所 KS 中。

3) 设备 B 使用会话密钥和预共享密钥 KMAC 对信息进行双重加密后传输给设备 A。库所 S5' 接收设备 A 传输过来的信息, 将其解密后存储在库所 MSG4' 中。通过变迁 DIvide 将消息分解并分别存储在 T2'、CMACA' 这 2 个库所中。变迁 COMPARE_A 将信息 cmaca 与 cmaca' 进行比较。两者若相同, 则认证成功, 保证了消息的完整性; 反之, 则中断数据传输过程。通过变迁 computeCMACB 把所要传输的消息用预共享密钥加密后存储在库所 CMACB 中。最后变迁 encrymsg3 通过协商好的会话密钥对 AU3 消息进行双重加密, 将加密后的信息传输给库所 S4'。至此消息流结束。

5.2 EN-RSSP 的一致性分析

表 8 汇总了 EN-RSSP 的状态空间分析报告, 其中死变迁和死节点的数量分别为 0 和 1, 表明

EN-RSSP 的 CPN 模型中所有变迁均已成功执行, 并按照协议流程进行交互, 最终正常结束。

表 8 EN-RSSP 的状态空间分析报告
Table 8 EN-RSSP state space analysis report

状态空间信息	数量
状态空间节点/个	3 269
状态空间有向弧/条	13 301
强连通节点/个	3 269
强连通弧/条	13 301
死节点/个	1
死变迁/个	0

通过引入 ASK-CTL 分支时间逻辑公式来进一步验证 CPN 模型的准确性^[23]。本文定义了一个 ASK-CTL 状态公式 myASKCTLformula, 用于验证 B 页面中库所 Auth_SUCCESS 是否为正常终止状态 (即判断该状态节点是死标识节点还是正常终止节点)。验证结果如图 14 所示, 从中可知结果返回为 true, 表明验证结果与预期一致, 模型是正确的。

```
val ExpectedMarking = fn : Node -> bool
val myASKCTLformula = FORALL_UNTIL (TT,NF ("Run complete",fn)) : A
val it = true : bool
```

```
use(ogpath^"/ASKCTL/ASKCTLloader.sml")
```

```
fun ExpectedMarking n=(Mark.B'Auth_SUCCESS 1 n=[]);
val myASKCTLformula = EV(NF("Run complete",ExpectedMarking));
eval_node myASKCTLformula InitNode;
```

图 14 ASK-CTL 公式及其验证结果

Figure 14 ASK-CTL formula and its verification results

5.3 基于 Dolev-Yao 攻击者模型 EN-RSSP 的安全评估及分析

在 EN-RSSP 的网络传输层中, 引入密钥恢复攻击、伪造攻击。EN-RSSP 攻击者模型如图 15 所示, 蓝色标识的库所和变迁表示 CPN 模拟的密钥恢复攻击。攻击者通过变迁 TA 截获协议传输的消息。库所 P1、P2、P3、P4、P5、P7、P8 以及 P1'、P2'、P3'、P4'、P5'、P7'、P8' 用于存储截获消息后的原子信息。随后, 攻击者利用变迁 TG 和 TG' 对截获的消息实施密钥恢复攻击。接下来, 通过变迁 TC、TE、TC'、TE' 将分



Figure 15 Attacker model of the EN-RSSP

解后的消息重新组合,并分别存储在库所 P6、P10、P6'、P10' 中。最后,攻击者通过变迁 ATTACK 和 ATTACK2 对 AU2 消息和 AU3 信息发起密钥恢复攻击。图中红色标注的库所和变迁模拟了伪造攻击,攻击者通过变迁 ATTACK' 发起伪造攻击。

5.4 EN-RSSP 的安全性验证分析

EN-RSSP 攻击者模型的状态空间分析报告汇总在表 9 中。与 RSSP-II 攻击者模型的状态空间分析报告进行对比分析,可以发现,死节点数量显著降低(从原来的 20 个减少到 4 个)。这一结果表明,攻击者无法对 EN-RSSP 实施密钥恢复攻击或伪造攻击,EN-RSSP 具有较高的安全性。

表 9 EN-RSSP 攻击模型的状态空间分析报告
Table 9 Analysis report on the state space of the EN-RSSP attack model

状态空间信息	密钥恢复攻击	伪造攻击
状态空间节点/个	5 182	8 468
状态空间有向弧/条	20 045	38 531
强连通节点/个	5 182	8 468
强连通弧/条	20 045	38 531
死节点/个	3	1
死变迁/个	0	0

此外,使用 SML 查询设备 A 和设备 B 的密钥信息,查询结果如图 16 所示,从中可以看出,通信双方的密钥值相同,这表明攻击者的攻击行为未能得逞。这是因为会话密钥的生成与协商是基于可信第三方的,并采用椭圆曲线双线性对的离散对数困难特性和哈希函数进行加固,这使得攻击者无法成功获得密钥信息,也难以实施篡改攻击。不仅如此,在通信过程中还添加了时间戳这一安全属性,使攻击者无法成功实施重放攻击。

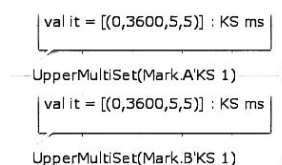


图 16 基于攻击者的 EN-RSSP 查询结果

Figure 16 Based on the attacker's EN-RSSP query results

6 安全性分析和性能评估

6.1 安全性对比

针对 RSSP-II 存在的密钥恢复与伪造安全漏洞, Liang 等^[17]提出了一种改进方案,本文选取该方案与 RSSP-II、EN-RSSP 展开安全性对比分析,结果见表 10。表中的“√”表示协议能够抵御定制类型的攻击,“×”表示无法抵御定制类型的攻击。

表 10 协议的安全性对比

Table 10 Security comparison of protocols

协议	密钥恢复攻击	伪造攻击	重放攻击	匿名性	中间人攻击	前后向安全性
RSSP-II	×	×	√	×	√	√
文献[17]	√	√	×	×	√	×
EN-RSSP	√	√	√	√	√	√

从表 10 可以看出, RSSP-II 无法抵御密钥恢复攻击和伪造攻击。文献[17]提出的方案尽管能够有效抵御密钥恢复攻击和伪造攻击,但无法抵御重放攻击,并且不满足匿名性和前后向安全性需求。本文提出的 EN-RSSP 不仅能够抵御密钥恢复攻击、重放攻击、伪造攻击、中间人攻击,还能满足匿名性和前后向安全性需求。

EN-RSSP 采用双重加密机制,弥补了 RSSP-II 完全依赖对称密钥 KMAC 的不足,有效提高了抵御密钥恢复和伪造攻击的能力。该协议基于可信第三方,并采用椭圆曲线双线性对的离散对数困难特性和哈希函数进行加固,使得攻击者无法通过会话密钥获得数据的完整消息,从而可以抵御密钥恢复、伪造攻击。

此外, EN-RSSP 在加密和验证过程中使用了双方的身份信息和时间戳,将消息隐藏在由多条信息构成的文本(Text3 和 Text5)中,接收方无法知道具体的身份信息,从而保证了匿名性。因受可信第三方的保护,攻击者无法获取设备的私钥来进行伪装攻击。同时,由于在通信双方设备的信息中加入了时间戳的安全属性,可以有效抵御重放攻击和中间人攻击。

综上所述,相比其余两种方案, EN-RSSP 具有更高的安全性。

6.2 性能评估

本节从计算开销维度评估EN-RSSP的性能。在配置为Intel(R) Core i7-9750H处理器、8 GB内存的Ubuntu 18.04 LTS环境下,采用Python库对多种密码学操作进行模拟实验,各项密码操作执行时间见表11,其中部分数据引用自文献[27]。其中, T_H 表示哈希函数, T_{SE} 表示对称加密运算, T_{ME} 表示对称解密运算, T_M 表示椭圆曲线点乘运算, T_P 表示椭圆曲线公钥加密运算, T_{bp} 表示双线性配对、 T_{mp} 表示映射到其上的点运算, T_{ECDH} 表示ECDH运算, T_S 表示私钥签名, T_{SV} 表示签名认证运算。

表 11 密码操作执行时间

Table 11 Execution time of password operation			
符号	执行时间/ms	符号	执行时间/ms
T_H	0.41	T_{bp}	234.62
T_{SE}	4.12	T_{mp}	3.927 9
T_{ME}	0.12	T_{ECDH}	117.31
T_M	1.205 1	T_S	88
T_P	3.615 3	T_{SV}	249

本文选取了4种与铁路通信相关的协议进行了对比分析,结果见表12。

从表12中的数据可以看出,RSSP-II的计算开销较低,但是其无法有效抵御密钥恢复攻击和伪造攻击。文献[17]提出的协议,通过改进的ECDH密钥协商算法增强了安全性,具有较高的计算开销,但其在安全性上存在一定的不足,未能有效抵御重放攻击,并且未能满足前后向安全性需求。文献[34]提出的协议,通过引入椭圆曲线加密和签名算法,显著提高了协议的安全性。但是这一改进也带来了计算开销的大幅增加,不适合资源受限场景。

表 12 不同协议的计算开销对比

Table 12 Comparison of computational costs for different protocols			
协议	发送端计算开销	接收端计算开销	总开销/ms
RSSP-II	$5T_{SE}$	$5T_{SE}$	41.2
文献[17]	$2T_P + 2T_M + T_{ECDH} + T_H$	$2T_P + 2T_M + T_{ECDH} + T_H$	254.841 6
EN-RSSP	$2T_M + 3T_H + T_{mp} + 2T_P + 2T_{bp} + T_{SE} + T_{SD}$	$2T_M + 3T_H + T_{mp} + 2T_P + 2T_{bp} + T_{SE} + T_{SD}$	976.317 4
文献[34]	$3T_{SV} + 4T_H + T_M + 2T_S + 2T_P$	$2T_{SV} + 16T_H + T_M + 4T_P + T_S$	1 541.301 7

EN-RSSP采用非对称加密与对称加密结合的算法,计算开销略高,但其在保证高安全性的同时,相比文献[34]提出的协议的计算开销要小一些,这使其在高安全性的场景中依然能够平稳运行[34]。

为了更直观地呈现EN-RSSP与其他铁路通信协议在计算开销方面的差异,本文对表12的数据进行了可视化处理,结果如图17所示。从图中可以清晰地看出,EN-RSSP在安全性与计算开销之间实现了良好的平衡,尤其适用于列车行驶过程中对数据传输要求较高的场景。

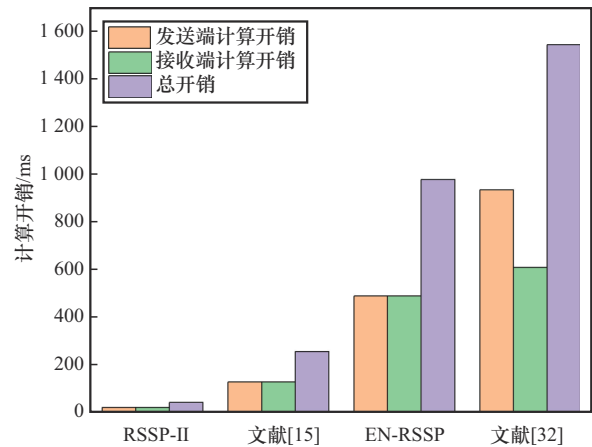


图 17 铁路通信相关协议计算开销对比

Figure 17 Comparison of computational overheads of relevant railway communication protocols

7 结束语

本文以RSSP-II为研究对象,使用CPN工具对其进行建模,并引入Dolev-Yao攻击者模型对该协议进行安全分析,证实RSSP-II中消息鉴别层确实存在密钥恢复、伪装攻击漏洞。为此,本文提出了改进方案EN-RSSP。

EN-RSSP通过可信的第三方动态计算并发送设备的临时密钥对,同时结合椭圆曲线双线性对

的离散对数困难特性和哈希函数来动态协商会话密钥,从而有效抵御密钥恢复攻击、伪装攻击。此外,EN-RSSP在消息传输过程中采用双重加密体系,并引入时间戳和CMAC消息认证码,确保安全相关设备间消息的保密性和完整性。形式化分析结果表明,EN-RSSP有效解决了RSSP-II存在的安全问题,增强了协议的整体安全性,并且在安全性与计算开销之间实现了良好的平衡。

下一阶段的工作将聚焦于在真实设备上部署已构建的协议,以验证其在模拟场景中的各项性能表现,并深入评估该方案在实际应用中的可行性,从而进一步确认协议的安全性。与此同时,研究引入区块链技术,并优化密钥协商方案,从而在提升安全性的同时降低计算开销。

参考文献:

- [1] LIU Y H, ZHAO H. Reliability analysis of CTCS-3 train operation control systems via binary decision diagrams method[C]//Proceedings of the 2018 IEEE International Conference on Information and Automation (ICIA). Piscataway: IEEE Press, 2018: 728-733.
- [2] XU W. High-speed railway signal system information security analysis and countermeasures[C]//Proceedings of the 2017 Chinese Automation Congress (CAC). Piscataway: IEEE Press, 2017: 4862-4866.
- [3] 李敏. 基于铁路RSSP-2安全通信协议的应用研究[D]. 北京: 北京交通大学, 2021.
LI M. Application research of railway RSSP-2 secure communication protocol[D]. Beijing: Beijing Jiaotong University, 2021.
- [4] LIAN H Z, MA L C, CAO Y. Improvement of key management mechanism for RSSP-II and its formal modeling and verification[C]//Proceedings of the 4th International Conference on Electrical and Information Technologies for Rail Transportation (EITRT) 2019. Berlin: Springer, 2020: 1-10.
- [5] 张凯, 伍忠东, 刘菲菲. 铁路信号安全协议中消息认证码算法的研究[J]. 铁道标准设计, 2020, 64(5): 181-189.
ZHANG K, WU Z D, LIU F F. Research on message authentication code algorithm in railway signal safety protocol[J]. Railway Standard Design, 2020, 64(5): 181-189.
- [6] 代新月. 基于认证加密机制的列控信号安全通信协议研究[D]. 四川: 西南交通大学, 2019.
DAI X Y. Research on signaling control signal safety communication protocol based on authentication encryption mechanism[D]. Sichuan: Xinan Jiaotong University, 2019.
- [7] WU P W, WU Z D, LI L Y. Research on MAC verification code of railway signal security communication protocol[J]. Journal of Physics: Conference Series, 2021, 1757(1): 012166.
- [8] 徐倩, 林俊亨. RSSP-II协议消息鉴定层的形式化描述及验证[J]. 计算机应用与软件, 2023, 40(6): 77-82, 180.
XU Q, LIN J T. Formal description and verification of message authenticate safety layer in RSSP-II[J]. Computer Applications and Software, 2023, 40(6): 77-82, 180.
- [9] 王海龙. RSSP-II安全通信协议在RBC/CBI接口中的特殊点[J]. 铁路通信信号工程技术, 2010, 7(6): 24-26.
WANG H L. Special cases of RSSP-II safety communication protocol for RBC/CBI interface[J]. Railway Signalling & Communication Engineering, 2010, 7(6): 24-26.
- [10] 刘国靖, 王静, 杨晓峰. RSSP-II安全通信协议软件自动测试研究[J]. 中国新通信, 2021, 23(9): 17-18.
LIU G J, WANG J, YANG X F. Research on automatic testing of RSSP-II security communication protocol software[J]. China New Telecommunications, 2021, 23(9): 17-18.
- [11] 乐超, 徐中伟, 陈邦兴, 等. 基于RSSP-II安全通信协议的TSRS-CTC测试接口设计与实现[J]. 机电一体化, 2016, 22(12): 48-54.
LE C, XU Z W, CHEN B X, et al. Design and implementation of TSRS-CTC test interface based on RSSP-II secure communication protocol[J]. Mechatronics, 2016, 22(12): 48-54.
- [12] 刘振玉, 任军. RSSP-II安全通信协议软件的自动测试设计及实现[J]. 铁路通信信号工程技术, 2015, 12(6): 44-47.
LIU Z Y, REN J. Automatic testing design and implementation of RSSP-II software[J]. Railway Signalling & Communication Engineering, 2015, 12(6): 44-47.
- [13] 左林, 刘贞, 王一民. SM4分组密码算法在RSSP-II铁路信号安全通信协议中的应用[J]. 铁路通信信号工程技术, 2020, 17(8): 24-27.
ZUO L, LIU Z, WANG Y M. Applications of SM4 block cipher algorithm in RSSP-II railway signal safety communication protocol[J]. Railway Signalling & Communication Engineering, 2020, 17(8): 24-27.
- [14] 张淼, 耿宏亮. 铁路信号安全通信协议中消息验证码算法的安全性分析和改进[J]. 铁路通信信号工程技术, 2014, 11(6): 4-7, 17.
ZHANG M, GENG H L. Security analysis and improvement of MAC algorithm in railway signal safety communication protocol[J]. Railway Signalling & Communication Engineering, 2014, 11(6): 4-7, 17.
- [15] 郭伟, 闫连山, 王小敏, 等. RSSP-II铁路信号安全通信协议的安全性分析[J]. 铁道学报, 2016, 38(8): 50-56.
GUO W, YAN L S, WANG X M, et al. Security analysis of railway signal safety communication protocol II[J]. Journal of the China Railway Society, 2016, 38(8): 50-56.
- [16] 张元玲, 徐中伟, 万勇兵, 等. 铁路信号安全通信协议中的MAC改进算法[J]. 计算机工程, 2012, 38(3): 246-248.
ZHANG Y L, XU Z W, WAN Y B, et al. Improved MAC algorithm in railway signal safety communication protocol[J]. Computer Engineering, 2012, 38(3): 246-248.
- [17] LIANG Z D, HEI X H, WANG Y C, et al. Analysis and protection of DDos attack based on RSSP-II protocol[C]//Proceedings of the 2018 International Conference on Networking and Network Applications (NaNA). Piscataway: IEEE Press, 2018: 117-120.

- [18] HEI X H, GAO W, WANG Y C, et al. Railway key exchange scheme for improving communication efficiency of RSSP-II protocol[C]//Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps). Piscataway: IEEE Press, 2019: 1-6.
- [19] XU M H, ZHAO H B. Simulation and verification of RSSP-II safety communication protocol[C]//Proceedings of the 2012 Second International Conference on Business Computing and Global Informatization. Piscataway: IEEE Press, 2012: 731-734.
- [20] 和晟姣. RSSP-2 协议安全性建模及铁路信号系统网络安全分析[D]. 北京: 北京交通大学, 2016.
HE S J. Security modeling of the RSSP-2 protocol and network security analysis of railway signal systems[D]. Beijing: Beijing Jiaotong University, 2016.
- [21] SANTOS F A, RODRÍGUEZ R J, FEITOSA E L. Automated broken object-level authorization attack detection in REST APIs through OpenAPI to colored Petri nets transformation[J]. International Journal of Information Security, 2025, 24(2): 83.
- [22] BHURKE A U, KAZI F. Methods of formal analysis for ICS protocols and HART - IP CPN modelling[C]//Proceedings of the 2021 Asian Conference on Innovation in Technology (ASIANCON). Piscataway: IEEE Press, 2021: 1-7.
- [23] LAGES D, BORBA E, TAVARES E, et al. A CPN-based model for assessing energy consumption of IoT networks[J]. The Journal of Supercomputing, 2023, 79(12): 12978-13000.
- [24] ZHANG J L, MIAO X H. Application of colored Petri nets in security protocol analysis[C]//Proceedings of the International Conference on Algorithms Software Engineering and Network Security. New York: ACM, 2024: 676-682.
- [25] ZROUG S, KAHLOUL L, BENHARZALLAH S, et al. A hierarchical formal method for performance evaluation of WSNs protocol[J]. Computing, 2021, 103(6): 1183-1208.
- [26] BENJBARA C, HABBANI A, MOUCHFIQ N. New multipath OLSR protocol version for heterogeneous Ad Hoc networks[J]. Journal of Sensor and Actuator Networks, 2022, 11(1): 3.
- [27] 郑路, 冯涛, 苏春华. 基于 CPN 的车载网络无证书匿名认证和密钥协商方案研究[J]. 通信学报, 2024, 45(6): 101-116.
ZHENG L, FENG T, SU C H. Research on certificateless anonymous authentication and key agreement scheme of vehicle network based on CPN[J]. Journal on Communications, 2024, 45(6): 101-116.
- [28] 龚翔, 冯涛, 杜谨泽. 基于 CPN 的安全协议形式化建模及安全分析方法[J]. 通信学报, 2021, 42(9): 240-253.
GONG X, FENG T, DU J Z. Formal modeling and security analysis method of security protocol based on CPN[J]. Journal on Communications, 2021, 42(9): 240-253.
- [29] ZHENG L, FENG T, XIE Z L, et al. BARM: blockchain-assisted anonymous authentication and reputation management for mobile crowdsensing in internet of vehicles[J]. IEEE Internet of Things Journal, 2025, (99): 1.
- [30] HEIDARI A, ALI JABRAEIL J M, NAVIMIPOUR N J. An innovative performance assessment method for increasing the efficiency of AODV routing protocol in VANETs through colored timed Petri nets[J]. Concurrency and Computation: Practice and Experience, 2025, 37(3): e8349.
- [31] ALI N, PUNNEKKAT S, RAUF A. Modeling and safety analysis for collaborative safety-critical systems using hierarchical colored Petri nets[J]. Journal of Systems and Software, 2024, 210: 111958.
- [32] WANG D, CAO Y, LAM K Y, et al. An accountable GAKA protocol with changeable thresholds and verifiable shares in UAVs-assisted IoVs for emergency rescue[J]. IEEE Transactions on Intelligent Transportation Systems, 2025, 26(4): 5522-5537.
- [33] SMART N P. Identity-based authenticated key agreement protocol based on Weil pairing[J]. Electronics Letters, 2002, 38(13): 630-632.
- [34] 陈永, 刘雯, 詹芝贤. 基于混合密钥增强的 LTE-R 车地认证密钥协商方案[J]. 铁道学报, 2023, 45(6): 69-79.
CHEN Y, LIU W, ZHAN Z X. A train-to-ground authentication key agreement enhanced scheme based on hybrid security key for LTE-R[J]. Journal of the China Railway Society, 2023, 45(6): 69-79.

[作者简介]



冯涛 (1970-), 男, 甘肃临洮人, 兰州理工大学研究员、博士生导师, 主要研究方向为网络与信息安全。



铁小平 (1999-), 女, 甘肃永登人, 兰州理工大学硕士生, 主要研究方向为网络与信息安全。



吴毅 (1999-), 男, 甘肃景泰人, 兰州理工大学博士生, 主要研究方向为工业物联网安全、工控协议安全等。



石建明 (1994-), 男, 甘肃张掖人, 兰州理工大学博士生, 主要研究方向为工业物联网协议安全分析。