基于身份认证的 BACnet/IP 分析与改进

谢鹏寿[1]，朱家锋[1]，康永平[2]，冯涛[1]，李威[1]，冉玉翔[1]
（1. 兰州理工大学计算机与通信学院，甘肃 兰州 730050；2. 兰州理工大学机电工程学院，甘肃 兰州 730050）

摘 要：为了解决 BACnet/IP 身份认证存在多种可攻击漏洞和密钥泄露带来的安全问题，提出了一种安全增强的 BACnet/IP-SA 协议认证方案。研究协议身份认证消息流模型，基于着色 Petri 网理论和 CPN Tools 对身份认证消息流建模，采用 Dolev-Yao 攻击者模型和形式化分析方法对 BACnet/IP 进行安全性分析，发现协议漏洞并提出改进方案。BACnet/IP-SA 协议使用设备的伪身份来保护真实身份信息，使用 PUF 响应进行认证，通过多信息集合的验证值来验证端身份的真实性并生成会话密钥。结合 BAN 逻辑和非形式化方法，对协议的安全性进行了证明。实验结果表明，所提方案能有效抵抗多类攻击和密钥泄露带来的安全威胁，在减少计算开销的同时增强了协议身份认证的安全性。

关键词：BACnet/IP；形式化分析；着色 Petri 网；BAN 逻辑；协议改进
中图分类号：TP309
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2024057

Analysis and improvement of the BACnet/IP based on identity authentication

XIE Pengshou[1], ZHU Jiafeng[1], KANG Yongping[2], FENG Tao[1], LI Wei[1], RAN Yuxiang[1]
1. School of Computer and Communications, Lanzhou University of Technology, Lanzhou 730050, China
2. School of Mechanical and Electrical Engineering, Lanzhou University of Technology, Lanzhou 730050, China

Abstract: To solve security issues arising from multiple attackable vulnerabilities and key leakage in BACnet/IP authentication, a security-enhanced BACnet/IP-SA protocol authentication scheme was proposed. By analyzing the authentication message flow model of the protocol and modeling it using colored Petri net theory and CPN Tools, vulnerabilities in the security of BACnet/IP were identified. An improvement scheme was proposed based on the Dolev-Yao attacker model and formal analysis method. The BACnet/IP-SA protocol utilized the device's pseudo-identity to safeguard the actual identity information. It emploied the PUF response for authentication and verified the authenticity of the counterparty's identity. The session key was generated through the authentication value of the multi-information set. The protocol's security was demonstrated by combining BAN logic and non-formal methods. The experimental results indicate that the proposed scheme can effectively resist security threats from multi-class attacks and key leakage, enhancing the security of the protocol authentication while reducing computational overhead.

Keywords: BACnet/IP, formal analysis, colored Petri net, BAN logic, protocol improvement

0 引言

智能建筑是建筑技术与信息技术有机结合的产物，能够为人们提供高效、舒适、温馨、安全和便利的居住环境。在智能建筑中，以信息技术为基础的楼宇自控系统（BAS, building automation system）是智能建筑各功能和可持续发展的主体[1]。通过对各个设备内部可编程逻辑控制器的集成，BAS

收稿日期：2023−09−01；**修回日期：**2024−02−20
通信作者：朱家锋，zhujiafeng688@163.com
基金项目：国家自然科学基金资助项目（No.61862040, No.62162039）
Foundation Items: The National Natural Science Foundation of China (No.61862040, No.62162039)

实现了对能源管理、监控、空调、电梯等建筑设备的控制[2]。不同厂商根据自己的产品特点开发了各自不同的标准，如 LonTalk、PROFIBUS、KNX 等[3]，但这些标准只能保障厂商内部产品的互操作性，很难实现不同厂商产品的互操作性[4]。诞生于 1995 年的建筑自动化控制网络（BACnet, building automation control network）标准成功解决了这一问题[5]。BACnet 标准由美国制冷和空调工程师学会（ASHRAE, American Society of Heating, Refrigerating, and Air-Conditioning Engineers）为楼宇之间实现自动控制系统而制定的一类新型的网络数据通信标准，是楼宇自控领域中第一个开放性的组织标准，正式编号为 ANSI/ASHRAE135-1995[6]。

为了使不同厂商的设备保持互操作性，BACnet 支持 IP、Ethernet、MS/TP、PTP、ZigBee、LonTalk 和 ARCNET 这 7 种类型的局域网，通过身份认证后可使用不同服务器或工作站操作不同局域网的设备[7]。BACnet 协议作为楼宇自控系统的通信基础，运行时需要保持与传感器的通信，来完成包括设备数据、音频数据、图片数据和普通视频数据的采集及各项指令的分发工作[8]。随着互联网在楼宇自控系统中的应用，BACnet 所连接的控制系统变得更加庞大。操作员在远端实时掌握设备运行信息和状态，以便能及时处理紧急操作和维护工作，从而为用户提供更好的服务[9]。在互联网兴起的大背景下，利用 IP 技术将是楼宇自控领域中网络控制系统的发展趋势，为了拓展 BACnet，开发人员定义了 BACnet/IP（后文简称为原方案）[10]。然而，BACnet/IP 在设计之初未考虑到操作员通过接入互联网实现远端操作的功能，导致其在设备认证方面存在缺陷，使攻击者很容易截获和篡改发送的数据，给整个系统带来网络与信息安全威胁[11]。

为了保障楼宇自控系统下的信息安全，服务器和 BACnet 内部设备需要对通信参与者进行身份认证，并在公开信道上建立安全有效的会话密钥。Feng 等[12]针对 BACnet/IP 在设备认证过程中存在的会话密钥泄露和消息篡改问题，提出改变密钥分发方式和引入随机数的方法，但未保护设备的真实身份。Feng 等[13]发现 BACnet/IP 存在重放、欺骗和篡改 3 种攻击漏洞，并针对这些漏洞，提出利用时间戳和引入随机数的方法增强设备间会话的安全性，但未重视设备身份安全的重要性。Feng 等[14]基于着色 Petri 网理论和 Dolev-Yao 攻击者模型的形式化分析方法对 LonTalk 认证协议进行分析，发现 LonTalk 认证协议存在重放、篡改和欺骗 3 种可攻击的漏洞，提出了一种添加可信第三方服务器的 LonTalk-SA 认证协议，虽然该服务器可以认证发送方和接收方的身份，同时通过随机数的 XOR 操作生成会话密钥，但未保护会话双方的身份隐私。

除上述数据安全方面的直接威胁外，侧信道攻击被视为一种间接的威胁[15]。侧信道攻击的目的是从系统中提取秘密，该攻击并不直接针对程序或其代码，而是通过测量和分析物理参数（如执行时间、电磁发射和电源电流）来收集信息。简单地说，侧信道攻击通过系统无意中泄露的信息来破坏加密，这种攻击对具有集成密码系统的模型构成了严重威胁。目前，侧信道分析技术已经成功地破解了许多鲁棒算法密码[16]。因此，本文考虑了侧信道攻击对系统攻击的可能性。

综上所述，现有的 BACnet/IP 没有匿名化设备身份，容易导致中间人攻击、拒绝服务（DoS）攻击、侧信道攻击等安全威胁发生。本文在 BACnet/IP 的基础上提出了一种安全增强的 BACnet/IP-SA（SA, security analysis）协议。

本文主要的贡献如下。

1) 利用着色 Petri 网（CPN, colored Petri net）理论和 CPN Tools 工具[17]对 BACnet/IP 的消息流建模，验证该模型的正确性；使用 Dolev-Yao 攻击者模型分析了协议的安全性，发现该协议存在仿冒攻击、重放攻击和篡改攻击等安全缺陷[18]。

2) 针对该协议存在的安全缺陷，提出了一种新的改进方案。该方案基于物理不可克隆函数（PUF, physical unclonable function）建立认证会话协议 BACnet/IP-SA，该协议使用简单哈希和异或运算保证消息的前向和后向保密性，使用设备的伪身份增加匿名属性，协议包含 2 个消息交互，增强了协议安全性。

3) 采用 BAN（Burrows-Abadi-Needham）逻辑证明和非形式化方法分析验证 BACnet/IP-SA 协议的安全性。与原方案和其他改进方案性能相比，该方案在匿名性、前向和后向保密性、抗仿冒攻击和密钥泄露攻击方面有了显著提升，同时减少了计算开销，在保证可用性和保密性的情况下，通信开销保持在合理的水平，具有较高的运行性能。

1　预备知识

1.1　BACnet/IP 系统模型

BACnet/IP 主要应用于智能建筑中，通过统一的数据通信标准，为各生产商生产的设备提供相互通信，进而达到了设备之间相互操作的目的[19]。BACnet/IP 主要提供了对等实体识别、数据源识别、操作员身份识别和数据保密与完整性方面的安全机制，并为实现上述安全功能定义了 2 个服务：请求密钥服务和认证服务。

如图 1 所示，本文提出的 BACnet/IP 系统模型主要由 BACnet 设备（SD_j）、服务器（SERVER）和外部 BACnet 设备（SD_i）组成。

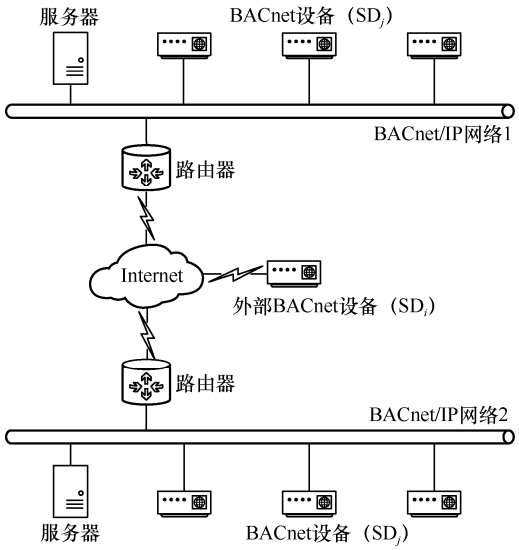


图 1　BACnet/IP 系统模型

1) BACnet 设备（SD_j）。BACnet 设备指已经部署在楼宇自控系统中的各个子系统（如照明系统、空调系统等）的传感器设备，主要用于采集楼宇数据，如温度、湿度、照明控制等，并将这些数据定期发送给控制中心。SD_j 属于 BACnet/IP 网络内部设备，已经被服务器确定了合法性，能够与服务器安全通信。

2) 服务器（SERVER）。服务器可整合整个楼宇内各个子系统的数据，为新加入某个子系统的设备或 BACnet/IP 网络设备提供设备认证、密钥交换、信息传输和信息服务等功能。

3) 外部 BACnet 设备（SD_i）。对于 BACnet/IP 网络中的服务器和设备来说，SD_i 设备是陌生的，它们在获得服务器的认证后为系统服务。SD_i 属于楼宇自控系统中的远端设备或工作站，它们使用互联网与服务器连接并提供系统所需的数据或指令，支撑服务器实现智能调控。

1.2　CPN 理论和 CPN Tools

CPN 是一种数学图形建模语言，具有定义良好的语法和语义。CPN 能够系统地表达协议的运行流程和特点，如并发、同步、资源冲突等，并通过分析系统的有界性、活动性、可达性、冲突、死锁等结构特性来判断系统的整体性能。同时，该方法具有可扩展的特性，可以处理带有条件约束的大规模消息，并支持向变迁添加时间元素[20]。

CPN Tools 是一个较成熟的建模仿真工具，它集成了建模、仿真、执行以及状态空间等实用工具，在工业及研究领域中得到了广泛的应用。该工具主要针对并发系统进行仿真分析，它将标准元语言（ML, meta language）与 Petri 网理论结合起来，具有建立层次化时态 CPN 模型的功能和模型状态空间查询功能，为用户提供一个可视化的集成开发环境[21]。通过 CPN Tools 建模工具导出的状态空间报告和状态空间有向图，可以精确定位错误路径，还可以显示路径中每个节点的状态并用于分析[22]。

本文使用 ML 在 CPN Tools 工具 4.0.1 版本中评估 BACnet/IP 及改进后 BACnet/IP-SA 协议的安全性，该软件运行的硬件环境为 Intel(R) i7-12700 @2.10GHz 处理器，32 GB 内存，Microsoft Windows 11 专业版操作系统。

1.3　攻击模型

Dolev-Yao 攻击者模型是一种基于符号分析的形式化验证方法，用于发现安全协议中可能包含的逻辑缺陷[23]。该模型描述的攻击者 *A* 具有以下能力。

1) *A* 拥有对网络的完全控制，并且可以窃听、阻止和拦截网络上的任何消息，记录了诚实实体之间发送的所有消息。

2) *A* 能够随意发送和重发消息，并能组合和分解消息。

3) *A* 可以执行协议中指定的任何加密操作，并在已知解密密钥的情况下解密加密的消息。

4) *A* 是合法的系统成员，意味着 *A* 在系统中注册，拥有所有的安全参数。

此外，与 eCK（extended Canetti-Krawczyk）安全模型一样，本文考虑了攻击者分别获取各种系统秘密的情况，以使协议尽可能安全[24]。本文使用 Dolev-Yao 攻击者模型模拟攻击者对协议发起仿冒、重放、中间人和密钥泄露攻击，以验证和分析协议的安全属性[25]。

1.4 单向哈希函数

单向哈希函数 $H(\cdot)$ 可以把任意长度的输入生成固定长度的输出[26]，其安全属性如下。

1) 对于给定哈希值 h 和单向哈希函数 $H(\cdot)$，很难找出任何原像 m，使 $h=H(m)$。

2) 对于给定的原像 a，很难找到另一个原像 b，使 $H(a)=H(b)$。

3) 对同一个单向哈希函数 $H(\cdot)$，很难找到 2 个不同的输入，使 $H(a)=H(b)$。

4) 对于给定哈希值 h 和单向哈希函数 $H(\cdot)$，提取相对应的输入 m 是困难的。

在 BACnet/IP-SA 协议中，单向哈希函数把设备伪身份、随机数、时间戳、验证值和 PUF 响应等关键信息之和作为输入生成 256 bit 的输出，来保证协议的各项安全属性。

1.5 物理不可克隆函数

物理不可克隆函数是嵌入物理结构中的物理实体，利用内在的物理构造对其进行唯一性标识，输入任意激励都会输出一个唯一且不可预测的响应。PUF 提供了一对从激励到响应的不可逆映射，与 Hash 函数有相似性，但非计算复杂性理论[27]。这种“激励–响应”映射容易实现且功耗极低，广泛应用于资源受限设备的安全认证[28]。由于轻量级、无密钥和防篡改，它为身份认证提供了强大的信任基础。PUF(·) 还可以充当设备的数字指纹[29]。Modarres 等[30]已经提出了使用 PUF 和无线指纹的双因素认证协议可以提高协议安全性。PUF 安全特性如下。

1) 唯一性。通过提取芯片制造过程中必然引入的工艺参数偏差，实现激励信号与响应信号唯一对应的函数功能。对于任意 2 个不同的 PUF，即 $\mathrm{PUF}_1(\cdot)$ 和 $\mathrm{PUF}_2(\cdot)$，给定同一输入 C，其输出 $R_1 \leftarrow \mathrm{PUF}_1(C)$ 和 $R_2 \leftarrow \mathrm{PUF}_2(C)$ 是不同的。

2) 可再现性。对同一集成芯片使用相同激励可以得到同一响应。

3) 不可克隆性。由于集成芯片制造技术限制，理论上不可能有完全相同的两块集成芯片。

4) 单向性。对于给定响应 R 和特定的 PUF(·)，不能逆向生成其激励 C。

本文中，设备 SD_i 和 SD_j 在注册阶段通过激励生成 PUF 响应并保存在服务器和本地内存中，之后在认证阶段设备 SD_i 和 SD_j 使用 PUF 响应作为验证值的一个因素，结合时间戳、随机数等信息，通过单向哈希函数生成验证值及会话密钥，来确保会话密钥的安全属性。

尽管 PUF 具有高可靠性，但其存在一个典型的问题，即函数输出对环境敏感。由于 PUF 响应是从电路中的微小物理变化中提取的，如温度、电压变化和时间等环境效应会在 PUF 响应中引入噪声。针对这一问题，Millwood 等[31]提出了一种基于新型 PUF 的机器学习分类系统，能准确地识别 PUF 响应的来源并确定其有效性，可作为依赖辅助数据的去噪技术方案。

2 基于 CPN 的 BACnet/IP 安全评估

2.1 BACnet/IP 消息流建模

BACnet/IP 在安全服务方面主要通过请求密钥规程和对等实体验证规程来确保设备身份认证的安全性。BACnet/IP 身份认证消息流模型使用密码学术语 Alice-Bob 语言描述，如图 2 所示，SK_{ab} 表示设备 A 和设备 B 的会话密钥，IDA、IDB 表示设备 A 和设备 B 的设备号，且设备号唯一，PK_a 表示设备 A 与服务器的会话密钥，PK_b 表示设备 B 与服务器的会话密钥，Authenticate 表示认证服务，PRN 表示消息中的伪随机数，MRN 表示响应信息中随机修改过的随机数。设备 A 和设备 B 通过运行 DES 算法来生成它们自己的私钥 K_a 和 K_b，且仅与密钥服务器共享。请求密钥规程如下。

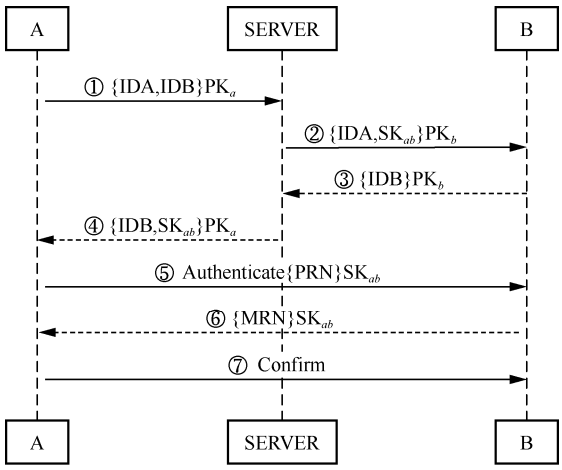


图 2 BACnet/IP 身份认证消息流模型

1) 设备 A 向密钥服务器发起请求，请求服务器分发用于设备 A 和 B 之间通信的会话密钥 SK_{ab}。

2) 在接收到来自设备 A 的密钥分发请求后，服务器生成会话密钥 SK_{ab}，并用设备 B 的公钥 PK_b 对 SK_{ab} 和 IDA 进行加密，然后发送给设备 B。

3) 设备 B 把设备号 IDB 用公钥 PK_b 加密后发送给服务器，服务器验证设备 B 的设备号。

4) 密钥服务器收到消息使用 PK_b 解密，将获得的 IDB 与设备 A 发送的 IDB 进行对比验证，如果一致，则使用设备 A 的 PK_a 对 SK_{ab} 和 IDB 进行加密，发送给设备 A，至此，设备 A 获得与设备 B 通信的会话密钥 SK_{ab}。

对等实体验证规程如下。

1) 设备 A 获得会话密钥 SK_{ab} 后与设备 B 进行认证，并发起一个认证请求。该请求的协议数据部分和伪随机数据使用 SK_{ab} 加密后发送给设备 B。

2) 设备 B 对接收到的设备 A 的认证请求进行解码，将伪随机数改为修改随机数，使用 SK_{ab} 加密，并向设备 A 返回复合消息。

3) 设备 A 对接收到的响应消息进行解密，如果含有“修改随机数”的报文正确，则完成对设备 B 的识别，并向 B 发送 Confirm 确认报文。

2.2　基于 CPN 对 BACnet/IP 形式化分析

本文使用 CPN Tools 软件，运用 Dolev-Yao 攻击者模型，对 BACnet/IP 进行了自顶向下的形式化分析，包括协议顶层模型和 3 个二层模型子页面。在该模型中，变迁用矩形表示；位置用椭圆表示；替代变迁用双线矩形表示，表明该变迁有更详细的子模型；设备间的数据传输用双线椭圆表示。在顶层模型中，库所 M1 到 M7 分别与图 3 中的第 1 到 7 条消息流一一对应。添加 Dolev-Yao 攻击者模型后的 BACnet/IP 身份认证 CPN 顶层模型如图 3 所示，该模型的具体颜色集定义如表 1 所示。

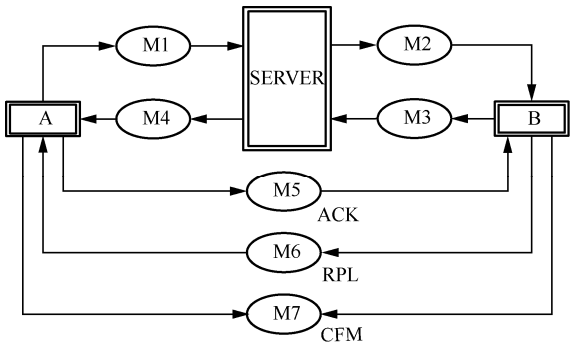


图 3　BACnet/IP 身份认证 CPN 顶层模型

表 1　　颜色集定义

颜色集	描述
ID	包含设备 A 或设备 B
KEY	包含公钥 PK_a、PK_b 和会话密钥 SK_{ab}
NONCE	包含随机数 N_a、N_b、N_c、N_k
DEV	DEV=ID*ID
INFO	INFO=KEY*ID
MSG1	MSG1=DEV*KEY
MSG2	MSG2=INFO*KEY
MSG3	MSG3=ID*KEY
MSG4	MSG4=INFO*KEY
CRY	CRY=NONCE*ID
ACK	ACK=CRY*KEY
RPL	RPL=NONCE*KEY
CFM	CFM=Connected|Unconnected

服务器添加 Dolev-Yao 攻击者模型后的 CPN 模型如图 4 所示。图 4 中，Attack3 模拟重放攻击，Attack4 模拟会话密钥泄露攻击和侧信道攻击，攻击者可以利用会话密钥成功与设备 B 通信。

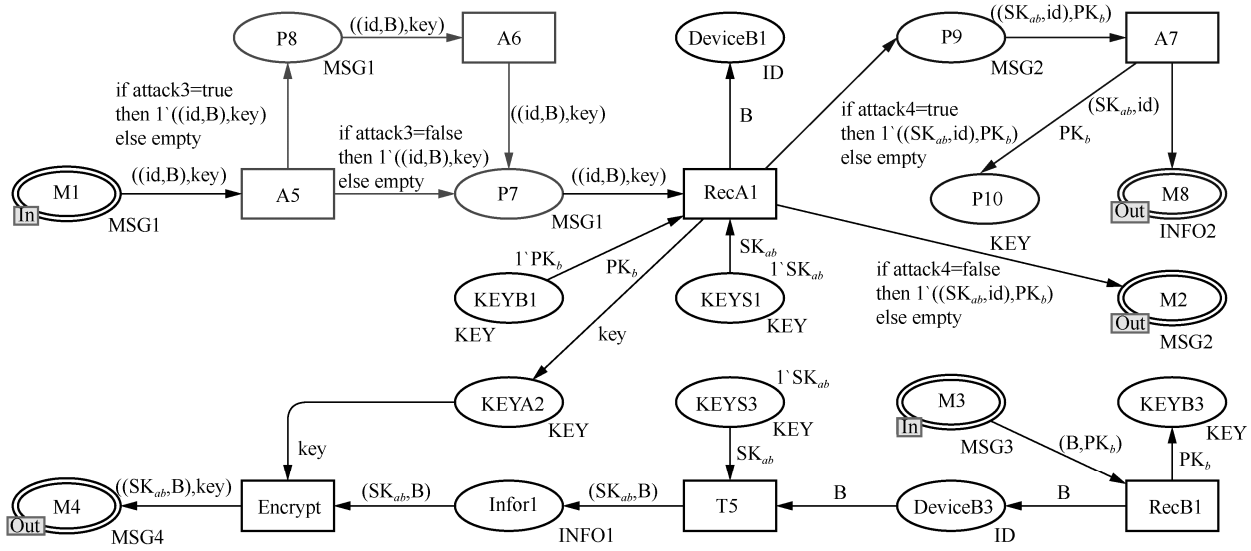


图 4　服务器添加 Dolev-Yao 攻击者模型后的 CPN 模型

设备 A 添加 Dolev-Yao 攻击者模型后的 CPN 模型如图 5 所示。图 5 中，Attack1 和 Attack2 模拟攻击者因密钥泄露、侧信道攻击等方式截获密钥后的仿冒攻击，通过分析信道中的消息，获得公钥 PK_a 和 A 的设备号，并通过设备 C 仿冒设备 A 与服务器通信，获得与设备 B 的会话密钥 SK_{ab}。由于设备 B 代表 BACnet/IP 网络内的安全设备，因此不添加攻击者模型，其 CPN 模型如图 6 所示。

2.3　BACnet/IP 一致性检验与安全分析

本文采用状态空间分析方法分析 BACnet/IP 的一致性。CPN Tools 生成的原始模型状态空间报告如表 2 所示，状态空间节点数及其连通弧数分别与强连通节点数及其弧数相同。这说明所建立的 BACnet/IP 模型没有产生状态循环，所有的状态节

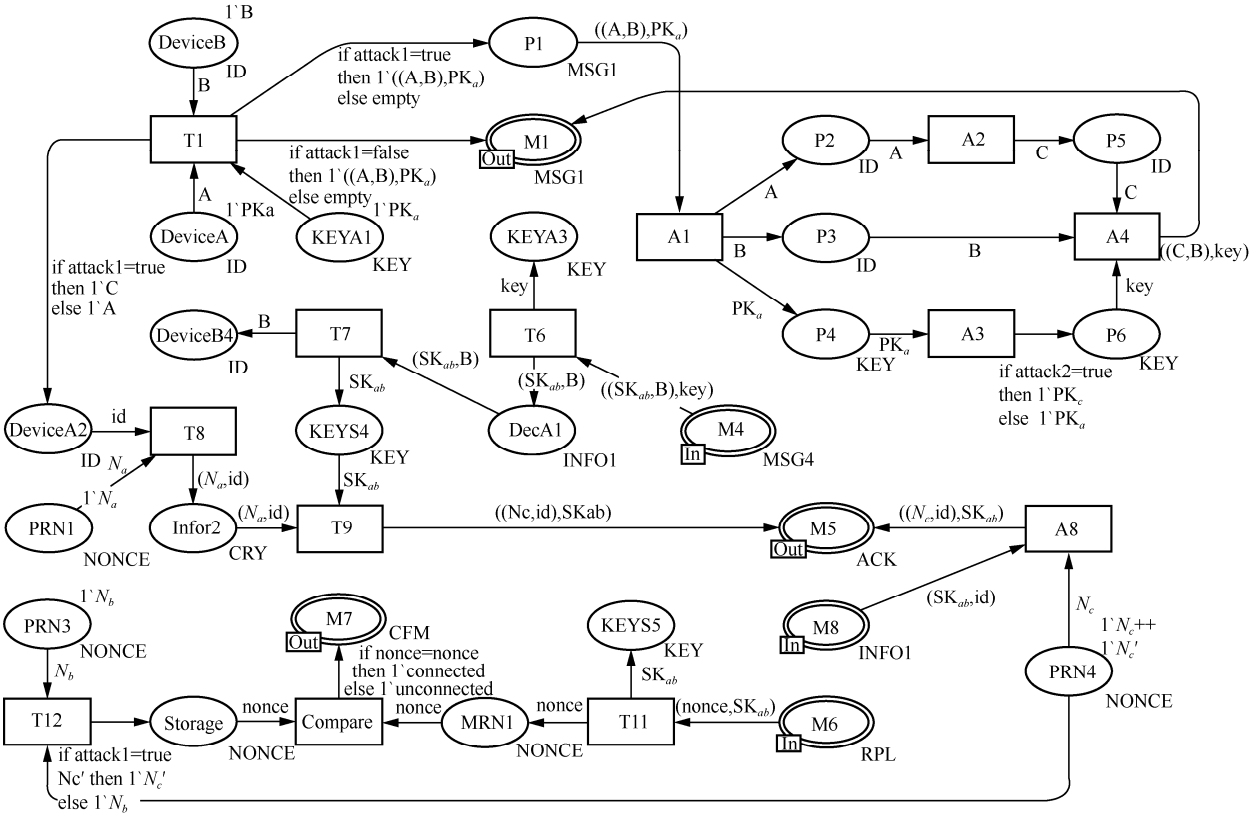


图 5　设备 A 添加 Dolev-Yao 攻击者模型后的 CPN 模型

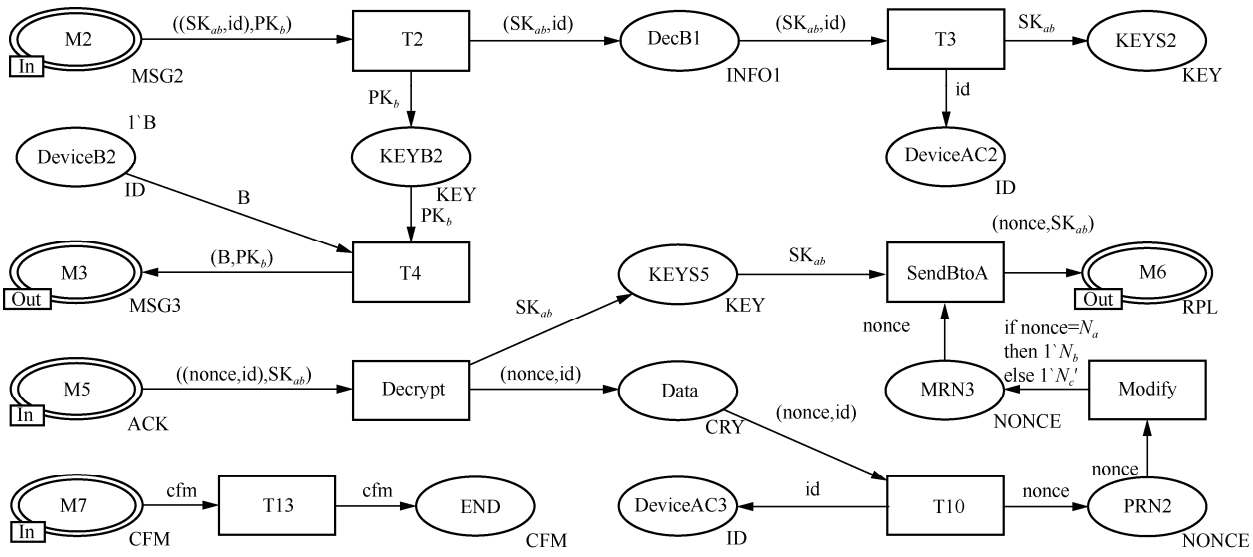


图 6　设备 B 的 CPN 模型

点都是可达的。一个主标记表示模型最终可以收敛到最终节点，一个死标记表示接收方处理了所有请求，且模型没有死变迁。上述分析表明针对 BACnet/IP 的 CPN 建模正确，之后的研究将在此模型基础上展开。

表 2　　原始模型状态空间报告

类型	数量
状态空间节点	96
状态空间连通弧	210
强连通节点	96
强连通弧	210
主标记	1
死标记	1
死变迁	0

本文在 BACnet/IP 模型的网络传输层中引入密钥泄露、仿冒、重放、篡改和侧信道攻击等。攻击者通过上述攻击，根据截获的设备身份信息分析该信息来自哪一台设备，通过密钥泄露或侧信道攻击获得关键密钥时，攻击者可以对设备之间传输的信息进行解密，并篡改传输的信息。

添加攻击者模型的状态空间报告如表 3 所示，状态空间节点数及其连通弧数分别与强连通节点数及其弧数相同。这说明所建立的 BACnet/IP 模型没有产生状态循环，所有的状态节点都是可达的。没有主标记表示模型因为受到攻击后通信连接不会收敛至最终节点。12 个死标记表示在攻击者模型的攻击下，原始模型有 12 处节点处于不安全状态，即在 4 类攻击下，协议存在 12 处漏洞。模型没有死变迁，表示添加攻击者模型未出现逻辑漏洞。对 BACnet/IP 的形式化分析结果表明，现有的协议身份认证方法是不安全的，本文后续将进一步研究协议身份认证部分的改进方法。

表 3　　添加攻击者模型的状态空间报告

类型	数量
状态空间节点	645
状态空间连通弧	1 509
强连通节点	645
强连通弧	1 509
主标记	0
死标记	12
死变迁	0

3　BACnet/IP-SA 三方认证协议

本节描述一种改进的身份认证密钥交换协议 BACnet/IP-SA。该协议分为设备注册阶段和密钥分发阶段。设备注册阶段采用安全信道，密钥分发阶段基于公开信道。本文规定如下假设。

1) 智能设备集成电路（IC）中已经嵌入 PUF。设备工作在恒温恒湿、电源供电稳定、相对封闭的适宜 PUF 芯片和设备良好工作的环境中。

2) 传感器、工作站和其他边缘节点被统称为设备，这些设备是资源受限设备。

3) 服务器具有较强的计算能力并且是安全可信的。本文协议中所使用的符号说明如表 4 所示。

表 4　　符号说明

符号	描述
$\mathrm{ID}_i, \mathrm{ID}_j$	设备 i 或设备 j 的身份标识
P_i, P_j	设备 i 或设备 j 的伪身份
T_n	第 n 个时间戳
$\mathrm{PK}_i, \mathrm{PK}_j$	服务器与设备 i 或设备 j 之间的密钥
$\mathrm{SK}_a, \mathrm{SK}_b$	服务器与设备 i 或设备 j 之间的新密钥
SK_{ab}	设备 i 和设备 j 之间的会话密钥
$< C_i, R_i >$	PUF 的“激励–响应”对
N_a, N_b	随机数
P_i'	设备 i 新的伪身份
$h(\cdot), \oplus, \Vert$	哈希运算，异或运算，连接符

4) BACnet/IP-SA 协议所运行的系统具有冗余配置，其服务器采用“一主一备”的方式工作，能够保证服务质量，不会因为服务器的单点故障、宕机等突发性因素影响系统的可用性和协议的身份认证与密钥交换过程。

3.1　BACnet/IP 外部网络设备注册阶段

在密钥交换之前，设备 SD_i 需要向服务器注册。SD_i 向服务器发送 ID_i、PK_a 以及注册请求 Req_i，服务器收到请求后，随机生成激励 C_i，并将 C_i 发送给设备 SD_i。设备 SD_i 接收到 C_i 后，输出响应 $R_i \leftarrow \mathrm{PUF}_i(C_i)$，并将 $\langle C_i, R_i \rangle$ 发送给服务器。服务器计算 $P_i = h(\mathrm{PK}_a \Vert R_i) \oplus \mathrm{ID}_i$ 作为 SD_i 的伪身份。最终，服务器将 ID_i、P_i、$\langle C_i, R_i \rangle$ 存储在其数据库中，SD_i 将 P_i、C_i 存储在内存中。上述消息同样在安全信道中传输。

3.2 BACnet/IP 内部网络设备注册阶段

设备SD_j向服务器注册，SD_j向服务器发送ID_j、PK_b以及注册请求Req_j，收到请求后，服务器随机生成激励C_j，并将C_j发送给设备SD_j。设备SD_j接收到C_j后，输出响应$R_j \leftarrow \mathrm{PUF}_j(C_j)$，并将$\langle C_j, R_j \rangle$发送给服务器。服务器计算$P_j = h(\mathrm{PK}_b \| R_j) \oplus \mathrm{ID}_j$作为$\mathrm{SD}_j$的伪身份。最终，服务器将$\mathrm{ID}_j$、$P_j$、$\langle C_j, R_j \rangle$存储在其数据库中，$\mathrm{SD}_j$将$P_j$、$C_j$存储在内存中。上述消息同样在安全信道中传输。

3.3 认证密钥交换阶段

设备认证双方将在不可信的信道中协商设备间的会话密钥，本节将对协议身份认证及密钥交换的过程进行说明，如图 7 所示。

1) $\mathrm{SD}_i \rightarrow \mathrm{SD}_j$。设备$\mathrm{SD}_i$根据其内存中的激励$C_i$，输出响应$R_i \leftarrow \mathrm{PUF}_i(C_i)$。然后生成随机数$N_a$和时间戳$T_1$，并利用其内存中的密钥$\mathrm{PK}_a$、$P_i$和$\mathrm{ID}_i$，计算验证信息$G_1 = h(\mathrm{ID}_i \| P_i \| R_i \| N_a \| \mathrm{PK}_a)$，随后$\mathrm{SD}_i$将消息$M_1 = \{P_i, N_a, T_1, G_1\}$通过公开信道发送给设备$\mathrm{SD}_j$。

2) $\mathrm{SD}_j \rightarrow \mathrm{SERVER}$。设备$\mathrm{SD}_j$接收到设备$\mathrm{SD}_i$的消息后，检查时间戳$T_1$，生成随机数$N_b$和时间戳$T_2$，检查通过后计算$G_2 = h(G_1 \| P_i \| P_j \| R_j \| N_b \| \mathrm{PK}_b)$，设备$\mathrm{SD}_j$利用其内存中的激励$C_j$，输出响应$R_j \leftarrow \mathrm{PUF}_j(C_j)$。随后$\mathrm{SD}_j$将消息$M_2 = \{M_1, N_b, T_2, G_2\}$通过公开信道发送给服务器。

3) $\mathrm{SERVER} \rightarrow \mathrm{SD}_j$。服务器收到$\mathrm{SD}_j$的消息后，生成时间戳$T_3$并检查$T_2$的有效性。用内存中的消息$P_i$、$\mathrm{PK}_a$和$R_i$计算得到$\mathrm{ID}_i = h(\mathrm{PK}_a \| R_i) \oplus P_i$，并与内存中的$\mathrm{ID}_i$进行对比，检验$\mathrm{ID}_i$的正确性。然后利用$\mathrm{ID}_i$、$P_i$、$R_i$、$R_j$、$N_a$、$N_b$、$\mathrm{PK}_a$、$\mathrm{PK}_b$和$M_2$中的消息计算验证值$G_1' = h(\mathrm{ID}_i \| P_i \| R_i \| N_a \| \mathrm{PK}_a)$和验证值$G_2' = h(G_1 \| P_i \| P_j \| R_j \| N_b \| \mathrm{PK}_b)$，并将结果与$M_2$

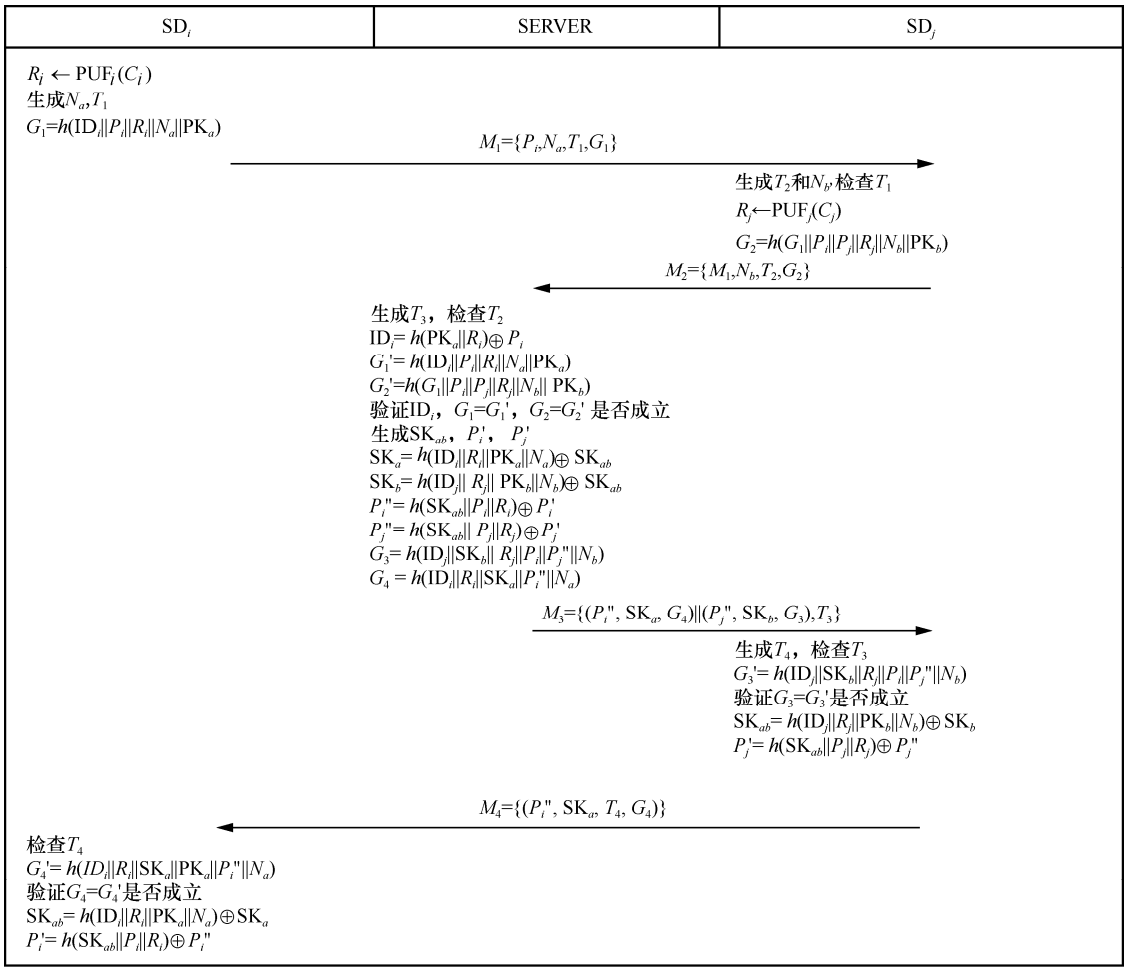


图 7 BACnet/IP-SA 身份认证及密钥交换过程

发来的 G_1、G_2 进行比对，验证 $G_1 = G_1'$ 和 $G_2 = G_2'$ 是否成立。如果验证失败，SERVER 将终止认证密钥交换过程；反之，SERVER 继续执行后续步骤，生成 SD_i 与 SD_j 的会话密钥 SK_{ab} 和 SD_i 新的伪身份 P_i'、SD_j 新的伪身份 P_j'，并计算 $\mathrm{SK}_a = h(\mathrm{ID}_i \| R_i \| \mathrm{PK}_a \| N_a) \oplus \mathrm{SK}_{ab}$，$\mathrm{SK}_b = h(\mathrm{ID}_j \| R_j \| \mathrm{PK}_b \| N_b) \oplus \mathrm{SK}_{ab}$，$P_i'' = h(\mathrm{SK}_{ab} \| P_i \| R_i) \oplus P_i'$，$P_j'' = h(\mathrm{SK}_{ab} \| P_j \| R_j) \oplus P_j'$，$G_3 = h(\mathrm{ID}_j \| \mathrm{SK}_b \| R_j \| P_i \| P_j'' \| N_b)$，$G_4 = h(\mathrm{ID}_i \| R_i \| \mathrm{SK}_a \| P_i'' \| N_a)$。最后，发送消息 $M_3 = \{(P_i'', \mathrm{SK}_a, G_4) \| (P_j'', \mathrm{SK}_b, G_3), T_3\}$ 到 SD_j。

4) $\mathrm{SD}_j \rightarrow \mathrm{SD}_i$。设备 SD_j 收到 SERVER 的消息后，SD_j 生成时间戳 T_4，检查 T_3 的有效性，通过计算 $G_3' = h(\mathrm{ID}_j \| \mathrm{SK}_b \| R_j \| P_i \| P_j'' \| N_b)$ 并验证 $G_3 = G_3'$ 是否成立。如果验证失败，SD_j 将终止认证密钥交换过程；反之，SD_j 继续执行后续步骤，计算 SD_i 与 SD_j 之间的会话密钥 $\mathrm{SK}_{ab} = h(\mathrm{ID}_j \| R_j \| \mathrm{PK}_b \| N_b) \oplus \mathrm{SK}_b$ 和 SD_j 新的伪身份 $P_j' = h(\mathrm{SK}_{ab} \| P_j \| R_j) \oplus P_j''$。至此，$\mathrm{SD}_j$ 新的伪身份 P_j' 和会话密钥 SK_{ab}。之后，SD_j 将消息 $M_4 = \{P_i'', \mathrm{SK}_a, T_4, G_4\}$ 发送给 SD_i。

5) SD_i 首先检查时间戳 T_4，随后使用接收到的消息 M_4 与本地内存中存储的信息 ID_i、R_i、PK_a、N_a 一起计算 $G_4' = h(\mathrm{ID}_i \| R_i \| \mathrm{SK}_a \| \mathrm{PK}_a \| P_i'' \| N_a)$ 并验证 $G_4 = G_4'$ 是否成立。如果验证失败，SD_i 将中断认证密钥交换过程；反之，SD_i 继续执行后续步骤，计算 SD_i 与 SD_j 之间的会话密钥 $\mathrm{SK}_{ab} = h(\mathrm{ID}_i \| R_i \| \mathrm{PK}_a \| N_a) \oplus \mathrm{SK}_a$ 和 $P_i' = h(\mathrm{SK}_{ab} \| P_i \| R_i) \oplus P_i''$。至此，$\mathrm{SD}_i$ 获得了新的伪身份 P_i' 和会话密钥 SK_{ab}。

4　安全性分析

4.1　基于 CPN 对 BACnet/IP-SA 协议安全评估

本节对 BACnet/IP-SA 协议进行了自顶向下的形式化建模和分析，新的模型包括协议顶层模型和 3 个二层模型子页面。在顶层模型中，库所 M1 到 M4 分别对应协议身份认证密钥交换阶段的步骤 1~步骤 4。BACnet/IP-SA 协议的 CPN 顶层模型如图 8 所示。设备 SD_i、服务器和设备 SD_j 的身份认证 CPN 子模型分别如图 9～图 11 所示。

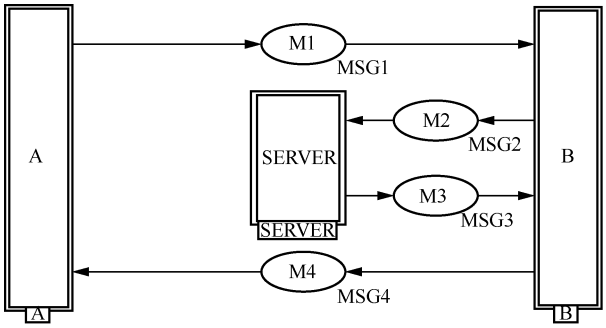


图 8　BACnet/IP-SA 协议的 CPN 顶层模型

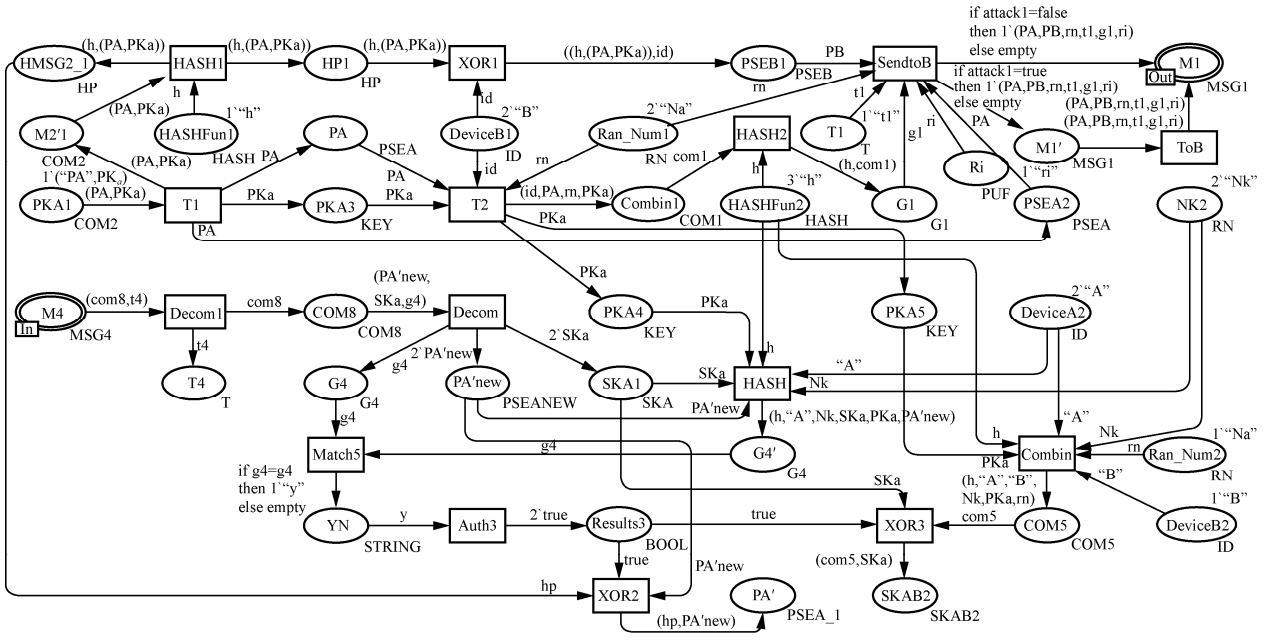


图 9　BACnet/IP-SA 中设备 SD_i 的身份认证 CPN 子模型

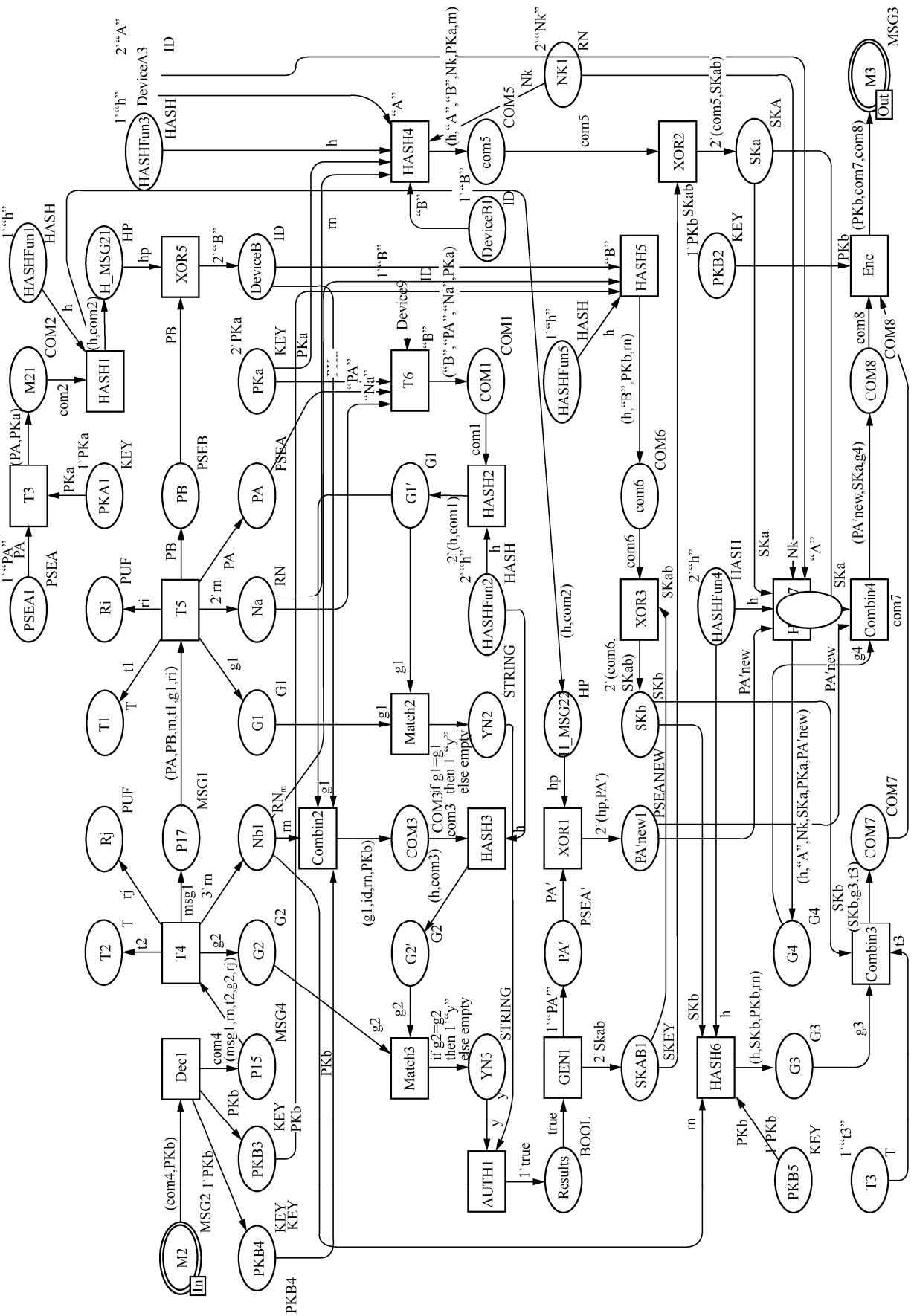


图 10　BACnet/IP-SA 中服务器的身份认证 CPN 子模型

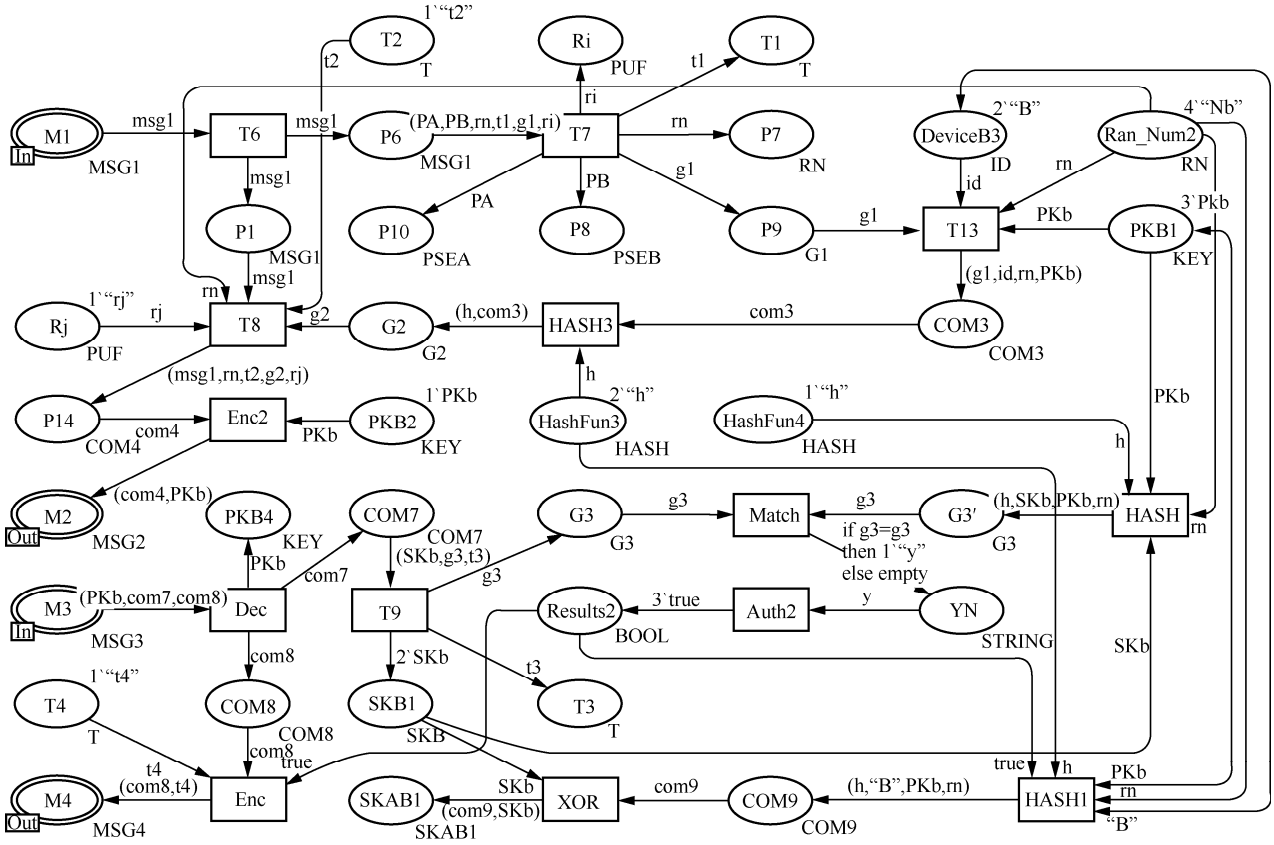


图 11　BACnet/IP-SA 中设备 SD_j 的身份认证 CPN 子模型

BACnet/IP-SA 协议的 CPN 模型状态空间报告如表 5 所示，状态空间节点数及其连通弧数分别与强连通节点数及其弧数相同。这说明所建立的 BACnet/IP 模型没有产生状态循环，所有的状态节点都是可达的。一个主标记表示模型最终可以收敛到最终节点，一个死标记表示接收方处理了所有请求，且模型没有死变迁。

表 5 BACnet/IP-SA 协议的 CPN 模型状态空间报告

类型	数量
状态空间节点	382
状态空间连通弧	931
强连通节点	382
强连通弧	931
主标记	1
死标记	1
死变迁	0

上述分析表明，针对 BACnet/IP-SA 协议的 CPN 建模正确，能够实现设备间的相互认证。引入 Dolev-Yao 攻击者模型后发现，模型抗仿冒、中间人、重放、密钥泄露、侧信道攻击，BACnet/IP-SA 协议达到改进目标。

4.2　BAN 逻辑证明

BAN 逻辑被广泛应用于认证协议的形式化分析，通过研究设备双方认证，描述设备双方相互接收和发送消息的过程以及从最初信任逐渐发展到协议运行的最终信任。本节使用 BAN 逻辑证明 BACnet/IP-SA 协议身份认证密钥交换过程，结果表明，该协议可以实现相互认证。BAN 逻辑符号说明如表 6 所示，BAN 逻辑规则如表 7 所示。

表 6　　BAN 逻辑符号说明

符号	含义
$P \mid\equiv X$	P 相信 X
$P \lhd X$	P 曾经收到包含 X 的消息
$P \mid\sim X$	P 曾经发送包含 X 的消息
$\#X$	X 是新鲜的
$P \mid\Rightarrow X$	P 对 X 有管辖权
$P \overset{K}{\longleftrightarrow} Q$	P 和 Q 之间共享密钥 K
$\langle X \rangle_K$	使用 K 加密 X
(X,Y)	X 和 Y 的连接

表 7 BAN 逻辑规则

标记	规则	计算式
R_1	消息含义规则	$\dfrac{P\mid\equiv Q\xleftrightarrow{K}P, P\lhd\{X\}_K}{P\mid\equiv Q\mid\sim X}$
R_2	管辖权规则	$\dfrac{P\mid\equiv Q\mid\Rightarrow X, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$
R_3	Nonce 验证规则	$\dfrac{P\mid\equiv \#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$
R_4	新鲜度规则	$\dfrac{P\mid\equiv \#(X)}{P\mid\equiv \#(X,Y)}$
R_5	信念规则	$\dfrac{P\mid\equiv (X), P\mid\equiv (Y)}{P\mid\equiv (X,Y)}, \dfrac{P\mid\equiv Q\mid\equiv (X,Y)}{P\mid\equiv Q\mid\equiv X}$

1) 进行 BAN 逻辑分析的理想化前提如下。

消息 1：

$\mathrm{SD}_i\rightarrow\mathrm{SD}_j:\langle P_i,G_1\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}},N_a,T_1$

消息 2：

$\mathrm{SD}_j\rightarrow\mathrm{SERVER}:$

$\langle G_2\rangle_{\mathrm{SD}_j\xleftrightarrow{R_j}\mathrm{SERVER}},N_b,T_2,\langle P_i,G_1\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}},N_a,T_1$

消息 3：

$\mathrm{SERVER}\rightarrow\mathrm{SD}_j:$

$\langle P_i\text{"},\mathrm{SK}_a,G_4\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}}$，$\langle \mathrm{SK}_b,G_3\rangle_{\mathrm{SD}_j\xleftrightarrow{R_j}\mathrm{SERVER}}$，$T_3$

消息 4：

$\mathrm{SD}_j\rightarrow\mathrm{SD}_i:\langle P_i\text{"},\mathrm{SK}_a,G_4\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}},T_4$

2) 需要证明的安全目标如下。

GOAL1：$\mathrm{SD}_i\mid\equiv(\mathrm{SD}_i\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

GOAL2：$\mathrm{SERVER}\mid\equiv\mathrm{SD}_i\mid\equiv(\mathrm{SD}_i\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

GOAL3：$\mathrm{SERVER}\mid\equiv(\mathrm{SD}_i\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

GOAL4：$\mathrm{SD}_i\mid\equiv\mathrm{SERVER}\mid\equiv(\mathrm{SD}_i\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

GOAL5：$\mathrm{SD}_j\mid\equiv(\mathrm{SD}_j\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

GOAL6：$\mathrm{SERVER}\mid\equiv\mathrm{SD}_j\mid\equiv(\mathrm{SD}_j\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

GOAL7：$\mathrm{SERVER}\mid\equiv(\mathrm{SD}_j\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

GOAL8：$\mathrm{SD}_j\mid\equiv\mathrm{SERVER}\mid\equiv(\mathrm{SD}_j\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

3) 本文方案的初始假设如下。

A1：$\mathrm{SD}_i\mid\equiv\#(N_a)$

A2：$\mathrm{SD}_j\mid\equiv\#(N_b)$

A3：$\mathrm{SERVER}\mid\equiv\#(N_a,N_b)$

A4：$\mathrm{SD}_i\mid\equiv(\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER})$

A5：$\mathrm{SERVER}\mid\equiv(\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER})$

A6：$\mathrm{SD}_i\mid\equiv\mathrm{SERVER}\mid\Rightarrow(\mathrm{SD}_i\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

A7：$\mathrm{SERVER}\mid\equiv\mathrm{SD}_i\mid\Rightarrow(\mathrm{SD}_i\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

A8：$\mathrm{SD}_j\mid\equiv(\mathrm{SD}_j\xleftrightarrow{R_i}\mathrm{SERVER})$

A9：$\mathrm{SERVER}\mid\equiv(\mathrm{SD}_j\xleftrightarrow{R_j}\mathrm{SERVER})$

A10：$\mathrm{SD}_j\mid\equiv\mathrm{SERVER}\mid\Rightarrow(\mathrm{SD}_j\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

A11：$\mathrm{SERVER}\mid\equiv\mathrm{SD}_j\mid\Rightarrow(\mathrm{SD}_j\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$

4) 证明过程如下。

S1：由消息 1 可得到 $\mathrm{SD}_j\lhd(\langle P_i,G_1\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}},N_a,T_1)$。

S2：由消息 2 可得到 $\mathrm{SERVER}\lhd(\langle G_2\rangle_{\mathrm{SD}_j\xleftrightarrow{R_j}\mathrm{SERVER}},N_b,T_2,\langle P_i,G_1\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}},N_a,T_1)$。

S3：根据 A5、A9 和 R5，得到 $\mathrm{SERVER}\mid\equiv\mathrm{SD}_j\mid\sim(G_2,N_b,T_2,P_i,G_1,N_a,T_1)$。

S4：根据 A3 和 R4，得到 $\mathrm{SERVER}\mid\equiv\#(G_2,N_b,T_2,P_i,G_1,N_a,T_1)$。

S5：根据 S4 和 A9，推导出 $\mathrm{SERVER}\mid\equiv\mathrm{SD}_j\mid\equiv(\mathrm{SD}_j\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$，即 GOAL6。

S6：根据 S4、S5 和 R2，推导出 $\mathrm{SERVER}\mid\equiv(\mathrm{SD}_j\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$，即 GOAL7。

S7：根据 S4 和 A5，推导出 $\mathrm{SERVER}\mid\equiv\mathrm{SD}_i\mid\equiv(\mathrm{SD}_i\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$，即 GOAL2。

S8：根据 S4、S7 和 R2，推导出 $\mathrm{SERVER}\mid\equiv(\mathrm{SD}_i\xleftrightarrow{\mathrm{SK}}\mathrm{SERVER})$，即 GOAL3。

S9：由消息 3 可得到 $\mathrm{SD}_j\lhd(\langle P_i\text{"},\mathrm{SK}_a,G_4\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}},\langle \mathrm{SK}_b,G_3\rangle_{\mathrm{SD}_j\xleftrightarrow{R_j}\mathrm{SERVER}},T_3)$。

S10：根据 A8 和 R1，得到 $\mathrm{SD}_j\mid\equiv\mathrm{SERVER}\mid\sim(\mathrm{SK}_b,G_3,T_3,\langle P_i\text{"},\mathrm{SK}_a,G_4\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}})$。

S11：根据 A2 和 R4，得到 $\mathrm{SD}_j\mid\equiv\#(\mathrm{SK}_b,G_3,T_3,\langle P_i\text{"},\mathrm{SK}_a,G_4\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}})$。

S12：根据 S10、S11 和 R3，得到 $\mathrm{SD}_j\mid\equiv\mathrm{SERVER}\mid\equiv(\mathrm{SK}_b,G_3,T_3,\langle P_i\text{"},\mathrm{SK}_a,G_4\rangle_{\mathrm{SD}_i\xleftrightarrow{R_i}\mathrm{SERVER}})$

S13：根据 S12 和 A8，推导出 $\mathrm{SD}_j\mid\equiv\mathrm{SERVER}\mid\equiv$

$(\mathrm{SD}_j \xleftrightarrow{\mathrm{SK}} \mathrm{SERVER})$，即 GOAL8。

S14：根据 S12、S3 和 R2，可得 $\mathrm{SD}_j \models (\mathrm{SD}_j \xleftrightarrow{\mathrm{SK}} \mathrm{SERVER})$，即 GOAL5。

S15：由消息 4 可得到 $\mathrm{SD}_i \lhd (\langle P_i'', \mathrm{SK}_a, G_4 \rangle_{\mathrm{SD}_i \xleftrightarrow{R_i} \mathrm{SERVER}}, T_4)$。

S16：根据 A4 和 R1，得到 $\mathrm{SD}_i \models \mathrm{SERVER} \mid\sim (P_i'', \mathrm{SK}_a, G_4)$。

S17：根据 A1 和 R4，得到 $\mathrm{SD}_i \models \#(P_i'', \mathrm{SK}_a, G_4)$。

S18：根据 S16、S17 和 R3，得到 $\mathrm{SD}_i \models \mathrm{SERVER} \models (P_i'', \mathrm{SK}_a, G_4)$。

S19：根据 S18 和 A4，推导出 $\mathrm{SD}_i \models \mathrm{SERVER} \models (\mathrm{SD}_i \xleftrightarrow{\mathrm{SK}} \mathrm{SERVER})$，即 GOAL4。

S20：根据 S18、S19 和 R2，可得 $\mathrm{SD}_i \models (\mathrm{SD}_i \xleftrightarrow{\mathrm{SK}} \mathrm{SERVER})$，即 GOAL1。

4.3 非形式化证明

4.3.1 相互认证性

BACnet/IP-SA 协议中的服务器通过验证 $G_1 = G_1'$ 和 $G_2 = G_2'$ 是否成立来认证 SD_i、SD_j 的身份，SD_j 和 SD_i 通过验证 $G_3 = G_3'$ 和 $G_4 = G_4'$ 来认证服务器的身份，并获取会话密钥 SK_{ab}，表明本文协议实现了相互认证性。

4.3.2 保密性

BACnet/IP-SA 协议中每次运行使用的参数是更新的，香农定理证明，如果 XOR 操作中至少有一项是随机的，则简单 XOR 加密是安全的。对于敌手 A 来说，截获消息的参数每轮都是随机变化的。因此，本文协议具有较强的保密性。

4.3.3 设备匿名性和不可链接性

BACnet/IP-SA 协议不使用设备的真实身份[32]。每一轮都要更换所有的伪身份和服务器与设备 SD_i、SD_j 的会话密钥，使敌手 A 无法通过拦截 M_1 或 M_2 来连接到设备或服务器。因此，本文协议提供了强匿名性和不可链接性。

4.3.4 完善的前向和后向保密

BACnet/IP-SA 协议中的密钥基于随机数、公钥等信息生成，使每次生成的会话密钥之间没有联系。敌手 A 也仅能获得设备与服务器的公钥，但是获得该密钥无法通过验证，即使 A 窃听并记录了多个交互消息，A 也无法计算出任何之前或后续的会话密钥。因此，本文协议满足完全前向和后向安全性。

4.3.5 抗克隆和物理攻击

BACnet/IP-SA 协议中，对设备的改动将影响 PUF 的输出，敌手 A 将无法获得完整的 PUF 激励响应对 $\langle C_j, R_j \rangle$，同时，物理不可克隆函数具有不可复制性，使敌手 A 不能通过侧信道攻击获取内存中的数据，或者篡改相关数据，因此，本文协议能抵抗克隆和物理攻击。

4.3.6 抗重放攻击

BACnet/IP-SA 协议中引入了时间戳 $T_n (n = 1,2,3,\cdots)$，在每次会话初始阶段，设备和服务器都会检查时间戳的有效性，敌手 A 无法通过重放攻击获取目标信息或干扰协议安全运行，协议中的验证值包含多个关键信息的哈希和 XOR 运算，即使重放也无法通过验证，因此，本文协议可抵抗重放攻击。

4.3.7 抗中间人攻击

BACnet/IP-SA 协议在设备和服务器之间进行相互认证，协议中验证码包含多个关键信息的哈希和 XOR 运算，敌手 A 仅凭部分信息无法获得设备或服务器的认证，时间戳可保证敌手不能通过中间人攻击篡改消息，因此，本文协议能抵抗中间人攻击。

4.3.8 抗仿冒攻击

BACnet/IP-SA 协议假设敌手 A 截取设备 SD_i 向 SD_j 发送的消息，然后试图伪装成 SD_i 重新发送仿冒消息，它必须重新计算 ID_i 的伪身份 $P_i = h(\mathrm{PK}_a \| R_i) \oplus \mathrm{ID}_i$ 以及验证信息 $G_1 = h(\mathrm{ID}_i \| P_i \| R_i \| N_a \| \mathrm{PK}_a)$。然而，$P_i$ 和 G_1 中涉及秘密值 ID_i 与 PK_a。由前述匿名性、抗克隆和物理攻击分析可知，敌手不能得到相关信息。类似地，敌手也无法成功冒充 SD_i 和 SERVER。因此，本文协议可以抵抗仿冒攻击。

4.3.9 抗密钥泄露

BACnet/IP-SA 协议中，交互消息传输经过 XOR 加密数据，或通过哈希值加密的验证值。假设敌手 A 获得设备公钥 PK_a、PK_b，并希望模拟设备或服务器中的任何一方来验证另一方。敌手 A 在获得密钥后，虽然能解密密文，但获得的消息不足以计算验证值，也无法知晓设备验证方法。因此，本文协议能够抗密钥泄露攻击。

4.3.10 抗 DoS 攻击

BACnet/IP-SA 协议通信双方在每次会话初始阶段都会检查消息时间戳 $T_n (n = 1,2,3\cdots)$ 的有效性和验证码，如果验证失败，则立即结束协商。阻止

DoS 攻击消耗实体的计算资源[33]。因此，本文协议能够抵抗 DoS 攻击。

4.3.11 抗去同步攻击

BACnet/IP-SA 协议中设备和服务器包含共享的秘密参数，这些参数每次都会发生变化。因此，去同步攻击是协议考虑抵抗的主要攻击之一[34]。假设敌手 A 通过截获等方式获得设备的伪身份，就有可能将伪身份与设备的真实身份联系起来。然而，协议中的服务器和设备保留当前和前几轮的先前参数，这些参数在被请求时都是可以接受的。如果设备使用一个已过时的参数不止一次，服务器将记录这一点，并向系统发出警报[35]。因此本文协议能抵抗去同步攻击。

4.3.12 抗侧信道攻击

BACnet/IP-SA 协议为实现抗侧信道攻击，从多方面做了预防[36]。在每轮会话中服务器都会随机生成激励使设备生成新的响应用于当前轮的会话，尽管侧信道攻击会通过揭示 PUF 的内部参数预测响应，但也很难起作用，因为即使已经学习了旁路信息或内部参数，响应也可能仍然未知。同时，对于生成的验证值、密钥等关键信息，协议增加了随机数作为噪声以模糊侧信道信息，这些噪声也是随机生成的。通过综合的策略，本文协议能够抵抗侧信道攻击。

5 安全与性能对比

本节从安全性、计算开销和通信开销 3 个方面对改进后 BACnet/IP-SA 协议身份认证方案进行分析，并与文献[12]方案和文献[13]方案进行比较。其中，文献[12]通过改变密钥分发方式，引入随机数来保证密钥的安全性；文献[13]利用时间戳和随机数来增强设备间会话的安全性。

5.1 安全性对比

本节对比了各方案的安全性，如表 8 所示。其中，“√”表示某方案具有所述的安全性；“×”表示某方案没有所述的安全性。结果表明，本文方案具有强匿名性、抗仿冒攻击、抗克隆攻击和抗密钥泄露等原方案、文献[12]和文献[13]所不具有的能力，这表明本文方案具有更高的安全性。

表 8 各方案的安全性对比

方案	相互认证性	匿名性	前、后向保密性	抗克隆攻击	抗重放攻击	抗中间人攻击	抗仿冒攻击	抗密钥泄露攻击	抗 DoS 攻击	抗去同步攻击	抗侧信道攻击
文献[12]方案	√	×	×	×	√	√	×	×	√	×	×
文献[13]方案	√	×	√	×	√	√	√	×	√	×	×
本文方案	√	√	√	√	√	√	√	√	√	√	√

5.2 计算开销对比

为统一计算开销评判标准，本文参考文献[21]中的统计结果，使用基于 ARM Cortex-A9 MPCore 890 MHz CPU、Android 5.1 系统、4 GB RAM 的设备模拟资源受限设备，同时使用基于 Intel Core i5-4300 2.9 GHz CPU、Ubuntu 12.04 系统、16 GB RAM 的设备模拟非资源受限设备，使用 JPBC 库计算上述方案中密码运算的执行时间，如表 9 所示。本文只考虑密集的计算，并将重点放在每个协议运行时的认证和密钥建立阶段[37]。

表 9 密码运算的执行时间

符号	描述	执行时间/ms	
		资源受限设备	非资源受限设备
T_{h}	Hash 函数	0.018	0.011
$T_{\mathrm{e/d}}$	对称加/解密	0.079	0.041
T_{PUF}	PUF	0.12	—

各方案计算开销对比如表 10 所示。结果表明，本文方案的时间成本是最低的，本文 BACnet/IP-SA 协议比原方案的计算开销降低了 21.59%。由于文献[12]和文献[13]的协议使用多次对称加解密运算，本文方案使用多次 Hash 运算和 PUF 运算，计算开销比文献[12]方案和文献[13]方案分别降低了 21.59%和 51.31%。

5.3 通信开销对比

通信开销是指参与者在完成认证过程时交换或传输的数据量。本文统一做出如下假设：随机数、身份标识、PUF 响应以及时间戳长度为 160 bit，加解密以及哈希函数的输出为 256 bit。各方案中 SD_j（需求端）、SERVER（网关端）和 SD_i（供给端）所需的通信开销对比如表 11 所示。其中，原方案、文献[12]方案和文献[13]方案主要使用了多次对称加解密运算，未使用 Hash 运算，本文方案使用了多次 Hash 运算和两次 PUF 运算，使通信开销略高。

表 10　　**各方案计算开销对比**

算，并计算开销/ms	计算开销/ms			
	SD_i	SERVER	SD_j	总计
本文方案	$4T_h + T_{PUF} \approx 0.192$	$9T_h \approx 0.099$	$4T_h + T_{PUF} \approx 0.192$	0.483
原方案	$4T_{e/d} \approx 0.316$	$4T_{e/d} \approx 0.164$	$4T_{e/d} \approx 0.316$	0.616
文献[12]方案	$4T_{e/d} \approx 0.316$	$4T_{e/d} \approx 0.164$	$4T_{e/d} \approx 0.316$	0.616
文献[13]方案	$7T_{e/d} \approx 0.553$	$3T_{e/d} \approx 0.123$	$4T_{e/d} \approx 0.316$	0.992

表 11　　**各方案通信开销对比**

方案	通信开销/bit			
	SD_i	SERVER	SD_j	总计
本文方案	1 568	2 656	4 480	8 704
原方案	1 980	2 976	1 824	6 780
文献[12]方案	4 192	2 208	1 984	8 384
文献[13]方案	2 784	2 944	2 144	7 872

结果表明，本文的 BACnet/IP-SA 协议比原方案的通信开销增加了 28.37%，这是由于本文方案为增强原方案的安全性而加入了多种验证信息。与文献[12]方案和文献[13]方案相比，本文方案通信开销分别增加了 3.81%和 10.56%，通信开销差距较小，不会增加设备通信负担，也不会提高设备运行性能需求。BACnet/IP-SA 协议在保证通信开销几乎不变的情况下增强了设备的安全属性。

6　结束语

本文使用 CPN 理论分析了楼宇自控系统中 BACnet 内部设备、外部设备和服务器之间的身份认证和会话密钥交换问题。研究表明，BACnet/IP 容易受到仿冒、重放、篡改、密钥泄露、侧信道攻击等一些常见攻击。针对 BACnet/IP 内部设备、外部设备和服务器之间的身份认证安全问题，本文提出了一种轻量级身份认证密钥交换方案 BACnet/IP-SA，该方案使用 PUF“激励−响应对”作为验证设备身份的方式，并且使用设备伪身份来保证通信的匿名性。本文对 BACnet/IP 采用 BAN 逻辑证明和 CPN 建模进行了形式化和非形式化分析，结果表明，该协议能够抵御重放、中间人、仿冒、密钥泄露、DoS、侧信道攻击，具有更好的安全性。通过与最近的相关研究工作比较表明，本文方案的计算开销与原方案、文献[12]方案和文献[13]方案的计算开销相比，分别降低了 21.59%、21.59%和 51.31%，但通信开销比文献[12]方案和文献[13]方案的略高，如何在安全增强、计算开销较小的前提下降低协议的通信开销将是下一步研究工作的重点。

参考文献：

[1] FAURI D, KAPSALAKIS M, SANTOS D R D, et al. Leveraging semantics for actionable intrusion detection in building automation systems[C]//International Conference on Critical Information Infrastructures Security. Berlin: Springer, 2019: 113-125.

[2] CASH M, WANG S, PEARSON B, et al. On automating BACnet device discovery and property identification[C]//Proceedings of the IEEE International Conference on Communications. Piscataway: IEEE Press, 2021: 1-6.

[3] 方栋梁, 刘圃卓, 秦川, 等. 工业控制系统协议安全综述[J]. 计算机研究与发展, 2022, 59(5): 978-993.
FANG D L, LIU P Z, QIN C, et al. Survey of protocol security of industrial control system[J]. Journal of Computer Research and Development, 2022, 59(5): 978-993.

[4] 杨婷, 张嘉元, 黄在起, 等. 工业控制系统安全综述[J]. 计算机研究与发展, 2022, 59(5): 1035-1053.
YANG T, ZHANG J Y, HUANG Z Q, et al. Survey of industrial control systems security[J]. Journal of Computer Research and Development, 2022, 59(5): 1035-1053.

[5] 董春桥. 智能楼宇 BACnet 原理与应用[M]. 北京: 电子工业出版社, 2003.
DONG C Q. Intelligent building BACnet principles and applications[M]. Beijing: Publishing House of Electronics Industry, 2003.

[6] 张少军. BACnet 标准与楼宇自控系统技术[M]. 北京: 机械工业出版社, 2012.
ZHANG S J. BACnet standard and building automation system technology[M]. Beijing: China Machine Press, 2012.

[7] NAST M, BUTZIN B, GOLATOWSKI F, et al. Performance analysis of a secured BACnet/IP network[C]//Proceedings of the 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS). Piscataway: IEEE Press, 2019: 1-8.

[8] HONG S H, LEE S J. Design and implementation of fault tolerance in the BACnet/IP protocol[J]. IEEE Transactions on Industrial Electronics, 2010, 57(11): 3631-3638.

[9] PAN Z W, HARIRI S, PACHECO J. Context aware intrusion detection

for building automation systems[J]. Computers & Security, 2019, 85: 181-201.

[10] MERZ H, HANSEMANN T, HÜBNER C. BACnet[M]. Berlin: Springer, 2009.

[11] 冯涛, 鲁晔, 方君丽. 工业以太网协议脆弱性与安全防护技术综述[J]. 通信学报, 2017, 38(S2): 185-196.
FENG T, LU Y, FANG J L. Summary of vulnerability and security protection technology of industrial Ethernet protocol[J]. Journal on Communications, 2017, 38(S2): 185-196.

[12] FENG T, JIANG X Y, FANG J L, et al. A new scheme of BACnet protocol based on HCPN security evaluation method[J]. International Journal of Network Security, 2022, 24(6): 1064-1075.

[13] FENG T, ZHAO S M, GONG X. Formal security evaluation and improvement of BACnet/IP protocol based on HCPN model[J]. International Journal of Network Security, 2022, 24(2): 193-205.

[14] FENG T, WU Y. Formal security analysis and improvement based on LonTalk authentication protocol[J]. Security and Communication Networks, 2022, 2022: 1-19.

[15] JIANG Q, ZHANG N, NI J B, et al. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(9): 9390-9401.

[16] WANG D, WANG P. Two birds with one stone: two-factor authentication with security beyond conventional bound[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(4): 708-722.

[17] 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.

[18] GAO J, ZHUANG W H, LI M S, et al. MAC for machine-type communications in industrial IoT—part I: protocol design and analysis[J]. IEEE Internet of Things Journal, 2021, 8(12): 9945-9957.

[19] KAUR J, TONEJC J, WENDZEL S, et al. Securing BACnet's pitfalls[C]//IFIP International Information Security and Privacy Conference. Berlin: Springer, 2015: 616-629.

[20] 马瑞洁. 基于着色 Petri 网的安全协议形式化分析理论与技术研究[D]. 西安: 西安电子科技大学, 2018.
MA R J. On the formal description and analysis of security protocols using colored petri nets[D]. Xi'an: Xidian University, 2018.

[21] GOPE P, SIKDAR B. An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication[J]. IEEE Transactions on Smart Grid, 2019, 10(6): 6607-6618.

[22] WU D H, LIU J T, WANG H W, et al. A CPN-based approach for studying impacts of communication delays on safety and availability of safety-critical distributed networked control systems[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3033-3042.

[23] MCGOWAN M K. Addressing the cybersecurity threat[J]. Ashrae Journal, 2019, 61(7).

[24] YU Y L, PENG W Y, LU J F. Wireless network security game based on conditional privacy policy[J]. Computer Communications, 2022, 184: 96-106.

[25] 肖美华. 安全协议形式化分析与验证[M]. 北京: 科学出版社, 2019.
XIAO M H. Formal analysis and validation of security protocols[M]. Beijing: Science Press, 2019.

[26] PITTALIA P P. A comparative study of Hash algorithms in cryptography[J]. International Journal of Computer Science and Mobile Computing, 2019, 8(6): 147-152.

[27] 王圣宝, 周鑫, 文康, 等. 适用于智能电网的三方认证密钥交换协议[J]. 通信学报, 2023, 44(2): 210-218.
WANG S B, ZHOU X, WEN K, et al. Tripartite authenticated key exchange protocol for smart grid[J]. Journal on Communications, 2023, 44(2): 210-218.

[28] SHAMSOSHOARA A, KORENDA A, AFGHAH F, et al. A survey on physical unclonable function (PUF)-based security solutions for Internet of things[J]. Computer Networks, 2020, 183: 107593.

[29] GONG X, FENG T, ALBETTAR M. PEASE: a PUF-based efficient authentication and session establishment protocol for machine-to-machine communication in industrial IoT[J]. Electronics, 2022, 11(23): 3920.

[30] MODARRES A M A, SARBISHAEI G. An improved lightweight two-factor authentication protocol for IoT applications[J]. IEEE Transactions on Industrial Informatics, 2023, 19(5): 6588-6598.

[31] MILLWOOD O, MISKELLY J, YANG B H, et al. PUF-phenotype: a robust and noise-resilient approach to aid group-based authentication with DRAM-PUFs using machine learning[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2451-2465.

[32] 王振宇, 郭阳, 李少青, 等. 面向轻量级物联网设备的高效匿名身份认证协议设计[J]. 通信学报, 2022, 43(7): 49-61.
WANG Z Y, GUO Y, LI S Q, et al. Design of efficient anonymous identity authentication protocol for lightweight IoT devices[J]. Journal on Communications, 2022, 43(7): 49-61.

[33] CETINKAYA A, ISHII H, HAYAKAWA T. An overview on denial-of-service attacks in control systems: attack models and security analyses[J]. Entropy, 2019, 21(2): 210.

[34] 王菲菲, 汪定. 基于雾计算的智能医疗三方认证与密钥协商协议[J]. 软件学报, 2023, 34(7): 3272-3291.
WANG F F, WANG D. Fog computing-based three-party authentication and key agreement protocol for smart healthcare[J]. Journal of Software, 2023, 34(7): 3272-3291.

[35] WANG D, WANG N, WANG P, et al. Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity[J]. Information Sciences, 2015, 321: 162-178.

[36] WANG Q X, WANG D. Understanding failures in security proofs of multi-factor authentication for mobile devices[J]. IEEE Transactions on Information Forensics and Security, 2022, 18: 597-612.

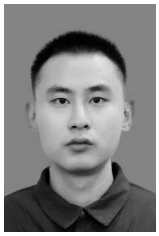
[37] GOPE P, MILLWOOD O, SIKDAR B. A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for Internet of medical things[J]. IEEE Transactions on Industrial Informatics, 2022, 18(3): 1971-1980.

[作者简介]

谢鹏寿（1972− ），男，甘肃清水人，兰州理工大学教授、硕士生导师，主要研究方向为隐私保护、车联网安全、工业互联网安全等。

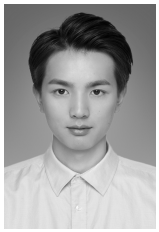
冯涛（1970− ），男，甘肃临洮人，博士，兰州理工大学研究员、博士生导师，主要研究方向为网络与信息安全、区块链、工业互联网安全等。

朱家锋（1997− ），男，甘肃兰州人，兰州理工大学硕士生，主要研究方向为网络与信息安全、工业互联网安全。



李威（1998− ），男，河南周口人，兰州理工大学硕士生，主要研究方向为网络与信息安全、工业互联网安全。

康永平（1970− ），女，甘肃永登人，兰州理工大学副教授，主要研究方向为生产设备故障诊断、工业互联网安全等。



冉玉翔（1999− ），男，甘肃金昌人，兰州理工大学硕士生，主要研究方向为网络与信息安全、访问控制。