基于 CPN 的安全协议形式化建模及安全分析方法

龚翔，冯涛，杜谨泽
（兰州理工大学计算机与通信学院，甘肃 兰州 730050）

摘 要：为了解决有色 Petri 网（CPN）对安全协议进行形式化建模分析时，仅能判断协议是否存在漏洞而无法找出漏洞具体位置和攻击路径的问题，以及 CPN 建模时随着攻击者模型引入，安全协议的形式化模型可能的消息路径数量激增，状态空间容易发生爆炸导致难以提取准确攻击路径的问题，改进了基于 CPN 的安全协议形式化建模方法，验证并提取攻击路径的同时，采用更细粒度的协议建模及控制。在状态空间收敛方面提出了 CPN 模型不同进程在各分层模型中等待−同步的方法控制状态空间规模。通过针对 TMN 协议的安全评估分析，成功提取出该协议 25 条攻击路径，评估了该协议安全性的同时证明了所述方法的有效性。

关键词：有色 Petri 网；安全协议；形式化分析；状态空间；攻击路径
中图分类号：TP393.06
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021175

Formal modeling and security analysis method of security protocol based on CPN

GONG Xiang, FENG Tao, DU Jinze
School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Abstract: To solve the problem of modeling and analyzing with colored Petri net (CPN), which was determining vulnerabilities in hole location but couldn't identify any attack path, and the problem of when the introduction of the attacker model, the number of possible message paths in the CPN formal model of security protocol surges the state space prone to explosion, which made it difficult to extract accurate attack paths, the formal modeling method of security protocol was improved base on CPN, the attack paths were verified and extracted, further the fine-grained protocol modeling and control were adopted. As well as in the aspect of state-space convergence, and a waiting-sync method for different processes of CPN model in each hierarchy model was proposed, which effectively controlled the state-space scale of the model. Through the security evaluation and analysis of TMN protocol, 25 attack paths of the protocol are extracted successfully, the security of the protocol is evaluated, and the effectiveness of the proposed method is proved.

Keywords: colored Petri net, security protocol, formal analysis, state space, attack path

1 引言

安全协议已成为现代计算机网络正常运转的基础，但由于其设计阶段的规范缺失和不可避免的逻辑缺陷，常会带来潜在的安全隐患，使各种协议的开发和安全性验证成为一项艰巨的任务[1]。

安全协议的形式化分析一直是网络安全领域的研究热点[2-6]。丹麦奥尔胡斯大学开发的有色 Petri 网（CPN, colored Petri net）工具软件 CPN-Tools，不仅实现了计算机上的 CPN 可视化建模，还提供了全部状态空间的自动计算以及生成状态空间报告的功能，集成的 SML（standard meta language）

收稿日期：2021−01−04；**修回日期**：2021−04−03
基金项目：国家自然科学基金资助项目（No. 62162039, No. 61762060）；甘肃省高等学校科研基金资助项目（No.2017C-05）；甘肃省科技厅重点研发计划基金资助项目（No.20YF3GA016）
Foundation Items: The National Natural Science Foundation of China (No.62162039, No.61762060), Educational Commission of Gansu Province (No.2017C-05), Foundation for the Key Research and Development Program of Gansu Province (No.20YF3GA016)

可以辅助完成各种安全协议的功能评价和状态路径搜索。

按照安全协议分析的目的，现有的 CPN 协议分析目标可分为三类。第一类是对协议本身进行建模，按照状态空间报告所提供的各种属性（活性、公平性等）来判断协议的设计是否正确，验证协议的正确性[7-8]。第二类是在协议建模的基础上引入攻击者模型，构建恰当合理的安全评估模型以快速找到协议中存在的潜在威胁[9-10]。第三类在第二类的基础上更进一步，提出协议改进方案并且利用安全评估模型验证，分析改进结果[11-13]。本文着重研究通过 CPN 对安全协议进行分析验证的方法，并通过实例说明该方法的有效性。

然而，由于没有统一标准，利用 CPN 针对协议安全分析的方法是多种多样的[14]。近年来，有较多文献提供了不同解决方案，存在的主要问题如下。

1) 部分文献中采用了正确性验证方法验证安全协议漏洞，在引入攻击者模型后，通过建立模型的关联矩阵，用线性代数的方法判定方程是否存在解，如果有解则认为某序列可达[15-16]；利用 CPN-Tools 中计算树逻辑库 ASKCTL 提供的公式验证模型某属性是否正确[10]；利用 CPN-Tools 计算模型状态空间之后，以死变迁、死节点的数量变化来说明安全性[11,13,17-18]。但是，这些方法只能判断协议模型是否存在安全漏洞，无法给出具体漏洞存在的位置或攻击路径。

2) CPN 对于建模人员的经验要求较高，主要难点聚焦在模型状态空间爆炸问题上[11-12,19-20]。大多数文献没有提出控制状态空间规模的有效方法。甚至部分研究者认为，CPN 建模的复杂度增大一定会使状态空间不可控甚至趋于爆炸[11,19]。如何将模型的状态空间维持在一个恰当范围是具有挑战的问题。文献[21]提出了一种使用抑制弧来减少状态空间的方法，该方法虽然可以减少状态空间的节点数，但避开了模型中的特殊节点，当模型足够大时，仍然存在状态空间爆炸的可能。

3) 针对攻击路径的提取，文献给出了以下 2 种方法。一种方法是在得到模型状态空间后，利用安全属性违背条件确定要找的死状态节点（以下简称死节点），再通过状态空间搜索到达死节点途经的全部节点[22]。然而，节点中包括除目标属性外的所有库所状态，逐一筛选库所状态导致过程极其烦琐，利用这种方法通常仅能找出模型个别攻击路径，难以实现完整的自动搜索。另一种方法是基于 on-the-fly[20]的方法，当生成状态空间时，同时计算状态的攻击路径，并存储在状态节点中[11,19]。路径计算与状态空间计算同时发生。在得到整个状态空间并找到攻击后，可以立即从状态中提取所有的攻击路径。

本文针对上述问题提出解决思路，主要贡献如下：改进了利用 CPN 进行协议安全性分析的一般方法，以找到协议漏洞并提取攻击路径为目标，采用更细粒度的建模及控制方法。攻击路径的提取中，将 on-the-fly 方法应用为多参数形式，配合 SML 代码，得到清晰的结果。提出基于 HCPN（hierarchical CPN）的并行令牌在层次间的等待–同步行进（Line-Up）建模思想，并行的多令牌同时进出不同分层，消除了大量无用的状态序列，控制了状态空间规模，提高了并行处理的效率。本文提出的 CPN 模型复杂度的增加不一定会增大状态空间规模，评估实验证明甚至可以通过增加模型复杂度的方法来减小状态空间规模。该研究为未来的 CPN 安全协议分析工作建立蓝本。

评估实验方面，本文针对 TMN（Tatebayashi, Matsuzaki, Newman）协议进行了安全性分析。此前已有较多针对 TMN 协议安全性分析的研究，该协议包含的大量漏洞已在部分文献中提出[19-20,23]。本文主要以 TMN 协议为例说明所提方法的有效性。

2　背景知识

2.1　协议安全形式化分析

形式化分析方法是指采用数学或逻辑方法描述系统模型，通过一定形式的推理验证系统是否满足要求的方法。将形式化分析的方法用于安全协议验证最早是由 Needham 和 Schroeder 提出的，后由 Dolev 和 Yao 具体采用并于 1983 年发表了重要成果[23]。此后，大量的安全协议形式化分析工具被开发，出现了许多可用于协议形式化分析的方法，例如早期的 BAN 逻辑、串空间、状态机等，这些方法的形式化验证聚焦在定理证明上，没有针对形式语义的分析工具。近年来，较强大的分析工具如 ProVerif、Scyther、Tamarin Prover 等逐渐流行起来，它们可以针对协议进行形式化安全验证及语义分析。CPN 与状态机类似，但因其状态空间分析能力强大且通俗易懂，使其同样成为主流的协议建模分析工具，在诸多领域被广泛使用。

2.2 CPN 协议安全性形式化分析

CPN 是在原始 Petri 网的基础上拓展而来的，属于高级 Petri 网范畴。与原始 Petri 网相比，CPN 的优势是其标记可以通过着色来代表多重含义，库所类型可以定义为颜色集，而非单一数据；令牌可以是颜色集类型元素的多集，大大提高了 Petri 网的数据表达能力。

CPN 的优点是建模过程比较灵活，自由度较高；借助 CPN-Tools 能够动态仿真模型，可视化界面允许用户观察模型每一步的执行过程，进行细粒度分析；模型较为直观，没有 CPN 知识的观察者也可以通过演示快速理解模型所表达的含义。而其缺点是高自由度使建模过程较为复杂，与现有其他自动协议安全验证工具相比，CPN 建模人员需要更多安全协议的建模分析经验。

CPN 与目前流行的几种自动协议安全性验证工具对比如下。ProVerif 声称可以计算多条攻击路径，是基于逻辑编程的方法。但它计算的攻击路径是受限的，多数情况下只能包含一条攻击路径[20]。ProVerif 计算的受限攻击路径集远小于基于 CPN 的方法提取的攻击路径集。

Scyther 是一种高性能的协议模型验证工具，能提供多条攻击路径的计算及分析功能。但它所使用的算法是千篇一律的，对于所有的安全协议，Scyther 试图用同一方法给出状态空间分析，这样确实可以找到部分攻击路径，但无法做到全面或根据不同协议有的放矢。

Tamarin Prover 能够穷尽搜索状态空间，最新的版本中加入了对异或运算的模拟支持。但该工具要求建模者与观察者都有较高的专业知识，相对 CPN 来说不够简单直观。同时，它也存在 Scyther 中用同一方法应对所有被测协议，使攻击路径被片面计算的弊端。

因此，上述或同类自动验证工具不需建模者研究其内部运行机制，写出规定格式的脚本即可完成验证工作。而 CPN 建模过程的高自由度成为其优势之一，状态空间完全由建模者自行把控，能够针对不同协议实现专属的建模及分析方法。这也是 CPN 协议验证往往比自动协议验证工具更有效的原因。

2.3 TMN 协议

TMN 协议是一种用于数字移动通信系统的安全密钥交换协议。TMN 协议规定发起者与响应者之间可借助可信服务器交换密钥。该协议发布至今已被证明有诸多安全隐患[24]，常被用作验证形式化工具和方法的有效性[19-20]。

TMN 协议的工作过程如下。

M_1: A → J: (B, $\{K_{aj}\}K_{JP}$), A

M_2: J → B: A

M_3: B → J : (A, $\{K_{ab}\}K_{JP}$), B

M_4: J → A : (B, $\{K_{ab}\}K_{aj}$)

其中，A 为发起者，B 为响应者，J 为服务器，K_{aj} 为 A 向 J 发起请求时生成的新鲜随机数（也称为 A 与 J 的临时密钥），K_{JP} 为服务器 J 的公开密钥，K_{ab} 为 B 收到请求后生成的用于与 A 通信的新鲜随机数（会话密钥），M_1～M_4 为 TMN 协议运行的 4 个步骤。

2.4 Dolev-Yao 攻击者模型

Dolev-Yao 攻击者模型[23]包含 2 种假设，首先，假设密码系统是“完美的”，安全协议的一次执行序列是严格按照协议规范定义的消息步骤交替序列。其次，攻击者具有比协议真实参与者更强大的计算能力，能够窃听、截获、篡改和重放协议运行过程中真实实体间交换的消息，也能加解密、拆分和组合原始消息，伪造消息内容。Dolev 和 Yao 的方法被概括为黑盒安全分析。

然而，Dolev-Yao 攻击者模型在引入形式化分析方法时，由于其定义的攻击者模型能力强大，能够根据其截获的消息拆分组合出任意消息，导致增加了许多无用的重复操作，使状态空间规模发生爆炸。为此，在建立协议评估模型时需要对消息的合成进行进一步假设和约束，具体如下。

1) 通过公共信道交换所有消息，攻击者可以窃听到网络中的任何消息。

2) 攻击者了解目标安全协议的全部细节，能够按规则拆分消息内容。

3) 攻击者可以存储截获的或自身产生的消息。

4) 攻击者可以根据记录的消息伪造并发送消息。伪造消息是按协议规则合成的。

5) 如果得到了匹配的密钥，攻击者可以将密文解密。

6) 攻击者能够作为合法实体之一，与其他实体进行正常通信。

3 基于攻击者的 TMN 协议安全评估模型

3.1 基于攻击者的协议形式化描述

在 CPN-Tools 中将协议消息定义为 product 类

型，消息集 PACKET 定义为 union 类型，各步骤消息从属于 PACKET 消息集。函数 keyPair 用于模拟验证服务器公私钥的匹配情况。

根据 2.4 节的攻击者能力假设，协议评估模型建模时加入攻击者实体，且攻击者参与每一次数据传输过程，原协议的 4 个步骤被攻击者分割为 8 个步骤（如图 1 所示）。模型规模庞大，将其进行分层（Hierarchical）处理。

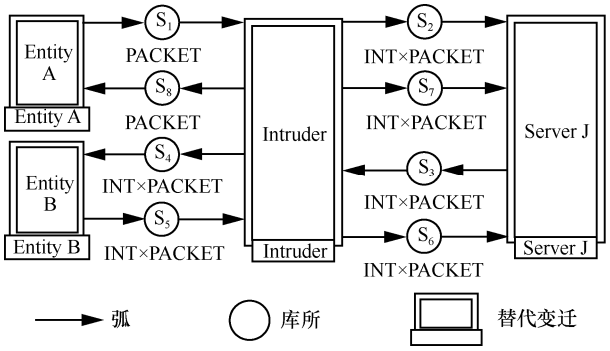

图 1　基于攻击者的 TMN 协议顶层 CPN 模型

图 1 中，Entity A 和 Entity B 分别代表实体 A 和 B，Server J 代表服务器 J，Intruder 代表攻击者（简称 IN），S_1～S_8 代表分割后各步骤中的网络信道接口。在实体 A 和 B 角色不变的情况下，攻击者既可以扮演协议发起者的角色，也可以扮演协议响应者的角色。

此外，攻击者的加入使模型中出现了多个可能的发起者和响应者，各个实体及服务器需加入处理并发会话的能力。Clark-Jacob 库中的安全协议已被证明最多涉及 2 次并发会话攻击[19]。在不影响协议验证结果的基础上，为减少状态空间数量，约定模型中协议并发最多运行 2 次，且实体 A 和 B 最多参与一次协议运行，攻击者最多可参与 2 次。为便于描述，下文将第一次协议运行称为进程 1，第二次运行称为进程 2。

并发顺序方面，攻击策略可归纳为 2 种情况，具体表示为

情况 1　$M_1, M_1', M_2', M_2, M_3, M_3', M_4', M_4$

情况 2　$M_1, M_2, M_3, M_4, M_1', M_2', M_3', M_4'$

其中，M_1'～M_4'为攻击者参与步骤。情况 1 中攻击者一旦接收到 A 发起会话的消息，立即存入知识库并转发，同时组装攻击数据发起一个新的消息，称为中间人（MitM, man in the middle）攻击。情况 2 中攻击者将窃听的一次完整协议运行全部存入知识库，之后试图伪装身份发起攻击会话，称为顺序攻击（SqA, sequence attack）。

因此，基于攻击者的协议消息步骤分层也必须能够处理二次并发过程，进程间不能产生错乱。

攻击者引入后的替代变迁 Intruder 的第二层 CPN 模型如图 2 所示。该模型由替代变迁 M_1～M_4 分别模拟协议运行 4 个步骤中的各阶段攻击行为。

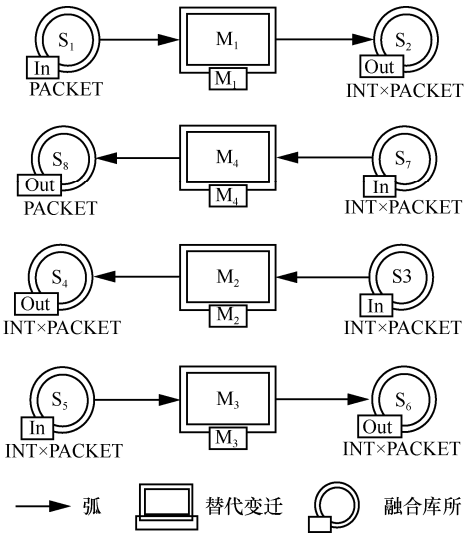

图 2　替代变迁 Intruder 的第二层 CPN 模型

3.2　TMN 协议 CPN 底层形式化描述

本节根据建模假设，给出加入攻击者后的 TMN 协议模型。模型所有层次中使用了多个融合库所，融合库所由库所和 Fusion ID 组成，相同 Fusion ID 的融合库所名称不同但可视为同一库所。多个融合库所出现在不同分层中。

实体 A 底层 CPN 模型如图 3 所示。实体 A 发送时，A_Encry_Pack 变迁作为模型运行起点，由自身存储的数据集中收集协议第一步消息 m_1 所需数据，加密后发送，包括自身 ID、接收方 ID、生成的临时密钥 Kaj，以及服务器公钥 KJP。此时由于攻击者也是可通信实体之一，因此 A 每次发起会话时可选择与 B 或是 IN 进行通信。接收时，A_Decry_Pack 变迁是模型运行的最后一步，将接收的数据包解密并验证，类型及 ID 正确的情况下将会话密钥存储至 Session_Key 库所，密钥交换成功。

实体 B 底层 CPN 模型如图 4 所示。实体 B 从 S_4 处接收 J 发来的第二步消息 m_2。Recv 库所接收后触发 B_Encry_Pack 变迁组装第三步消息 m_3，并由 S_5 发送给 J。带有 INT×前缀的库所是为应对并发时状态激增问题，加入进程序号的库所类型。

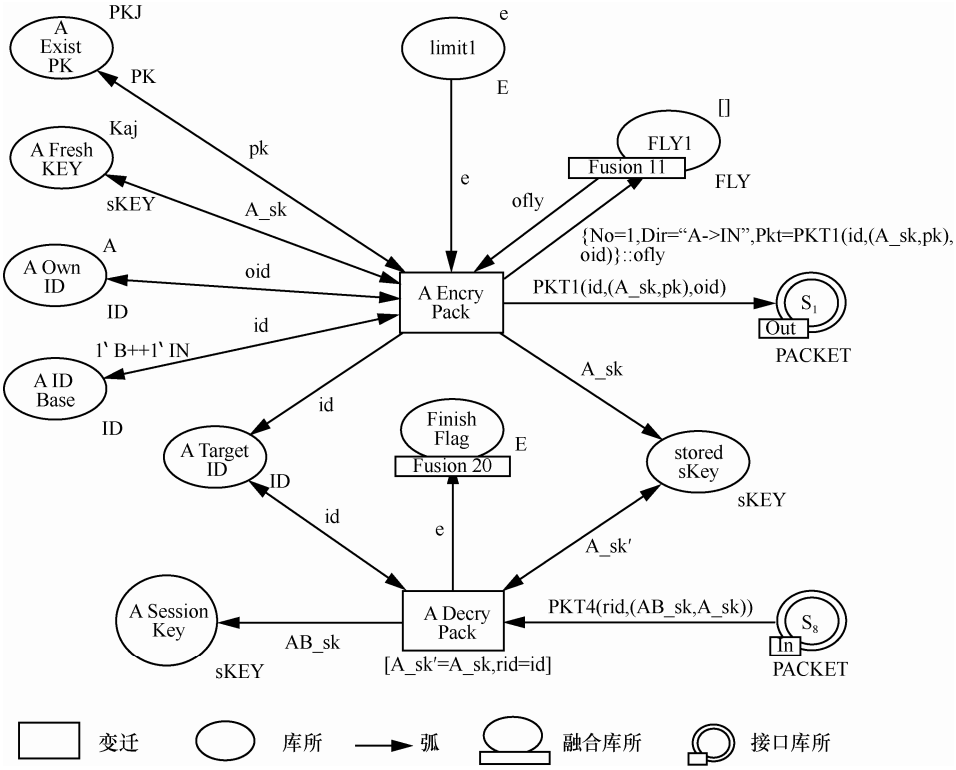

图 3　实体 A 底层 CPN 模型

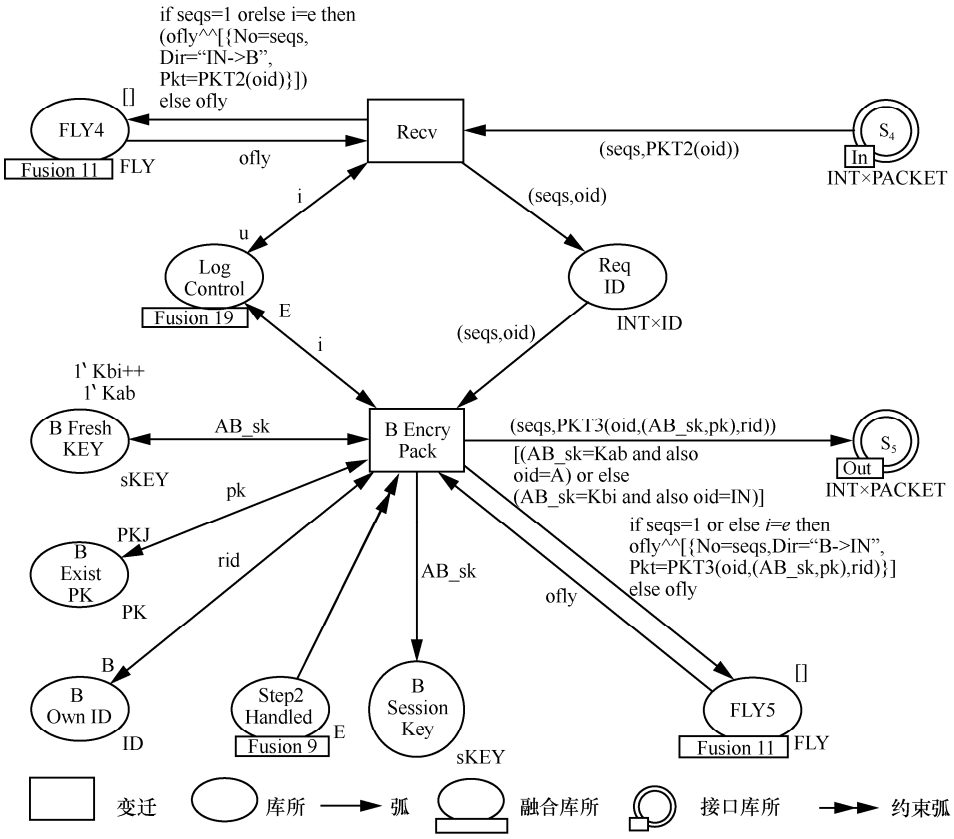

图 4　实体 B 底层 CPN 模型

服务器 J 底层 CPN 模型如图 5 所示。服务器由 S_2 接收 A 发来的消息 m_1，经 Decry_Unpack1 变迁解密拆分验证并存储后生成 m_2 消息，并由 S_3 发送给 B。此外，J 从 S_6 接收 m_3 消息，经 Decry_Unpack2 变迁解密、拆分、验证并存储后处理，再由 J_Encry_Pack 组装生成第四步消息 m_4 交由 S_7 发送给 A。

3.3　TMN 协议安全评估模型

根据 TMN 协议步骤 M_1～M_4 分别描述 TMN 协议安全评估模型，这些模型分别称为基于攻击者的 TMN 协议安全评估模型 H_{M_1}～H_{M_4}。

基于攻击者的 TMN 协议安全评估模型 H_{M_1} 如图 6 所示，其主要功能是选定一种攻击模式，将 A 发来的消息拆分、记录并转发，按不同攻击模式在不同的时机生成攻击消息后发送至目标网络接口，具体如下。S_1 接收消息 m_1 后，$Transmit_1$ 变迁从库所 Attk_Mode 中随机选择攻击模式 MitM 或 SqA，选定的攻击模式存入 Attk_Conf 库所。接收的消息存入 $Buffer_1$ 库所，标志计数器 Seq_No'令牌值为 1 时，令牌被消耗并点火 DIR_Send 变迁，该变迁将 m_1 消息拆分成目标 ID 和密文两部分，分别存储至融合库所 DEST_ID_In'和 Cipher_Base，同时将 m_1 交给库所 $Sender_1$，使变迁 $Transmit_1$'点火，计数器 Seq_No 值变为 2，此时模型运行出现以下分支情况。

1) 如果 Attk_Conf 的值为 SqA，则 m_1 被发送至 S_2，Seqs_Lock 库所不获得令牌。监听到实体 A 获得会话密钥后，SqA_Att_Trigger 变迁点火，Chosen 库所获得令牌，随机选择 IN_Pack_1 或者 Remake 库所点火，IN_Pack_1 变迁随机取出知识库

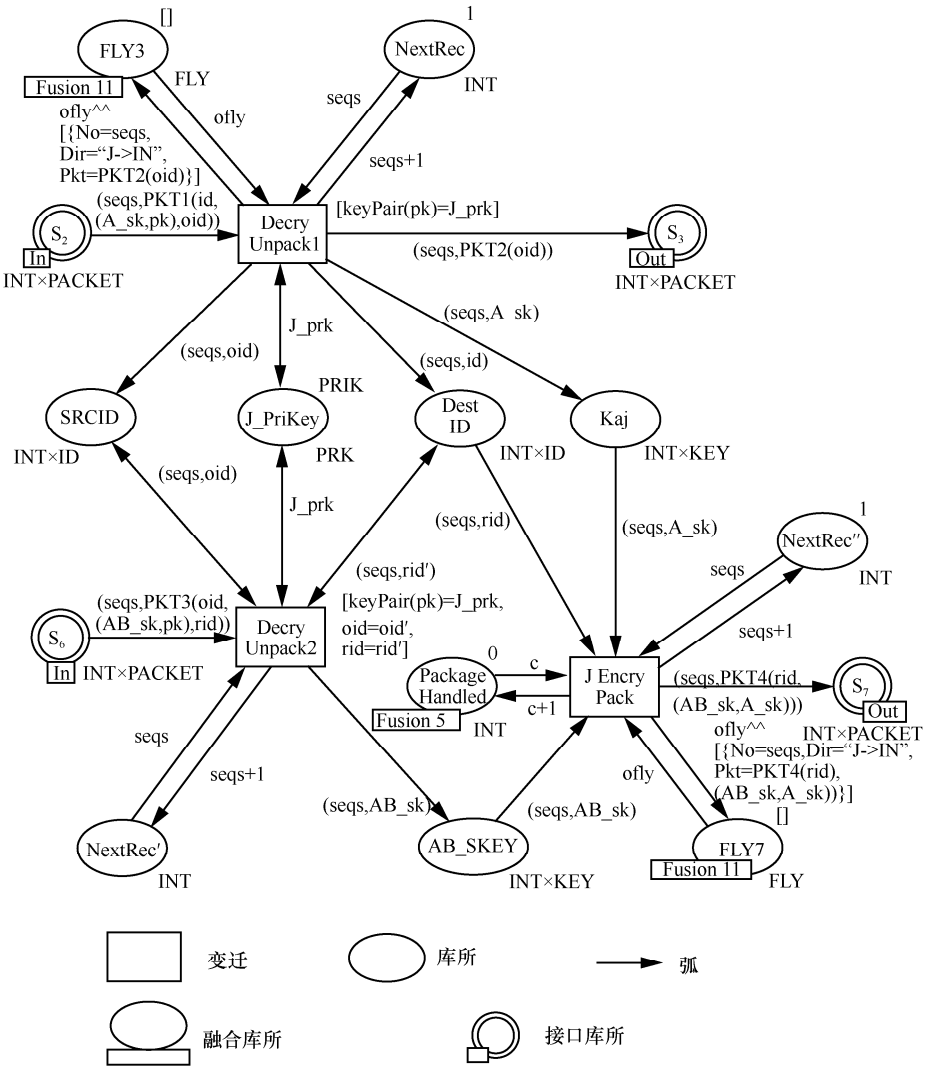

图 5　服务器 J 底层 CPN 模型

中累积的原始数据，包括未解密的密文，按规则合成攻击消息 m_1'（上角标'代表有攻击者参与的消息）后发至 $Sender_1$。而 Remake 变迁则不通过知识库，以合法实体身份，用自己生成的密钥按规则生成消息 m_1'后发至 $Sender_1$。由 $Transmit_1$'发送 m_1'至 S_2。

2) 如果 Attk_Conf 的值为 MitM，则 m_1 进入 Line-Up 库所 Queue1 等待，Seqs_Lock 库所得到令牌，$Unpack_1$ 变迁点火，Chosen 库所获得令牌，与情况 1)过程相同，生成消息 m_1'后发送至 $Sender_1$。$Transmit_1$'变迁将 m_1'送入 Line-Up 库所 $Queue_2$，此时 $State\_Control_1$ 点火条件满足，将 m_1 和 m_1'同时发送至 S_2。

本文提出的 Line-Up 建模方式，在该模型分层中体现在模型的右下方 $Transmit_1$' 变迁和 State_Control 变迁及其连接弧和中间库所上。当模型中存在多个令牌（并行进程）时，该方法可以使多个令牌同时进出某一分层。如不使用该方法，先到达的令牌将可能提前进入下一模型分层，造成不同进程间由于后续变迁点火的随机错位，产生大量无用状态空间。该方法的使用在不影响结果判断的同时缩减了状态空间规模，提高了并行计算的效率。

后续模型分层中如出现某令牌等待另一令牌同时行进的情况均为 Line-Up 建模，不再重复说明。

基于攻击者的 TMN 协议安全评估模型 H_{M_2} 如图 7 所示，其主要功能是，分别处理 2 个进程的消息。如果是进程 1 消息，此时知识库中尚未收集到足以发动攻击的数据，故将进程 1 消息记录后直接转发；如果是进程 2 则重新组装消息并转发。此外，

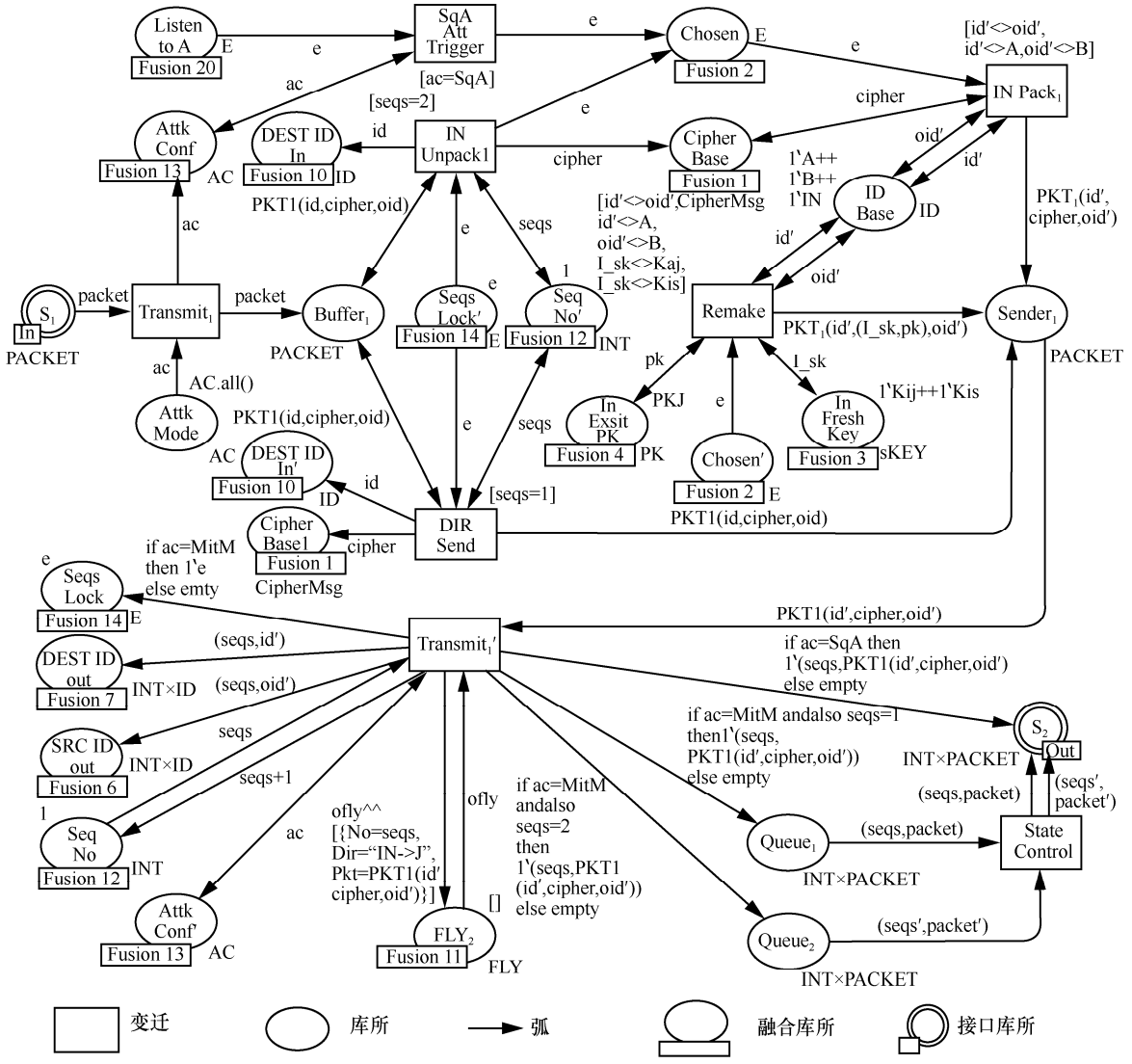

图 6　基于攻击者的 TMN 协议安全评估模型 H_{M_1}

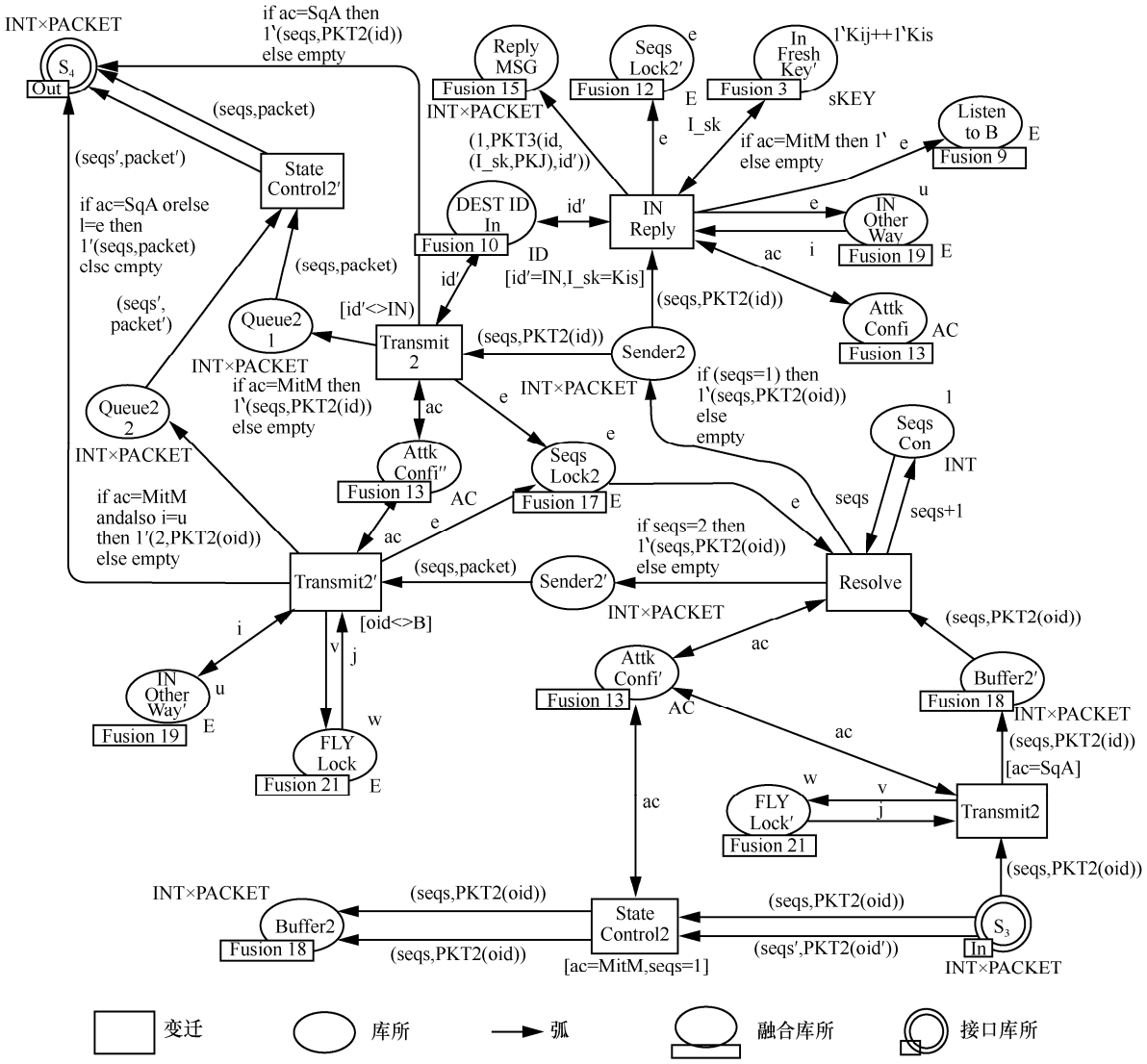

图 7　基于攻击者的 TMN 协议安全评估模型 H_{M_2}

由于攻击者也可能是合法实体，分层还需处理 A→IN 请求的情况，不能让令牌进入 B，而是直接生成 m_3 消息后将其发送至 H_{M_3} 模型。

具体过程如下。S_3 接收到 m_2 消息后，根据 Attk_Conf'的值点火不同变迁，如为 SqA 则点火 $Transmit_2$ 变迁，将数据直接送入融合库所 $Buffer_2$，如为 MitM 则点火 $State\_Control_2$ 变迁，将同时收到的 2 个令牌送入 $Buffer_2$。$Buffer_2$ 变迁可以点火 Resolve 变迁，该变迁将不同进程的消息送入不同库所中，形成 2 条分支。

1) 进程 1 消息进入 $Sender_2$ 库所，由于消息目标对象不同，如果消息发送给 B，则点火 $Transmit_2$ 变迁，之后该消息进入 Line-Up 变迁 $Queue_{2\_1}$（MitM 攻击）或者直接转发（SqA 攻击），交由 S_4 发送给 B。如果消息的目标对象是攻击者 IN，则点火 IN_Reply 变迁，生成 m_3 消息后交由下一分层 H_{M_3} 处理。

2) 进程 2 消息进入 $Sender_2$'库所，由于是攻击数据所以 $Transmit_2$'变迁会直接转发或生成新的 m_2'消息，之后消息进入 Line-Up 变迁 $Queue_{2\_2}$（MitM 攻击）或者直接转发（SqA 攻击），交由 S_4 发送给 B。

基于攻击者的 TMN 协议安全评估模型 H_{M_3} 如图 8 所示。H_{M_3} 的目标与 H_{M_2} 类似，收到进程 1 的 m_3 数据后发送至 J，收到进程 2 的数据直接发送或重组后再由 S_6 发至 J。具体描述如下。

S_5 接收到的消息由 $Transmit_3$ 变迁点火，之后由 IN_Unpack_2 解密并拆包存储，如果未成功解密则由

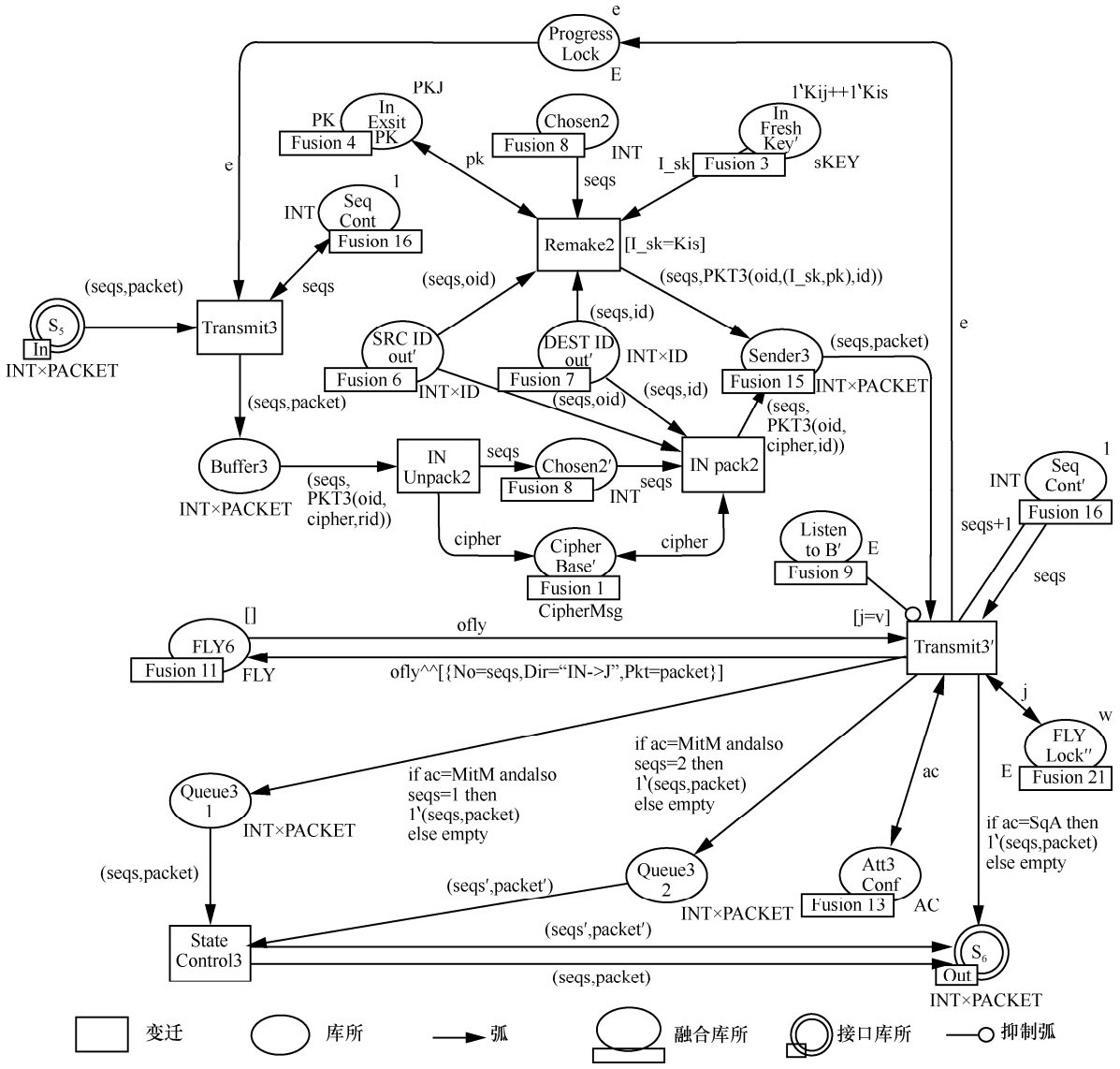

图 8　基于攻击者的 TMN 协议安全评估模型 H_{M_3}

IN_Pack_2 从知识库中提取数据按格式组装消息并发送至库所 $Sender_3$；否则 Remake 和 IN_Pack_2 库所随机点火，重新生成或按格式组装消息后发送至库所 $Sender_3$。此外，如果进程 1 中信息目标实体为 IN，则 H_{M_2} 直接将其组合好的 m_3 消息发入 $Sender_3$。随后 $Transmit_3$'变迁点火将消息由 S_6 接口处发出。

基于攻击者的 TMN 协议安全评估模型 H_{M_4} 如图 9 所示。H_{M_4} 主要作用是分别处理进程 1 和进程 2 的消息，将进程 1 消息发回给 A，进程 2 消息自己处理，尝试提取所需的密钥，判断是否攻击成功。

具体模型运行过程如下。$Transmit_4$ 变迁从 S_7 接口处接收 m_4 消息并存入 $Buffer_4$ 中，接着进程被按序号交由不同变迁处理。进程 1 数据交给 $State\_Control_4$ 变迁处理后交由 $Transmit_4$'发回 A。进程 2 由 Receive 变迁尝试解密，如解密成功则将得到的密钥存入 IN_Obtain_Key 库所，Decry_Cipher_Attmpt 继续尝试由该密钥解密其他知识库中的密文消息，如成功则存入观察库所 AB_Session_Key 中。IN_Obtain_Key 库所或 AB_Session_Key 库所中存在会话密钥，则认为攻击成功。

4　安全评估模型分析

4.1　模型状态空间报告

表 1 为 CPN-Tools 生成的模型状态空间报告节选。模型状态空间节点数为 4 252，因加入了大

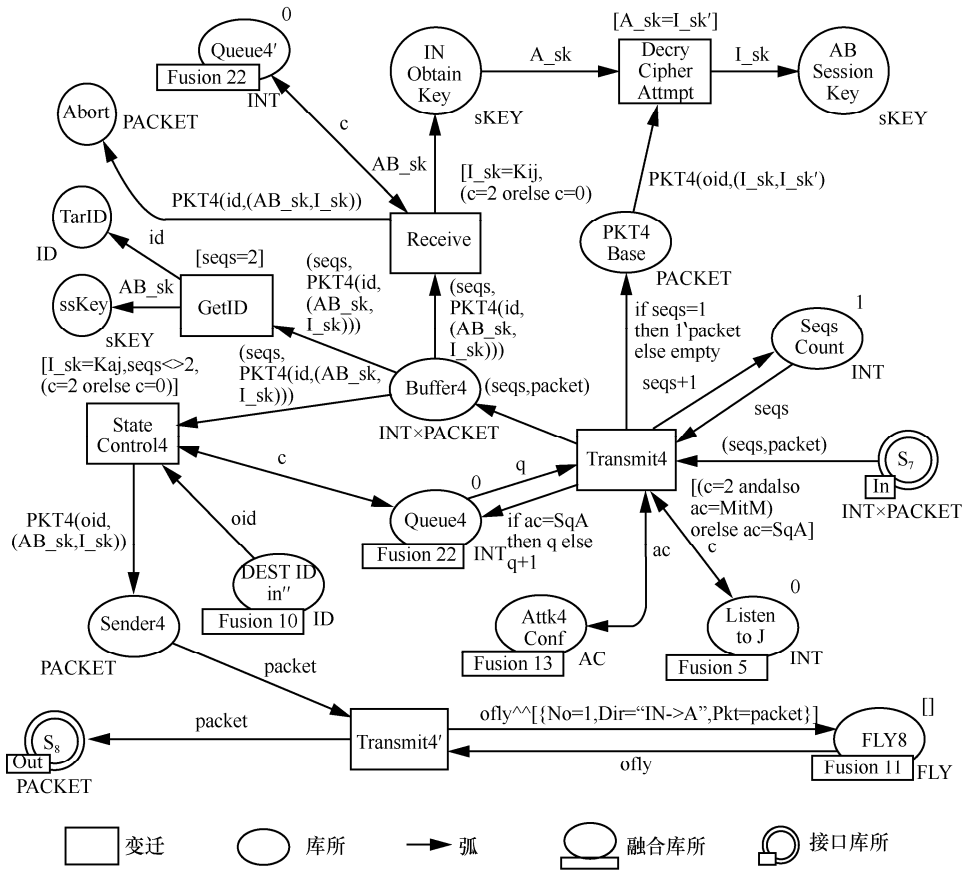

图 9　基于攻击者的 TMN 协议安全评估模型 H_{M_4}

量的控制变迁和库所，模型的复杂度大大提升。尽管如此，控制效果仍非常显著，目前的状态空间大小使分析工作具有了较高可行性。由此可见，CPN 模型状态空间增加直接原因是模型运行时可能出现的状态及路径变多，而非模型复杂度增大。

表 1　TMN 协议安全评估模型状态空间报告

类型	值
状态空间节点数量/个	4 252
有向弧数量/条	5 319
状态	完全
强联通节点数量/个	4 252
强联通弧数量/条	5 319
死节点数量/个	333

最终模型的运行过程状态一共有 4 252 个节点，5 319 条弧。全部节点和弧为强连接图，模型不存在循环结构。没有统一的最终状态所以不存在家节点。333 个死节点意味着生成图共存在 333 个终止状态。

4.2　TMN 协议安全测试分析规则

搜索攻击路径的前提是确定违背安全属性的不安全状态。密钥交换协议应满足的安全属性包括保密性、完整性和认证性[25]。

1) 保密性。通信实体之间交换的会话密钥应为保密的，不能被除合法实体之外的第三方获知。

2) 完整性。通信实体之间交换的消息不能被攻击者篡改、删除或替代。换言之，完整性是指收到的数据和原始数据之间保持完全一致的特性。

3) 认证性。认证性是安全通信的重要保障，协议需要通过认证对通信主体进行识别，当一方声称自己就是某个主体的身份时，另一方需要验证该身份。

TMN 作为典型的密钥交换协议，理应满足上述安全属性。但其在设计时没有充分考虑认证属性，使攻击者实施伪装成为可能，并借此实现各种可能的攻击。因此，按照协议规则，在形式化验证该协议时主要聚焦于保密性和完整性两方面。

协议的安全分析和评估，即证明是否存在违背上述安全属性的状态。根据 2.4 节假设的攻击者能

力，攻击者通过截获、篡改、伪造等能力，将收到的每一步消息拆分并存入自己知识库，之后按协议消息格式任意组合攻击消息并将其发送至其余协议参与者。在这过程中，一旦攻击者获得了他人有效的会话密钥，即违背了协议的保密性。而如果攻击者使实体A或B实际交换的密钥与各自认可的会话密钥出现差异，则违背了协议的完整性。违背一条或多条安全属性均视为不安全状态达成。虽然因Dolev-Yao 攻击者模型引发的大量重复无用数据已在协议建模时被消除，但模型中仍存在不能构成攻击的非攻击路径，此类路径的存在给攻击路径提取工作带来干扰，为制定正确有效的攻击路径提取规则，需排除可能的非攻击路径。

基于 3.1 节中对攻击者模型的分析，TMN 协议安全性评估模型中攻击过程全部为二次并发过程，且实体 A、B 分别只参与一次会话。因此加入攻击者后模型可能出现的数据流向如下。

1) 进程 1 是 A→B 的情况，进程 2 中所有角色均是由攻击者 IN 伪造的，分为以下三类。

① $p_1.\mathrm{A}\to\mathrm{B};\ p_2.\mathrm{IN}(\mathrm{A})\to\mathrm{IN}(\mathrm{B})$

② $p_1.\mathrm{A}\to\mathrm{B};\ p_2.\mathrm{IN}(\mathrm{A})\to\mathrm{IN}$

③ $p_1.\mathrm{A}\to\mathrm{B};\ p_2.\mathrm{IN}\to\mathrm{IN}(\mathrm{B})$

其中，括号中为攻击者伪装的角色，p_1、p_2 分别代表进程 1 和进程 2。上述 3 种运行方向对于攻击者而言，有两类目标数据，分别为进程 1 中 A 和 B 达成的会话密钥 K_{ab}、A 的临时密钥 K_{aj}。获得 K_{aj} 后攻击者可解密其知识库中的$\{K_{ab}\}K_{aj}$ 从而间接获得 K_{ab}。而获得 K_{ab} 意味破坏了协议的保密性。此外，由于进程 1 中消息 1 和消息 3 格式相同，攻击者可在进程 1 时调换消息 1 和 3 中加密数据的位置，从而使 A 认为正确的会话密钥是 K_{aj}，而 B 认为是 K_{ab}，在这种情况下如果攻击者获得 K_{aj} 则同时破坏了协议的保密性与机密性。

2) 进程 1 是 A→IN 的情况，分为以下四类。

① $p_1.\mathrm{A}\to\mathrm{IN};\ p_2.\mathrm{IN}(\mathrm{A})\to\mathrm{B}$

② $p_1.\mathrm{A}\to\mathrm{IN};\ p_2.\mathrm{IN}\to\mathrm{B}$

③ $p_1.\mathrm{A}\to\mathrm{IN}(\mathrm{B});\ p_2.\mathrm{IN}\to\mathrm{B}$

④ $p1.\mathrm{A}\to\mathrm{IN}(\mathrm{B});\ p_2.\mathrm{IN}(\mathrm{A})\to\mathrm{B}$

除②中 IN 两次运行均为合法参与者身份不予考虑以外，其余三类均由 A 请求与不同身份的 IN 发起密钥交换请求，由于攻击者具有合法实体的能力，不论是 IN 伪装成 A（即 IN(A)→B）还是 IN 伪装成 B（即 A→IN(B)）均可在协议单次运行中实现。为避免内容重复，④中 IN 可同时伪装成 A 和 B，寻找攻击路径时以④为准，不再单独处理①和③的情况。进程 1 中 A 与伪装成 B 的 IN 交换密钥 K_{is}，进程 2 中 IN 伪装成 A 与 B 交换密钥 K_{ab}。攻击者一旦成功则破坏了协议的机密性与完整性。

3) 进程 1 是 IN→B 的情况，同样分为以下四类。

① $p_1.\mathrm{IN}\to\mathrm{B};\ p_2.\mathrm{A}\to\mathrm{IN}(\mathrm{B})$

② $p_1.\mathrm{IN}\to\mathrm{B};\ p_2.\mathrm{A}\to\mathrm{IN}$

③ $p_1.\mathrm{IN}(\mathrm{A})\to\mathrm{B};\ p_2.\mathrm{A}\to\mathrm{IN}$

④ $p_1.\mathrm{IN}(\mathrm{A})\to\mathrm{B};\ p_2.\mathrm{A}\to\mathrm{IN}(\mathrm{B})$

上述类型与进程 1 是 A→IN 的情况相比只有顺序改变而无实质性变化，攻击路径搜索以进程 1 是 A→IN 为准。

由此可制定评估模型的安全分析测试规则如下。

规则 1 A 和 B 交换密钥 K_{ab} 成功，攻击者获得 A、B 的会话密钥 K_{ab}。

规则 2 A 和 B 交换密钥 K_{ab} 成功，攻击者获得 A 的临时密钥 K_{aj}，由 K_{aj} 解密$\{K_{ab}\}K_{aj}$ 得 K_{ab}。

规则 3 A 和 B 认可的会话密钥分别是 K_{aj} 和 K_{ab}，攻击者获得密钥 K_{aj}，由 K_{aj} 解密$\{K_{ab}\}K_{aj}$ 得 K_{ab}。

规则 4 A 和 B 认可的会话密钥分别是 K_{is} 和 K_{ab}，攻击者获得密钥 K_{is} 和 K_{ab}。

由图 2 可知，攻击者介入后，每一次正常实体间的通信过程都有攻击者参与。首次会话的运行步骤由最初的 4 个步骤变为 8 个步骤，具体为：1) A→IN，2) IN→J，3) J→IN，4) IN→B，5) B→IN，6) IN→J，7) J→IN，8) IN→A。如果出现 A 的通信目标是 IN 的情况，则运行步骤变为 6 个：1) A→IN，2) IN→J，3) J→IN，4) IN→J，5) J→IN，6) IN→A。而第二次会话由于可能出现 IN 伪装 A 和 B 而不发送给真实实体 A、B 的情况（4 个步骤），或者 IN 发给 B 的情况（6 个步骤）。为使攻击路径提取更加全面，防止不必要的疏漏，规定完整的步骤记录为 12 个步骤。

在此基础上，由于采用了 on-the-fly 路径记录方法，状态空间生成的同时所有路径记录已经存在于状态节点中，按条件提取后即可获得协议的攻击路径。

4.3 搜索攻击路径

本节以安全分析测试规则 1 为例，即 A 和 B 交换密钥 K_{ab} 成功，攻击者获得 A、B 的会话密钥 K_{ab}。在模型中体现为实体 A 中的观察库所 A_Session_Key

获得令牌 Kab，且 M_4 的攻击者观察库所 IN_Obtain_Key 中获得令牌 Kab 的情况。

编写代码在状态空间计算后执行，结果如图 10 所示。

```
val attRes1 = [4169,4148,4111,4097,4065,4049,3379,3371,3367] : Node list
```

图 10　规则 1 查询代码运行结果

图 10 的节点编号代表通过 SML 查询出的全部结果。这些节点均为到达测试规则 1 的死节点。继续提取模型中 FLY 库所所记录的内容，例如 Mark.M4'FLY8 1 4169 为提取编号为 4169 的节点中 FLY 库所的内容，其结果如图 11 所示。

```
val it =
 [[{Dir="A->IN",No=1,Pkt=PKT1 (B,(Kaj,PKJ),A)},
   {Dir="IN->J",No=1,Pkt=PKT1 (B,(Kaj,PKJ),A)},
   {Dir="IN->J",No=2,Pkt=PKT1 (B,(Kij,PKJ),IN)},
   {Dir="J->IN",No=1,Pkt=PKT2 A},{Dir="J->IN",No=2,Pkt=PKT2 IN},
   {Dir="IN->B",No=1,Pkt=PKT2 A},{Dir="B->IN",No=1,Pkt=PKT3 (A,(Kab,PKJ),B)},
   {Dir="IN->J",No=1,Pkt=PKT3 (A,(Kab,PKJ),B)},
   {Dir="IN->J",No=2,Pkt=PKT3 (IN,(Kab,PKJ),B)},
   {Dir="J->IN",No=1,Pkt=PKT4 (B,(Kab,Kaj))},
   {Dir="J->IN",No=2,Pkt=PKT4 (B,(Kab,Kij))},
   {Dir="IN->A",No=1,Pkt=PKT4 (B,(Kab,Kaj))}]] : FLY ms

Mark.M4'FLY8 1 4169
```

图 11　节点 4169 的 FLY 库所内容

模型中出现的库所数量远大于 FLY 库所记录的属性数量，因此某些不同的状态节点可能记录的数据完全相同，导致 2 个或多个节点内容重复。编码将重复节点删除后，图 10 中 9 个节点变为 6 个，如图 12 所示。

```
val it = [3367,3371,3379,4065,4111,4169] : Node list

listUnique(attRes1)
```

图 12　标识有效攻击路径的节点

利用 SML 将所有节点中 FLY 库所的内容提取并转化为文本，格式化后保存至 TXT 文件中，可以得到图 11 中 6 个节点中记录的具体攻击路径，将其中之一归纳后示例攻击路径如下。

M_1 : A → J: (B, $\{K_{aj}\}K_{JP}$), A

M_1' : IN → J: (B, $\{K_{ij}\}K_{JP}$), I

M_2' : J → IN: I

M_2 : J → B: A

M_3 : B → J: (A, $\{K_{ab}\}K_{JP}$), B

M_3' : IN → J: (I, $\{K_{ab}\}K_{JP}$), B

M_4' : J → IN: (B, $\{K_{ab}\}K_{ij}$)

M_4 : J → A: (B, $\{K_{ab}\}K_{aj}$)

攻击者成功获得实体 A、B 之间交换的会话密钥 K_{ab}，实现了对协议的攻击。这就意味着一条有效攻击路径已被找到。同理，批量导出实验中前述安全测试规则的全部可达路径，合计找到有效攻击路径 25 条，表 2 为每种测试规则产生的攻击路径数量。

表 2　　各测试规则下攻击路径数量

安全测试规则	攻击路径数量/条
规则 1	6
规则 2	6
规则 3	6
规则 4	7
合计	25

4.4　协议安全评估结论

综上所述，CPN 建模的方法有效提取出 25 条 TMN 协议的攻击路径，其中 Line-Up 并行建模方法起到了重要作用。引入 Line-Up 控制前后的状态空间对比如表 3 所示。

表 3　　Line-Up 引入前后状态空间数量对比

控制方法	节点/个	弧/条	死节点/个
Line-Up 引入前	41 501	62 540	4 560
Line-Up 引入后	4 252	5 319	333
缩减	91.27%	93.13%	94.93%

由此可见，引入 Line-Up 控制方法后状态空间被大规模减小了，使状态空间数缩减到比较易于分析和操作的状态，模型中大量无用状态被消除，TMN 协议的安全性被有效验证，同时提高了 CPN 模型并行处理的效率。这种针对安全协议并行建模状态空间削减的规模及方法在先前的同类研究中没有出现过。

本文方法与现有方法状态空间规模对比如表 4 所示。文献[19-20]均未采用有效的状态空间控制方法，其状态空间数已到达爆炸的边缘。而本文在最终 333 个死节点中提取出有效攻击路径，经归纳整理及合并重复路径后，这些攻击路径基本涵盖了目前已发现 TMN 协议的所有攻击路径。模型的攻击路径提取效率比文献[19-20]高。

4.5　评估方法优势分析

通过实验可知，在建模方法与效果方面，本文方法与其他利用 CPN 对安全协议建模分析的方法相比，在效率和可行性方面具有较大优势。

首先，利用 CPN 进行协议模型检测时，状态

空间爆炸是获取有效数据的阻碍。多数研究工作选择将模型状态空间划分成若干小块，再分别研究每一块的状态空间。但即使如此，每一块状态空间的规模仍维持在了一个可观的数量级。在这种情况下，模型检测的效率是不高的。本文所述 Line-Up 方法属于偏序规约范畴，通过修改并行进程的执行顺序，在不影响分析结果的前提下，将运行过程中由于变量先后绑定问题出现的大量无用状态剔除，使状态空间维持在了一个较小的数量级。

表 4　本文方法与现有方法状态空间规模对比

方法	协议	节点/个	弧/条	死节点/个
文献[19]方法	TMN	79 722	418 627	8 655
文献[20]方法	TMN	106 962	116 040	未知
本文方法	TMN	4 252	5 319	333

其次，部分研究利用 CPN 验证了安全协议是否存在可能的安全问题，但没有找到具体的攻击路径，研究粒度不够细致，甚至没有达到形式化分析的一般标准。本文提出的研究方法是配合改进后的状态空间控制进行的，在为数不多的状态空间之中通过 on-the-fly 方法和 SML，将违背协议安全声明的“不安全状态”到达路径全部提取，从而保证了发现协议安全问题的同时能够提出“反例”（攻击路径）。本文方法与同类 CPN 协议安全性分析方法的对比如表 5 所示。

表 5 所列对比方法为近年来具有代表性的 CPN 形式化协议分析研究，其中所述协议均存在一定安全缺陷，而这些研究大多没有实现状态空间有效控制或攻击路径提取。因此，本文所述 CPN 形式化协议建模分析方法具有较大优势，能够将状态空间控制在一个合理可行的范围，同时分析协议可能存在的漏洞并找到攻击路径。

5　结束语

本文提出了一种改进的基于 CPN 对协议安全性分析的方法，该方法能够提取出有效攻击路径。在并发控制状态空间方面提出了 Line-Up 偏序规约建模思想，保证了实验客观性的同时避免了因并发令牌先后进入其他模型分层造成的状态空间爆炸。这样增加了模型的复杂度，但剔除了 CPN 并行建模中大量无用状态从而大规模缩减了模型状态空间。

实验证明本文方法是有效的，通过与现有同类研究对比可知，本文方法在状态空间的缩减、攻击路径提取、验证效率和可行性等方面具有较大优势。未来可以尝试用于其他安全协议的安全性形式化验证。然而本文也存在一些不足之处，由于篇幅所限协议验证结果没有给出全部攻击路径的细节描述，协议中各种漏洞是由安全机制不完善引起的，应进一步分析这些漏洞产生的原因。此外，本文选用的 TMN 协议较落后，已不是主流安全协议，本文只是借其说明方法的有效性。

未来的工作将继续研究 CPN 形式化分析过程中存在的问题及解决方案，针对不同协议探究如何在保证正确性的情况下收敛其状态空间规模。由于各种协议所保障的安全属性不同，下一步将尝试利用本文方法研究更多的安全协议，总结该方法的适用范围以及如何验证更多的安全属性，并继续采用 CPN 形式化建模的方法为方案改进提供良好的支撑。

参考文献：

[1] 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 verification of security protocols[M].

表 5　本文方法与同类 CPN 协议安全性分析方法对比

方法	状态空间搜索	状态空间控制	状态空间规模	状态空间完整	提取攻击路径	攻击路径数量	批量搜索状态
文献[7]方法	×	√	可变	×	×	0	×
文献[11]方法	×	√	数万	×	×	1	×
文献[15]方法	×	×	×	×	×	2	×
文献[19]方法	√	√	10 万	×	√	5	√
文献[20]方法	√	√	10 万	×	√	10	√
文献[22]方法	√	√	数百	×	×	0	×
本文方法	√	√	数千	√	√	25	√

Beijing: Science Press, 2019.

[2] 黎波涛, 罗军舟. 不可否认协议的Petri网建模与分析[J]. 计算机研究与发展, 2005, 42(9): 1571-1577.
LI B T, LUO J Z. Modeling and analysis of non-repudiation protocols by using petri nets[J]. Journal of Computer Research and Development, 2005, 42(9): 1571-1577.

[3] XU Y, XIE X, ZHANG H. Modeling and analysis of security protocols using colored petri nets[J]. Journal of Software, 2011, 6(7): 19-27.

[4] NORTA A, MATULEVICIUS R, LEIDING B. Safeguarding a formalized blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns[J]. Computers & Security, 2019, 86(9): 253-269.

[5] COHN G K, CREMERS C, DOWLING B, et al. A formal security analysis of the signal messaging protocol[J]. Journal of Cryptology, 2020, 33(4): 1914-1983.

[6] WANG D, HUANG X, MA X F. Formal analysis of smart contract based on colored petri nets[J]. IEEE Intelligent Systems, 2020, 35(3): 19-30.

[7] RODRÍGUEZ A, KRISTENSEN L M, RUTLE A. Formal modelling and incremental verification of the MQTT IoT protocol[J]. Transactions on Petri Nets and Other Models of Concurrency, 2019, 11(XIV): 126-145.

[8] BECHAR R, TAHAR A M, MEZOUDJ F, et al. On formal modeling and validation of wireless sensor network protocols[J]. Wireless Personal Communications, 2020, 114(4): 2855-2888.

[9] MACHADO P, SILVA M R, SOUZA L E, et al. Modeling using colored petri net of communication networks based on IEC 61850 in a microgrid context[J]. Journal of Control, Automation and Electrical Systems, 2018, 29(6): 703-717.

[10] ANSAROUDI Z E, PASHAZADEH S. Modeling and formal verification of the ticket-based handoff authentication protocol for wireless mesh networks[C]//2019 International Symposium on Pervasive Systems, Algorithms and Networks. Berlin: Springer, 2019: 140-154.

[11] 鲁晔. 基于 HCPN 模型检测方法的 DNP3-SA 协议形式化安全评估与改进[D]. 兰州: 兰州理工大学, 2018.
LU Y. Formal security assessment and improvement of DNP3-SA protocol based on HCPN model detection[D]. Lanzhou: Lanzhou University of Technology, 2018.

[12] 姜筱彦. 基于HCPN 模型检测方法的 BACnet 协议形式化安全评估与改进[D]. 兰州: 兰州理工大学, 2020.
JIANG X Y. Formal security evaluation and improvement of BACnet protocol based on HCPN model detection method[D]. Lanzhou: Lanzhou University of Technology, 2020.

[13] 冯涛, 王帅帅, 龚翔, 等. 工业以太网 EtherCAT 协议形式化安全评估及改进[J]. 计算机研究与发展, 2020, 57(11): 2312-2327.
FENG T, WANG S S, GONG X, et al. Formal security evaluation and improvement of industrial Ethernet EtherCAT protocol[J]. Journal of Computer Research and Development, 2020, 57(11): 2312-2327.

[14] FAN Y T, SU G P, HE L, et al. Study on a CPN-based auto-analysis tool for security protocols[C]//2012 Fourth International Symposium on Information Science and Engineering. Piscataway: IEEE Press, 2012: 179-182.

[15] IGOREVICH R R, SHIN D, MIN D. CPN Based analysis of in-vehicle secure communication protocol[C]//2016 International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Berlin: Springer, 2016: 12-21.

[16] WANG C L, TAO Y G, ZHOU Y. Protocol verification by simultaneous reachability graph[J]. IEEE Communications Letters, 2017, 21(8): 1727-1730.

[17] AMOAH R, CAMTEPE S, FOO E. Formal modelling and analysis of DNP3 secure authentication[J]. Journal of Network and Computer Applications, 2016, 59: 345-360.

[18] 田学成. 工业控制系统 EtherNet/IP 协议安全性分析[D]. 兰州: 兰州理工大学, 2020.
TIAN X C. Safety analysis of EtherNet/IP protocol of industrial control system[D]. Lanzhou: Lanzhou University of Technology, 2020.

[19] 白云莉. 基于 CP-nets 模型的安全协议形式化方法研究[D]. 呼和浩特: 内蒙古大学, 2013.
BAI Y L. Research on security protocol formal method based on colored petri nets model[D]. Hohhot: Inner Mongolia University, 2013.

[20] PERMPOONTANALARP Y, SORNKHOM P. On-the-fly trace generation approach to the security analysis of cryptographic protocols: coloured petri nets-based method[J]. Fundamenta Informaticae, 2014, 130(4): 423-466.

[21] SUN T, ZHANG W, GUO X, et al. Research on CPN model reduction focus on parallel tested behaviors[C]//2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications. Piscataway: IEEE Press, 2017: 827-833.

[22] DRESP W. Security analysis of the secure authentication protocol by means of coloured petri nets[C]//2005 IFIP International Conference on Communications and Multimedia Security. Berlin: Springer, 2005: 230-239.

[23] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[24] 刘秀英, 张玉清, 杨波, 等. 协议的形式化分析[J]. 西安电子科技大学学报自然科学版, 2004, 31(5): 785-790.
LIU X Y, ZHANG Y Q, YANG B, et al. An approach to the formal analysis of the TMN protocol[J]. Journal of Xidian University-Natural Science, 2004, 31(5): 785-790.

[25] 赵华伟, 李大兴. 密钥交换协议的安全性分析[J]. 山东大学学报(理学版), 2006, 41(4): 101-106.
ZHAO H W, LI D X. Key-exchange protocols' security analysis[J]. Journal of Shandong University (Natural Science), 2006, 41(4): 101-106.

[作者简介]

龚翔（1986− ），男，上海人，兰州理工大学博士生，主要研究方向为制造业信息化系统与网络安全、工业物联网协议安全的形式化验证等。

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、区块链和工业互联网等。

杜谨泽（1986− ），男，甘肃会宁人，博士，兰州理工大学讲师，主要研究方向为无线传感器网络、工业物联网、室内定位、网络安全等。

《通信学报》第十届编辑委员会

收录声明

本刊对发表的文章，拥有出版电子版、网络版版权，并拥有和其他网站交换信息的权利。本刊支付的稿酬中已经包含上述费用。

Journal on Communications has the copyright to publish electronic edition, online edition of the published articles, and has the right to exchange information with other sites. The expenses have been included in the fee paid by editorial department.

道德声明

本刊发表的论文是作者独立取得的原创性研究成果，无一稿多投；论文内容不涉及国家机密；未曾以任何形式用任何文种在国内外公开发表过；论文内容不侵犯他人著作权和其他权利。若发生一稿多投、侵权、泄密等问题，论文作者将承担全部责任。

The authors of *Journal on Communications* guarantee that their submitted articles are original and contain nothing confidential. The said article is only submitted to *Journal on Communications*. The said article has not been published before and has not been submitted elsewhere for print or electronic publication consideration. The said article is no way whatever a violation or an infringement of any existing copyright or license from the third party. Otherwise, the authors of the said article shall take the blame for the violation or infringement of the related copyright and the leakage of secrets.

通信学报

Journal on Communications

发行代号：国内2-676 / 国外M395　2021年9月25日出版　定价：98.00元

ISSN 1000-436X

CN 11-2102/TN