第 35 卷 第 1 期 计 算 机 工 程 2009 年 1 月
Vol.35 No.1 Computer Engineering January 2009
·人工智能及识别技术· 文章编号：1000—3428(2009)01—0159—03 文献标识码：A 中图分类号：TP393

基于 Petri 网的指挥信息系统死锁防治算法

张 力，慕晓冬，赵宗涛
(第二炮兵工程学院 401 教研室，西安 710025)

摘 要：多兵种联合作战指挥信息系统死锁防治是保障系统安全可靠的根本问题，也是有待解决的难点之一。该文提出一种描述指挥信息系统的形式化方法——Petri 网模型，以抽取某级通信指挥系统与筹划作战方案的智能运作模型为实例，系统归纳了模型抽取方法，进而提出其死锁防治算法 DLPCA，它能够防止系统出现的死锁等弊端，为组建一体化信息系统提供可靠的理论基础。经仿真试验，算法是有效可行的，在系统较长时间的工作中，可将死锁的次数减少 50%左右。

关键词：Petri 网模型；信息系统；作战指挥；死锁防治

Prevention and Cure of Deadlock Algorithm for Command Information System Based on Petri Net

ZHANG Li, MU Xiao-dong, ZHAO Zong-tao
(401 Division, Second Artillery Engineering Institute, Xi'an 710025)

【Abstract】The prevention and cure of deadlock of command information system for united combat of multi-troops is the fundamental problem to ensure the safety and the reliability of system. It is also one of difficult problems to be solved. This paper puts up a kind of formal method which describes the command information system——Petri net model, giving an example of setting up intelligent running models of planning battle plan and brigade-level communication and command system, sums up the method of setting up models, puts up its deadlock prevention and cure algorithm DLPCA, it can prevent deadlocks of system and provide reliable theory foundation for setting up integration information system. Through simulation test, the algorithm is proved to be effective and feasible. In longer period of system's working, the amount of deadlocks has been reduced by about 50%.

【Key words】Petri net model; information system; battle command; prevention and cure of deadlock

以信息化为基础的一体化联合作战将成为未来信息战的基本形式。人们从实践中认识到，要使系统能够正常地工作，必须首先抽取其数学模型，经过反复论证才能生成有效的信息系统。否则，在应用中就会出现死锁等许多弊端，而且对系统也无法进行定量评估。在联合作战训练中，利用 Petri 网理论抽取了指挥信息系统以及机关智能运作的形式化模型，有效地解决了因资源竞争而引发的死锁等问题。

1 指挥信息系统及 Agent 智能运作的 Petri 网模型

某指挥信息系统的组成主要为 2 大部分：一部分是实现信息无缝链接的通信系统；另一部分是模拟机关智能运作的 Agent 软件系统。下面以抽取这两者 Petri 网模型为实例来研究其技术方法。

1.1 指挥信息系统 Petri 网模型

为便于描述，假设某指挥信息系统结构形式在拓扑上是一个 1-4-6 树型数据结构。这种结构的优点是容易利用树理论进行系统性能评价，例如信息节点的遍历等，都已经具有现成的算法。缺点是可靠性较差。若一个节点缺失，则下属信息节点则全部失控。

经过长时间的实践，该系统具有以下的问题：

(1)互联不能互通。也就是说各单元通过信道已经连通但信息不能传输，或迟滞现象严重。

(2)资源竞争严重。即整个系统局部或全部死机等待，出现死锁，系统不能正常工作。

(3)数据打包集成可以传输，散列数据不能传输。即像命令字这样简单的数据串不能可靠传输，严重影响作战任务的执行。

(4)在应用操作中不能出错，一旦出错必须从头重来。

(5)系统建成后无法定量评估系统的性能。即无法定性地总结一些经验。

分析出现以上情况，硬件软件不能可靠工作等诸多的因素是一些基本原因。但根本原因是，在系统集成时论证不充分，缺乏必要的基础理论支持。因此，应对所想象的网络结构，抽取其数学模型，包括变量设置和动态运作进行系统分析。

图 1 是抽取的 Petri 网模型，其中，图中的矩形框表示事件转移；小圆圈表示处所；弧线代表信息运行方向；t0 主要做信息归纳整理和判断。逻辑值等于 0 时，将其处所中的托肯置成 1 个，以此控制转向相应的分枝。逻辑值等于 1, 2, 3 时，依此类推。图中带有交叉的箭头指：在判断中还需其他分枝加密后的信息是否与此相等。若相等，则调制发送，否则停止发送。

基金项目：国家部委预研基金资助项目
作者简介：张 力(1964－)，女，副教授、博士，主研方向：计算机软件理论；慕晓冬、赵宗涛，教授、博士生导师
收稿日期：2008-05-11 **E-mail：**wascom4@sohu.com

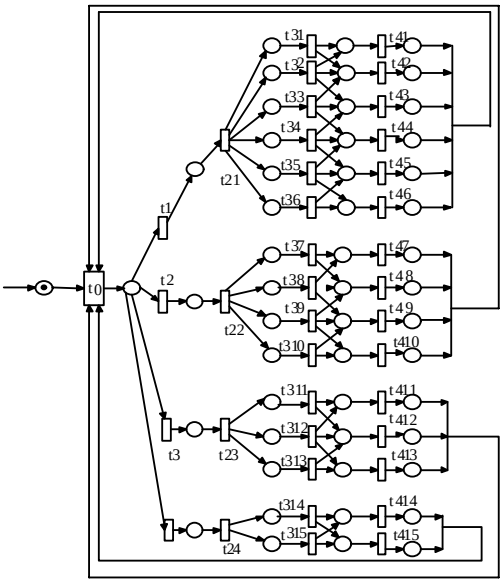

图 1　系统的 Petri 网模型

1.2　指挥信息系统 Agent 模型

Agent 是一个运行于动态环境的具有较高自治能力和智能运作的实体[1]。Agent具有自主决断能力，能够感知其所处的环境、适应环境的变化和模拟人的行为，使之制定作战方案等智能运作实现自动化。Agent的工作过程如图 2 所示。

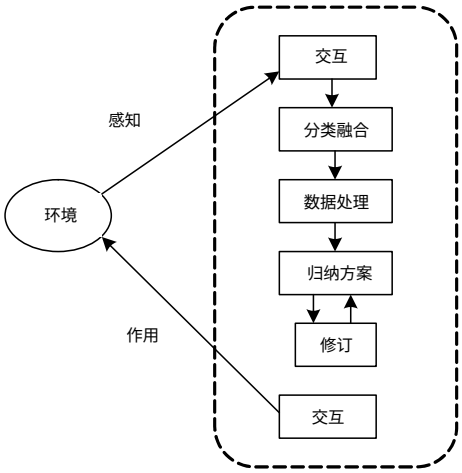

图 2　Agent 的工作过程

Agent 接收到的信息首先要以适当的方式进行融合、分类，并能为 Agent 知识库所接受；数据处理是按软件需求的数据结构进行格式编排，便于统一存储管理；归纳方案是指在分类加工知识的基础上，依据适应客观环境的需求拟订行动计划。对作战指挥系统来说，就是制定参考性作战方案；修订是反复搜索已整理的环境信息，对归纳的方案进行完善性修改；交互主要是 Agent 的主体部分与环境进行信息交流，其界面犹如人机交互界面。一旦 Agent 接收外部消息，信息处理过程成为 Agent 的核心，因为它反映 Agent 的真正功能。信息处理的目的是揭示可用数据，形成具体规划。

按照文献[1]的方法，结合笔者实践，将指挥信息系统 Agent 结构进行重新修订设计。修订后的结构描述如下：

(1)通信模块和接收模块。通信模块是负责与外部的通信联络。而接收模块主要是接收情报信息和上一级作战指令。

(2)归纳分类模块。主要是将情报信息分类成敌我武器装备信息、战场地形信息以及其他武器信息，后者列为特殊一类，以便进行应急决策。此项分类有利于决策利用。

(3)态势评估模块。主要从已经接收的情报信息来进行定量评估敌我作战意图及发展趋势，以便为进一步计划火力、作战方案优化提供依据。

(4)决策模块。采用预案选择和修订作为制定作战方案的主要方法。预案库在作战准备中已经存储若干预先制定的方案。修订主要是根据作战实际进行修订。

(5)应急反应模块。应急反应主要是指必要时指挥员可以越级指挥，随机选定作战阵地和火力计划方案。在此情况下，可更快地实施作战行动。

归纳起来，从功能上说，主要是感知、归纳、运作和驱动 4 大部分。

图 3 用 Petri 网来表达 Agent 及多 Agent(MAS)。

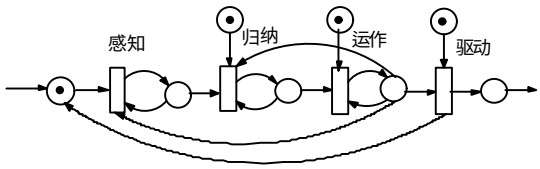

图 3　Agent 的 Petri 图

它表达了 Agent 进行智能运作的形式化模型。其过程为：感知-归纳-运作-驱动 4 个转移事件。所谓感知就是通过各种传感器将外部信息进行接收，它主要的动作是将各传感器传来的信息进行数据融合，生成情报信息；归纳主要是将感知的信息数据进行归纳、整理、析取有用的要点归纳成文件；运作就是智能运作，它是 Agent 的核心操作，它主要是将归纳的敌情我情的信息加工成作战文书。一般情况下这种智能运作是通过专家系统来实现的。对作战方案的生成，通常是根据情报和上级的任务在作战预案库中选取，再进行适当修改而成；驱动就是将作战文书实施指挥的过程。

多 Agent 系统（MAS）如图 4 所示，表达的是 3 个 Agent 通过通信网多次交互来完成协作任务。图中双向弧线表达是一个判决条件的生成是要经过反复进行事件的转移运作才能完成。更多的 Agent 连接图可进行类似抽取 Petri 网。

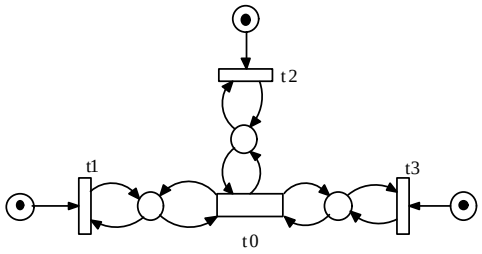

图 4　指挥决策 MAS 的 Petri 网

2　指挥信息系统死锁发生与防治方法

在实际作战中，由于涉及到多部队大区域，因此信息系统结构复杂。从外军所披露的情报信息知道，美军由于信息系统死锁，导致不能正常工作而引发的误警信号和错误发射指示，不止一次地警示人们防治系统死锁的重要性。

2.1　系统防治死锁算法

首先由信息系统的结构抽取其 Petri 网模型。预编一个遍历 Petri 网的子程序，其功能可完成统计和登记必要的信息。在此基础上，进行搜索查找 Petri 网的枝权点，并统计计算在枝权点动态点火后各分支表征需求资源的托肯数。若 2 只以上的枝权都需求对方所占有的条件及托肯，则有可能发生死锁。完成此项工作需编排一个搜索程序然后将搜索的结果列表登记，并归入该系统的动态表中。本文主要是根据上述思

想构造算法。以下列出死锁防治算法——DLPCA：

Step 1 绘制信息系统结构图，反复审视，力求完整，并整理成树形结构，以便搜索和修改。

Step2 据 Step 1 来抽取其 Petri 网模型。必须示出状态和转移。转移路径必须明确。

Step 3 应用 Step2 搜索信息系统及相应的 Petri 网图。将搜索结果记入表格。特别在表格栏目中应示出枝权点，且予以编号。

Step 4 继续搜索 Petri 网图，查找处所中的 Token 数量，归入专门的统计表格。

Step 5 归纳各枝权中在实施行动后所需要的 Token 数。若 2 个以上的枝权中各自需要的 Token 在对方处所中，则发生死锁，处置方法进入 Step6；若否，则转入 Step 1。

Step 6 根据各枝权信息需求所配置的权数，按大小论处。权值小的则无条件停止信息传输，从而避免死锁。

2.2 试验结果分析

在表 1 中列举了采用算法 DLPCA 分析指挥信息系统在动态工作后所发生死锁次数与原来相比较的数据。所列数据显示，实验次数越多，发生死锁的次数也越多。但是，采用新算法后由于系统结构有了形式化描述，为自动寻找可能发生的死锁节点提供了一种方法。由于 Petri 网中表征了信息流动所需的资源情况，也就是托肯数，因此可预测动态工作后，也就是行动后节点发生死锁的可能性。

表 1 原来与现在死锁次数比较

实验次数	原来死锁次数	现在死锁次数
5	5	4
10	7	5
15	9	7
20	11	8
25	12	9
30	13	9
35	14	10
40	15	11

图 5 所示的曲线是表 1 数据的直观显示。由实验可以看出，算法是有效的，也是可行的。在作战训练中，一般在数天时间中，系统可能动态工作上千次之多。由此更能显示算法的优越性。

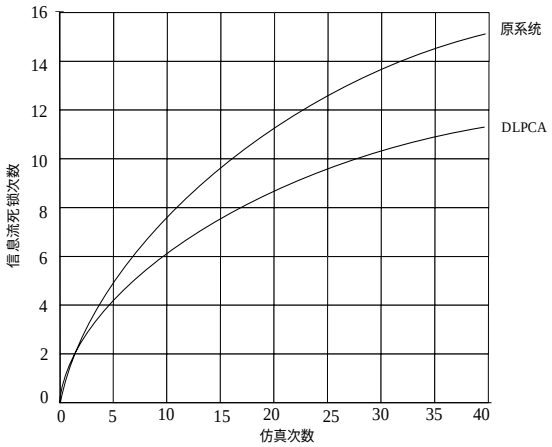

图 5 运用 DLPA 算法后死锁情况

3 结束语

在某级三级信息系统中，用 Petri 网理论抽取其数学模型，是一种重要的研究方法。一是可据此研究信息系统可能发生死锁的节点，二是为系统的评估创造了有利的条件。本文提出了一种查找系统动态工作时死锁可能发生的节点，为防治做了准备工作。实验表明，算法是行之有效的。但对相关的搜索、表格登记等软件要预先置于工具包中。从表 1 数据可以看出，当实验 35 次时，死锁次数可减少 4 次。在一次训练近千次的动态工作中，死锁的次数可减少 50%。需要说明的是，系统死锁不完全是发生在枝权点，相关问题仍需进一步研究。

参考文献

[1] 杨瑞平，郭齐胜. C^3I系统建模与仿真[M]. 北京: 国防工业出版社, 2006-01.

（上接第 137 页）

息、对 TUNNEL 值进行判断以及执行 tunnel_ setup()和 tunnel clean()时，分别打印相关语句作为辅助信息。具体操作为：V=1，打印“we need no tunnel”; V=0，打印“we need tunnel”;TUNNEL=0，打印“no tunnel already”;TUNNEL=1，打印“tunnel already”;tunnel_ setup()，打印“tunnel built”; tunnel_ clean()，打印“tunnel cleaned”;

根据内部网络检测机制验证和移动 VPN 隧道验证实验过程，绘制实验结果如表 1 所示。

表 1 实验结果分析

实验步骤	内部网络检测机制	隧道机制	实验结果
1	V=1，VPN 内部，无需隧道	明文通信	正确
2	V=0，VPN 外部，需要隧道	建立隧道通信	正确
3	V=0，VPN 外部，需要隧道	重新建立隧道通信	正确
4	V=0，VPN 外部，需要隧道	重新建立隧道通信	正确
5	V=1，VPN 内部，无需隧道	拆除隧道，明文通信	正确
6	V=1，家乡网络，无需隧道	明文通信	正确

显然，本文给出的方案完全符合移动 VPN 的要求。MN 在 VPN 内部时始终能够采用明文通信，而当 MN 离开 VPN 时通信则有 IPSec 隧道的保护。

6 结束语

目前，移动 VPN 已经作为未来 3G 的一项主要业务为广大运营商所接受，可以说移动 VPN 蕴含着巨大商机。对于移动通信运营商来说，实现移动 VPN 可以借助蜂窝移动网络，也可以借助 WLAN，甚至是 WiMax。本文针对移动 IP 技术和 VPN 技术的研究旨在有效解决无线上网的安全问题，为企业和个人提供一个安全无缝的网络接入环境。

参考文献

[1] David B. A Seamless Mobile VPN Data Solution for CDMA2000, UMTS, and WLAN Users[J]. Bell Labs Technical Journal, 2002, 7(2): 143-165.

[2] Vaarala S. Mobile IPv4 Traversal Across IPsec-based VPN Gateways[S]. RFC 5265, 2005.