一种理性安全协议的博弈逻辑描述模型

刘 海[1,2] 彭长根[1,2] 张 弘[3] 任祉静[1,2]
(贵州大学理学院 贵阳 550025)[1] (贵州大学密码学与数据安全研究所 贵阳 550025)[2]
(贵州大学计算机科学与技术学院 贵阳 550025)[3]

摘 要 博弈逻辑ATL和ATEL可以对传统安全协议的公平性、安全性等性质进行分析与验证。但在理性环境中，由于参与者对知识的自利性，ATL和ATEL都不能形式化分析与验证理性安全协议。因此在CEGS中引入效用函数和偏好关系知识，得到新的rCEGS，并在合作模态算子《Γ》中加入行为ACT参数，提出新的可形式化分析理性安全协议的交替时序认知逻辑rATEL-A。然后运用rATEL-A构建两方理性安全协议的形式化模型，并基于rCEGS的等价扩展式博弈，对具体的两方理性交换协议进行形式化分析，结果表明构建的形式化模型可以有效地形式化分析理性安全协议的正确性、理性安全性和理性公平性。

关键词 ATEL，博弈论，理性安全协议，形式化分析，理性安全性，理性公平性
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.9.023

Game Logic Formal Model of Rational Secure Protocol

LIU Hai[1,2] PENG Chang-gen[1,2] ZHANG Hong[3] REN Zhi-jing[1,2]
(College of Science, Guizhou University, Guiyang 550025, China)[1]
(Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China)[2]
(College of Computer Science & Technology, Guizhou University, Guiyang 550025, China)[3]

Abstract The fairness and security properties of traditional secure protocol can be analyzed and verified by the game logics, alternating-time temporal logic and alternating-time temporal epistemic logic. However, for the formal analysis of rational secure protocol, taking players' selfishness to knowledge into consideration, ATL and ATEL can not formally analyse and verify rational secure protocol. So by introducing utility function and preference relation in the concurrent epistemic game structure, new concurrent epistemic game structure rCEGS can be gotten. By introducing action ACT parameter in the cooperation modality operator《Γ》, a novel alternating-time temporal epistemic logic rATEL-A can be gotten that can be used to formally analyse rational secure protocol. Then, rATEL-A was used to construct formal model of two-party rational secure protocol. Based on extensive form game of equivalent to rCEGS, two-party rational exchange protocol was formally analysed, which shows that the formal model can formally analyse correctness, rational security and rational fairness of rational secure protocol effectively.

Keywords Alternating-time temporal epistemic logic(ATEL), Game theory, Rational secure protocol, Formal analysis, Rational security, Rational fairness

1 引言

安全协议的形式化分析已成为研究热点，更重要的是形式化方法相当丰富。形式化方法可以表达和分析安全协议的公平性、安全性、非否认性和适时终止性等性质，不过对于理性交换协议[1]、理性秘密共享和理性安全多方计算[2]等理性安全协议的形式化分析，考虑到参与者的自利性，传统的形式化方法已不再适用。对于理性安全协议的形式化分析，交替时序逻辑(Alternating-time Temporal Logic, ATL)和交替时序认知逻辑(Alternating-time Temporal Epistemic Logic, ATEL)都不能表达理性参与者的行为与知识之间的相互关系。因此，需要基于ATEL提出适合于理性环境的新的形式化分析方法。

为了形式化分析与验证多方参与者的博弈系统性质，1997年，Rajeev Alur等[3]提出了交替时序逻辑ATL，ATL是计算树逻辑(Computation Tree Logic, CTL)的推广；1998年，Rajeev Alur等[4]基于交替转换系统(Alternating Transition System, ATS)定义了ATL的语法和语义；2002年，Ra-

到稿日期：2014-09-22 返修日期：2014-12-25 本文受国家自然科学基金项目(61262073, 61363068)，全国统计科学研究计划项目(2013LZ46)，贵州省自然科学基金项目(20092113, 20132112)，贵州省高层次人才科研条件特助经费项目(TZJF-2008-33)资助。
刘 海(1989－)，男，硕士生，主要研究方向为密码学与安全协议；彭长根(1963－)，男，博士，教授，主要研究方向为密码学与信息安全，E-mail：gzu_liuhai@163.com(通信作者)；张 弘(1964－)，男，硕士，副教授，主要研究方向为信息安全；任祉静(1989－)，女，硕士生，主要研究方向为密码学与安全协议。

jeev Alur 等[5]基于并行博弈结构(Concurrent Game Structure,CGS)定义了 ATL 的语法和语义。基于 Rajeev Alur 等提出的 ATL,安全协议的形式化分析和 ATL 扩展都得到了研究和发展。

首先基于博弈逻辑 ATL,安全协议的形式化分析研究进展如下。2005 年,针对没有形式化分析与验证许多预防拒绝服务技术和协议正确性的问题,Ajay Mahimkar 和 Vitaly Shmatikov[6]提出了新的预防恶意的带宽消耗协议,并且基于 ATS,使用 ATL 形式化描述协议的安全性,然后基于模型检测工具 MOCH 成功验证了其安全性。2006 年,文静华等[7]基于博弈的 ATL 逻辑分析电子商务协议,克服了传统时序逻辑把协议看成封闭系统进行分析的缺点。新的形式化分析方法可以成功地对电子商务协议的保密性、安全性、非否认性及公平性等进行分析。然后使用新的形式化分析方法对 Zhou-Gollmann 协议进行了形式化分析,结果表明基于博弈的 ATL 逻辑比传统 CTL 更适合于形式化描述和分析复杂的电子商务协议。接着,2008 年张梅等[8]也基于博弈的 ATL 逻辑形式化方法,对周明天等人提出的 FNORP 协议及其变式进行形式化分析,结果也表明了基于博弈的 ATL 逻辑比传统的 CTL 更适合于形式化描述和分析复杂的电子商务协议。2008 年,龙士工等[9]将一个无线安全协议模型化为 Kripke 结构,然后考虑在该结构中公式的模型检测问题,首先对 ATL 进行了扩展,提出一个有效的知识性质的 ATL 模型检测算法;接着在 2009 年定义时间 Petri 网(Timed Petri Nets,TPN)用于描述 ATL 的语义,并且得到 ATL 与 TPN 之间一种自然的关系,然后基于 TPN 和 ATL,对一个具体的例子进行了安全协议的验证[10]。2010 年,基于模型检测工具 Mocha 考虑了 ATL 博弈语义的性质规范,以及 ATL 需要制胜策略计算的模型检测问题,Zhang Ying 等[11]运用 Mocha 分析了 MR 和 MRT 协议(其中有 5 个签名者的 MR 协议是安全的,有 3 个签名者的 MRT 协议中存在攻击),并提出了解决方法;同时还设计了有 3 个和 4 个签名者的 MRT 协议,并用模型检测工具 Mocha 进行验证。2012 年,Zhang Ying 等[12]发现有 3 个签名者的 MRT 协议不满足公平性,且所有 MRT 协议存在一般的自由攻击,其对这些攻击提出了解决方法;然后设计了具有 3 个或者 4 个签名者的 MRT 协议,而且运用 Mocha 进行成功验证。2012 年,Wojciech Jamroga 等[13]基于博弈逻辑 ATL 提出了用于非否认协议与其他公平交换协议的公平性验证的两个问题,然后运用新的公平性定义解决这两个问题,还构建了各种公平定义的层次结构,并表明现有工作的相关结果。2013 年,Jiang Yun 等[14]运用一种新的基于博弈逻辑 ATL 的形式化分析方法对通信协议进行建模和分析,通过对 TMN 协议的形式化分析表明该协议不满足公平性,然后提出改进方法。

其次,基于 Rajeev Alur 等提出的 ATL,2002 年 Wiebe van der Hoek 等[15]为了解决一组参与者基于拥有的知识合作实现如何计划的认知目标,通过增加表示参与者 i 知道知识 φ 的模态算子 $K_i\varphi$ 将 ATL 推广到 ATEL,其中参与者 $i\in\Sigma$。ATEL 包括"每个参与者知道"模态算子 $E_\Gamma\varphi$ 和"共同知识"模态算子 $C_\Gamma\varphi$,其中参与者集合 $\Gamma\subset\Sigma$。不过在 ATEL 中,由于没有明确的表示行为的描述,使得一些自然情况很难被模型化。因此,Wojciech Jamroga[16]于 2004 年基于并行认知博弈结构(Concurrent Epistemic Game Structure,CEGS),在 ATEL 中引入了表示行为的描述。在此基础上,Thomas Agotnes[17]于 2006 年运用 ATEL 研究了行为和知识之间的相互关系,利用 ATEL 可以表达行为和知识之间相互关系的性质,但是理性参与者的行为与知识之间的相互关系还是很难被 ATEL 模型化。

于是为了形式化分析理性安全协议,考虑到理性参与者的自利性,基于 Thomas Agotnes 的 CEGS 和 ATEL 的语法和语义,在 CEGS 中引入效用函数[18,19]和偏好关系[20,21]知识,提出新的并行认知博弈结构 rCEGS;然后基于 rCEGS,在合作模态算子《Γ》中引入行为 ACT 参数,从而提出新的交替时序认知逻辑 rATEL-A。理性参与者由于是基于自己的知识选择行为,因此通常会最大化自己的知识,同时最小化对手的知识。所以,基于 rATEL-A 形式化描述理性参与者,使得理性安全协议的形式化分析更方便,也便于理性安全协议的形式化验证。

然后基于 rCEGS 构建两方理性安全协议的形式化模型,并运用 rATEL-A 对理性安全性、理性公平性进行建模,运用模型对具体的两方理性交换协议进行形式化描述。最后运用等价于 rCEGS 的扩展式博弈分析构建的两方理性安全协议形式化模型、理性安全性模型和理性公平性模型,并且以此形式化分析两方理性交换协议的正确性、理性安全性和理性公平性。而且,基于 rCEGS 构建的理性安全协议形式化模型可扩展到多方理性安全协议,用于对多方理性安全协议的形式化分析。所以,可以将基于 rATEL-A 的两方理性交换协议的形式化分析推广到多方理性交换协议。最后,通过将新的交替时序认知逻辑 rATEL-A 与现有的安全协议形式化分析方法进行比较,可知 rATEL-A 适合于理性安全协议的形式化分析。

2 准备知识

在这里介绍扩展式博弈和 ATEL 基础知识。

2.1 扩展式博弈

五元组 $G(q)=\langle N,H,P,(S_i^q)_{i\in N},(u_i)_{i\in N}\rangle$ 是扩展式博弈[28],状态 $q\in Q$ 表示博弈 $G(q)$ 中的每个状态,其中

- N:为参与者集合,是整数集合,$N=\{1,\cdots,k\}$;
- H:H 是一个有限的历史序列,初始空历史序列 $\varepsilon\in H$。若 $\{s_i\mid(h,s_i)\in H,s_i\in S_i^q,i\in N\}=\Phi$,那么 $h\in H$ 是终端历史序列,终端历史序列用符号 Z 表示,其中 Φ 表示空集,接下来继续用这个符号表示空集;
- P:$(H\backslash Z)\to N$ 映射每个历史序列 $h\in H\backslash Z$ 到下一个参与者;
- S_i^q:$\forall i\in N$,在状态 q 处,对于参与者 $i\in P(h)$,对历史序列 $\forall h\in H\backslash Z$ 分配有限的可利用策略集合 S_i^q。集合 $S_{G(q)}=S_1^{q_0}\times\cdots\times S_i^{q_k-1}$ 表示所有可能的策略组合,其中策略组合 $s=(s_1,\cdots,s_k)\in S_{G(q)}$,策略 $s_i\in S_i^q$;
- u_i:$Z\to R$ 是参与者 $i\in N$ 的效用函数。

事实上,一个策略是占优策略当且仅当其他参与者选定策略时,它是参与者的最佳选择策略。可形式化定义占优策略和纳什均衡。

占优策略:在扩展式博弈 $G(q)$ 中,若策略 $s_i,s_i^*\in S_i^q$ 是参与者 i 的可选策略,对于其他参与者可能的策略组合 s_{-i},参与者 i 选择策略 s_i 的效用函数值大于选择 s_i^* 的效用函数值,也就是说 $u_i(s_i^*,s_{-i})\leqslant u_i(s_i,s_{-i})$,则称 s_i 是相对于 s_i^* 的占优策略。

基于占优策略的定义，在扩展式博弈 $G(q)$ 中形式化定义纳什均衡。

纳什均衡：在 $G(q)$ 中，有策略组合 (s_i, s_{-i})，任意参与者 i 的策略 s_i 都是对其他参与者策略组合 s_{-i} 的最佳策略，也就是说 $u_i(s_i, s_{-i}) \geqslant u_i(s_i^*, s_{-i})$ 对任意 $s_i^* \in S_i^q$ 都成立，那么 (s_i, s_{-i}) 是扩展式博弈的一个纳什均衡。

于是，下面可以定义子博弈精炼纳什均衡。其中在扩展式博弈 $G(q)$ 中，$s_{i|h}$ 表示参与者 $P(h)=i$ 在历史序列为 $h \in H \backslash Z$ 下子博弈的策略，$u_{i|h}$ 表示参与者 $P(h)=i$ 在历史序列为 $h \in H \backslash Z$ 下子博弈的效用函数值。

子博弈精炼纳什均衡：在 $G(q)$ 中，任意历史序列 $h \in H \backslash Z$ 有策略组合 $(s_{i|h}, s_{-i|h})$，使得参与者 $P(h)=i$ 的策略 $s_{i|h}$ 都是对其他参与者策略组合 $s_{-i|h}$ 的最佳策略，对于参与者 i 的任意 $s_{i|h}^* \in S_{i|h}^q$，满足 $u_{i|h}(s_{i|h}, s_{-i|h}) \geqslant u_i(s_{i|h}^*, s_{-i|h})$，那么 $(s_{i|h}, s_{-i|h})$ 是扩展式博弈的一个子博弈精炼纳什均衡。

2.2 ATEL

为了形式化分析理性安全协议，基于 Thomas Agotnes 的 CEGS 和 ATEL 的语法和语义，在 CEGS 中引入效用函数和偏好关系知识，提出新的并行认知博弈结构 rCEGS。基于 rCEGS，并在合作模态算子《Γ》中引入行为 ACT 参数，提出可用于形式化分析理性安全协议的交替时序认知逻辑 rATEL-A。

3 可形式化描述理性安全协议的 rATEL-A

通过在 CEGS 中引入效用函数和偏好关系，提出新的 rCEGS，并在 ATEL 的算子《Γ》中引入行为 ACT 参数，提出可用于形式化分析理性安全协议的 rATEL-A。

3.1 rCEGS

在 CEGS $S=\langle k, Q, \Pi, \pi, ACT, d, \delta, (\sim_i)_{i\in\Sigma}\rangle$ 中引入效用函数和偏好关系知识，提出新的并行认知博弈结构 rCEGS $S_r=\langle S, (U_i)_{i\in\Sigma}, (\preceq_i)_{i\in\Sigma}, \| \cdot \|_{s_r}(q)\rangle$，其中

- Σ：参与者集合 $\Sigma=\{1,\cdots,k\}$，k 是参与者个数。
- Q：状态的有限集合。
- Π：命题的有限集合。
- π：解释函数，对于每个状态 $q \in Q$，在 q 处的真命题集合 $\pi(q) \subseteq \Pi$。
- ACT：在状态 q 处行为的有限集合。
- d：对于参与者 $i \in \Sigma$，状态 $q \in Q$，非空集合 $d_i(q) \in ACT$ 表示每个参与者 i 在状态 q 处的可利用行为。$D(q)=d_1(q)\times\cdots\times d_k(q)$ 表示所有参与者 i 在状态 q 处的联合行为的集合，其中 $a_i \in d_i(q)$，$(a_1,\cdots,a_k) \in D(q)$。
- δ：转换函数，将每个状态 $q \in Q$ 和联合行为 $(a_1,\cdots,a_k) \in D(q)$ 映射到状态 $\delta(q,a_1,\cdots,a_k) \in Q$。
- $\sim_i$：对于参与者 $i \in \Sigma$，$\sim_i \subseteq Q\times Q$ 是认知访问关系，要求每个 $\sim_i$ 是等价关系。
- $U_i: Z \to R$ 是参与者 $i \in \Sigma$ 关于终端策略序列集合 Z 的效用函数。对于有限计算 $\lambda=q_0\cdots q_m$ 和参与者 i 在状态 q_m 处的可利用行为集合 $d_i(q_m)$，有限计算 $\lambda=q_0\cdots q_m q_{m+1}$ 表示参与者 i 遵循策略 $f_i(q_0\cdots q_m) \in d_i(q_m)$ 所得的有限序列，其中策略的定义见下文。若不存在策略 $f_i(q_0\cdots q_m) \in d_i(q_m)$ 使得 $\lambda=q_0\cdots q_m q_{m+1}$，那么 $f_i(q_0\cdots q_{m-1}) \in d_i(q_{m-1})$ 是参与者 i 的终端策略，用符号 Z 表示终端策略序列组成的集合。因此，效用函数也可以是 $U_i: U_i(\lambda=q_0\cdots q_m) \to R$。
- $\preceq_i$：参与者 $i \in \Sigma$ 关于终端策略序列集合 Z 的偏好关系。
- $\| \cdot \|_{s_r}(q): f_\Gamma \to (\bigcup_{i\in N} S_i^q)$，表示在状态 $q \in Q$ 处，对于 rCEGS S_r 中的每个策略组合 f_Γ，见下文策略组合的定义，用 $\| f_\Gamma \|_{s_i}(q)$ 表示扩展式博弈 $G(q)$ 中的策略组合 s。

认知关系：若 $\Gamma \subseteq \Sigma$，用 $\sim_\Gamma^E$ 表示 Γ 的访问关系的并集，因此 $\sim_\Gamma^E=(\bigcup_{i\in\Sigma}\sim_i)$，$\sim_\Gamma^C$ 表示 $\sim_\Gamma^E$ 的闭包。在 ATEL 中，模态算子 $\sim_\Gamma^C$ 表示“共同知识”，模态算子 $\sim_\Gamma^E$ 表示“每个参与者知道的知识”。

计算：用 Q^+ 表示 Q 的非空有限序列集合。计算 $\lambda=q_0q_1\cdots$ 是状态的无限序列，其中，对于每个 $t \geqslant 0$，存在一个联合行为 $a \in D(q_t)$，使得 $\delta(q_t,a)=q_{t+1}$。从状态 q 开始的计算称为 q-计算。$\lambda[t]$ 表示 λ 中的第 t 个元素 q_t，而 $\lambda[0,t] \in Q^+$ 表示 λ 中长度为 $t+1$ 的有限前缀 $q_0q_1\cdots q_t$，$\lambda[t,\infty] \in Q^+$ 表示计算 λ 中的无限后缀 $q_tq_{t+1}\cdots$。

策略：对于参与者 i 的策略是函数 $f_i: Q^+ \to ACT$，其中 $f_i(q_0\cdots q_m) \in d_i(q_m)$。对于参与者集合 $\Gamma \subseteq \Sigma$，$Str(\Gamma)$ 表示所有策略组合的集合。策略组合 $f_\Gamma \in Str(\Gamma)$ 当且仅当 $f_\Gamma=\{f_i: i \in \Gamma\}$。

结果：给定状态 q，以及参与者集合 Γ 的一个策略组合 f_Γ，若 Γ 中的参与者遵循策略组合 f_Γ，那么 $out(q,f_\Gamma)$ 包含所有可能的 q-计算。形式化地，$\lambda \in out(q,f_\Gamma)$ 当且仅当

- $\lambda[0]=q$；
- $\forall t \geqslant 0, \exists a \in D(\lambda[0,t])$：

(i) $\forall i \in \Gamma, a_i=f_i(\lambda[0,t])$；

(ii) $\delta(\lambda[t],a)=\lambda[t+1]$。

另外，对于所有参与者的集合 Σ 可以合作唯一决定博弈系统将来的状态，因此 $out(q,f_\Sigma)$ 是唯一的。相似地，$out(q,f_\Phi)$ 表示系统所有可能的 q-计算。

效用函数和偏好关系：对于参与者 $i \in \Sigma$，$v \in U$ 表示参与者 i 至少期望可获得的效用函数值，那么理性参与者 i 获得的效用函数值 U_i 满足 $v \preceq_i U_i$。因此，为了后面形式化分析理性安全协议，将 $v \preceq_i U_i$ 看作原子命题。

另外，作为知识与行为之间的相互关系，首先是在采取行为之前需要必要的知识，其次是行为可以改变知识。因此，为了形式化分析理性安全协议，基于 rCEGS，在合作模态算子《A》中引入行为 ACT 参数，定义新的交替时序认知逻辑 rATEL-A 的语法和语义。

3.2 rATEL-A 语法

形式化地，rATEL-A 的语法是关于命题集合 Π 和参与者集合 Σ 的定义，rATEL-A 公式是下列情形之一：

(S1) $\top$ 是任意的重言式命题；

(S2) 命题 $p \in \Pi$，其中 $(v \preceq_i U_i) \in \Pi$；

(S3) $\neg\varphi$，或 $\varphi \vee \phi$，其中 φ 和 ϕ 是 rATEL-A 公式；

(S4) $\langle\Gamma, ACT\rangle\bigcirc\varphi$，$\langle\Gamma, ACT\rangle\Box\varphi$ 和 $\langle\Gamma, ACT\rangle\varphi \cup \phi$，其中参与者集合 $\Gamma \subseteq \Sigma$，ACT 是行为的有限集合，φ 和 ϕ 是 rATEL-A 公式；

(S5) $K_i\varphi$，其中参与者 $i \in \Sigma$，φ 是 rATEL-A 公式；

(S6) $E_\Gamma\varphi$ 或 $C_\Gamma\varphi$，其中参与者集合 $\Gamma \subseteq \Sigma$，φ 是 rATEL-A 公式。

rATEL-A 是 ATEL 的推广，而 ATEL 是经典命题逻辑的扩展，因此包含所有的传统连接词：$\wedge$，$\vee$，$\leftrightarrow$，$\rightarrow$ 等；另外 rATEL-A 还包含了 ATL 的时序合作模态算子《…》，以及时

序算子○(next)、□(always)、◇(eventually)和∪(until)。

对于合作模态算子《…》,以行为集合 ACT 和参与者作为参数,这样一来,就可以表达在给定行为下参与者可以实现的认知目标。也就是说,ATEL 公式《Γ》○φ 可以用《Γ,ACT》○φ 或《ACT_Γ》○φ 来表达。公式《Γ,ACT》○φ 不仅限制集合 Γ 中参与者的合法行为,而且限制了集合 Γ 以外的参与者的合法行为。类似地,ATEL 公式《Γ》□φ 和《Γ》φ∪ϕ 分别用《Γ,ACT》□φ(或《ACT_Γ》□φ)和《Γ,ACT》φ∪ϕ(或《ACT_Γ》φ∪ϕ)来表示。《Γ》◇φ 也可以表示为《Γ,ACT》◇φ(或《ACT_Γ》◇φ),并且《Γ,ACT》◇φ 与《Γ,ACT》⊤∪φ 等价。

3.3 rATEL-A 语义

对于 rATEL-A 的语义,形式化地,S_r 是 rCEGS,q 是 S_r 的状态,φ 是关于 S_r 的 rATEL-A 公式。若 φ 在 S_r 中的状态 q 处是满足的,那么记为 $S_r,q\vdash\varphi$,由于这里 S_r 是明确的,因此 S_r 可以省略,可以记为 $q\vdash\varphi$,其满足关系 ⊢ 定义如下:

- $S_r,q\vdash\top$;
- $S_r,q\vdash p\Leftrightarrow p\in\pi(q)$;
- $S_r,q\vdash\neg\varphi\Leftrightarrow S_r,q\nvdash\varphi$;
- $S_r,q\vdash\varphi_1\vee\varphi_2\Leftrightarrow S_r,q\vdash\varphi_1$ 或 $S_r,q\vdash\varphi_2$;
- $S_r,q\vdash$《Γ,ACT》○$\varphi\Leftrightarrow\exists f_i(q)\in ACT,(v\leq_i U_i)\in\Pi$, $\exists f_\Gamma\in Str(\Gamma),\forall\lambda\in out(q,f_\Gamma),S_r,\lambda[1]\vdash\varphi$;
- $S_r,q\vdash$《Γ,ACT》□$\varphi\Leftrightarrow\exists f_i(q)\in ACT,(v\leq_i U_i)\in\Pi$, $\exists f_\Gamma\in Str(\Gamma),\forall\lambda\in out(q,f_\Gamma),\forall t\geqslant 0,S_r,\lambda[t]\vdash\varphi$;
- $S_r,q\vdash$《Γ,ACT》φ∪$\phi\Leftrightarrow\exists f_i(q)\in ACT$, $(v\leq_i U_i)\in\Pi,\exists f_\Gamma\in Str(\Gamma),\forall\lambda\in out(q,f_\Gamma),\exists t\geqslant 0,S_r,\lambda[n]\vdash\phi$,且$\forall 0\leqslant t<n,S_r,\lambda[t]\vdash\varphi$;
- $S_r,q\vdash K_i\varphi\Leftrightarrow\forall q',q\sim_i q':S_r,q'\vdash\varphi$;
- $S_r,q\vdash E_\Gamma\varphi\Leftrightarrow\forall q',q\sim_\Gamma^E q':S_r,q'\vdash\varphi$;
- $S_r,q\vdash C_\Gamma\varphi\Leftrightarrow\forall q',q\sim_\Gamma^C q':S_r,q'\vdash\varphi$。

后面需要形式化分析理性安全协议,需要用到经典命题逻辑中的连接词:$\bot=\neg\top$,$\varphi\rightarrow\phi=\neg\varphi\vee\phi$,$\varphi\leftrightarrow\phi=(\varphi\rightarrow\phi)\wedge(\varphi\leftarrow\phi)$。

由于新的算子《Γ,ACT》限定了参与者在下一个状态的行为,那么满足关系 $S_r,q\vdash$《Γ,ACT》○φ 必须考虑状态 q 处每个参与者的可利用行为,包括在集合 Γ 中和集合 $\Sigma\backslash\Gamma$ 中的参与者。因此,在《Γ,ACT》○φ 情况下,存在一个联合行为 $D(q)$保证系统可以从 q 进入下一个状态。

非形式化地,《Γ,ACT》○φ 成立当且仅当:(i)所有在或者不在 Γ 中的参与者限制在 ACT 中采取行为,(ii)所有在或者不在 Γ 中的参与者被 ACT 限制,无论其他参与者做什么,Γ 可以实施行为使得 φ 在下一个状态将是正确的。

类似《Γ,ACT》○的语义,算子《Γ,ACT》□和《Γ,ACT》∪也可以在 rATEL-A 中被定义。因此,通过限制下一个状态可利用的行为,根据算子《Γ》□和《Γ》∪的不动点理论[23],那么《Γ,ACT》□和《Γ,ACT》∪的派生算子定义如下:

(i)《Γ,ACT》□$\varphi\equiv\varphi\wedge$《Γ,$ACT$》○《Γ,$ACT$》□$\varphi$;

(ii)《Γ,ACT》φ∪$\phi\equiv\phi\vee(\varphi\wedge$《Γ,$ACT$》○《Γ,$ACT$》$\varphi$∪$\phi$)。

其中,(i)、(ii)的语义解释与《Γ,ACT》○类似。

对于《Γ,ACT》◇φ,因为《Γ,ACT》◇φ 与《Γ,ACT》⊤∪φ 等价,同样可以给出算子《Γ,ACT》◇φ 的派生算子的定义。因此,对于每一个时序算子 T,ATL 算子《Γ》T 可以写为《Γ,ACT》T,其语义解释限定参与者在下一状态可利用的行为。对偶形式[[Γ,ACT]]○,[[Γ,ACT]]□,[[Γ,ACT]]◇,[[Γ,ACT]]∪的定义与对应的 ATL 对偶形式定义相同。形式化地,[[Γ,ACT]]○φ 是¬《Γ,ACT》○¬φ 的缩写,而[[Γ,ACT]]◇φ 是¬《Γ,ACT》□¬φ 的缩写,[[Γ,ACT]]□φ 是¬《Γ,ACT》◇¬φ 的缩写。

另外,对于知识和行为的相互作用关系,下面进行形式化描述。对于行为的认知前件,形式化为参与者 i 可以用一个行为 a_i 实现目标 φ,记为 K_i《i,a_i》○φ,表示参与者 i 通过实施行为 a_i 实现认知目标 φ,或者说参与者 i 知道认知目标 φ 是实施行为 a_i 的结果。

对于行为的认知后件,也可用 rATEL-A 形式化描述为《i,a_i》○$K_i\varphi$,表示实施行为 a_i 后,参与者 i 知道 φ。或者形式化描述为 K_i《i,a_i》○$K_i\varphi$,表示参与者 i 知道实施行为 a_i 后在下一个状态知道 φ。

4 rATEL-A 与扩展式博弈

在 rATEL-A 中定义均衡策略,并说明新的认知博弈结构 rCEGS S_r 与扩展式博弈的等价关系。

4.1 rATEL-A 中的均衡定义

下面基于 rATEL-A,由于在 rCEGS 中引入了效用函数和偏好关系知识命题,可以在 rCEGS 中定义纳什均衡。首先定义 rCEGS 中参与者 $i\in\Sigma$的占优策略。

定义 1(占优策略) $BR_i(f_i,f_{-i})$表示对于参与者 i,给定参与者$\Sigma\backslash i$ 的策略组合 f_{-i},那么策略 f_i 是参与者 i 的最佳选择策略。也就是说

$$BR_i(f_i,f_{-i})=\bigwedge_{f_{-i}\in Str(\Gamma)}(\text{《}f_{-i}\text{》}\Diamond(v\leq_i U_i)\rightarrow\text{《}f_i,f_{-i}\text{》}\Diamond(v\leq_i U_i))$$

定义 2(纳什均衡) 策略组合(f_i,f_{-i})是 rCEGS S_r 的一个纳什均衡,当且仅当

$$NE(f_i,f_{-i})=BR_i(f_i,f_{-i})\wedge BR_{-i}(f_{-i},f_i)$$

定义 3(子博弈精炼纳什均衡) 策略组合(f_i,f_{-i})是 rCEGS S_r 的一个子博弈精炼纳什均衡,当且仅当

$$SPNE(f_i,f_{-i})=\text{《}f_i,f_{-i}\text{》}\Box NE(f_i,f_{-i})$$

4.2 rATEL-A 与扩展式博弈等价

新的认知博弈结构 rCEGS S_r 与扩展式博弈紧密相关。由于 rATEL-A 公式《Γ,ACT》T 可转换为 ATL 公式《Γ》T,因此《Γ,ACT》○可以看作一个博弈中单个策略推理的形式化,而算子《Γ,ACT》□和《Γ,ACT》◇涉及到整个博弈的分析。所以,《Γ,ACT》○可以被理解为参与者有能力执行单个博弈,算子《Γ,ACT》□和《Γ,ACT》◇可被理解为参与者集合无限地进行博弈。因此,rATEL-A 可以根据扩展式博弈来进行解释,反之,rATEL-A 适合于推理扩展式博弈。

将扩展式博弈 $G(q)$与 rCEGS S_r 相比较,由于在 rCEGS 中引入效用函数和偏好关系知识,rCEGS 中的状态转换就是一个博弈过程,因此两个博弈结构非常相似,一是因为博弈的结果取决于参与者选择的策略,博弈的状态不是独立的;二是参与者关于结果有偏好关系,通过其效用函数来决定。

将 rCEGS $S_r=\langle S,(U_i)_{i\in\Sigma},(\leq_i)_{i\in\Sigma},\|\cdot\|_{s_r}(q)\rangle$与 $G(q)=\langle N,H,P,(S_i^q)_{i\in N},(u_i)_{i\in N}\rangle$相比较,可以认为 rCEGS S_r 与 $G(q)$等价[24,25],记为 $S_r,q\cong G(q)$,其中

- 参与者的集合是相同的:$N=\Sigma$;
- $G(q)$中的参与者 i 可利用策略 $s_i\in S_i^q$ 对应于 S_r,q 中可利用行为 $a_i=f_i(q)\in d_i(q)$,使得 $s_i=\|a_i\|_{s_r}(q)$;

·在 $G(q)$ 中的每个策略组合 $s\in S_G$，对应于 S_r 中有 $f_\Gamma\in Str(\Gamma)$，使得 $s=\|f_\Gamma\|_{s_r}(q)$；

·$\{v\leq_i U_i\,|U_i\in(u_i)_{i\in N},v\in U\}\subseteq\Pi$；

·对于所有 $f_\Gamma\in Str(\Gamma)$，$q'=\delta(q,f_\Gamma)$，使得 $(v\leq_i U_i)\in\pi(q')\Leftrightarrow u_i(\|f_\Gamma\|_{s_r}(q)=s)\geqslant v$。

定理 1 $G(q)$ 是扩展式博弈，rCEGS S_r 是含状态 q 的并行认知博弈结构，假设策略向量 $s,s'\in S_G$，参与者 $i\in\sum=N$，那么

(i) $u_i(s)>u_i(s')\Leftrightarrow\exists v\in U,S_r,\delta(q,f_\Gamma)\vdash(v\leq_i U_i)$，且 $S_r,\delta(q,f_\Gamma')\vdash\neg(v\leq_i U_i)$；

(ii) $u_i(s)\geqslant u_i(s')\Leftrightarrow\forall v\in U,S_r,\delta(q,f_\Gamma')\vdash(v\leq_i U_i)$，那么 $S_r,\delta(q,f_\Gamma)\vdash(v\leq_i U_i)$。

定理 2 $G(q)\cong S_r,q$，在 $G(q)$ 中，s_i 是参与者 $i\in N$ 的一个策略，那么 s_i 是一个占优策略当且仅当 $S_r,q\vdash BR_i(f_i,f_{-i})$。

定理 3 $G(q)\cong S_r,q$，在 $G(q)$ 中，s_i 是参与者 $i\in N$ 的一个策略，那么 (s_i,s_{-i}) 是一个纳什均衡当且仅当 $S_r,q\vdash NE(f_i,f_{-i})$。

定理 4 $G(q)\cong S_r,q$，在 $G(q)$ 中，s_i 是参与者 $i\in N$ 的一个策略，那么 (s_i,s_{-i}) 是一个子博弈精炼纳什均衡当且仅当 $S_r,q\vdash SPNE(f_i,f_{-i})$。

5 基于 rATEL-A 的理性安全协议形式化模型

在这里，为了方便理性安全协议的形式化分析，主要考虑两方理性安全协议，对理性参与者建模，并构建理性安全协议形式化模型，以及理性安全性和理性公平性的模型。可将构建的理性安全协议形式化模型推广到多方的理性安全协议，并将其用于具体的两方理性交换协议进行形式化分析，当然可扩展到多方理性交换协议的形式化分析。

(1)理性参与者建模

在理性安全协议中，根据博弈论的观点，考虑到理性参与者的自利性，非形式化描述理性参与者，理性参与者在执行协议的过程中最大化自己的收益。基于 rATEL-A，理性参与者根据自己的知识[22,26]进行选择，并且最大化自己的知识，同时最小化对手的知识。因此，运用 rATEL-A 形式化理性参与者如下：

定义 4(理性参与者) 形式化地，理性参与者可描述为：

$S_r,\lambda\vdash Rat(i,f_i)=\vee_{v\in U}(\vee_{f_j\in d_j(q)}\langle\!\langle f_i\rangle\!\rangle(Rat(j,f_j)\wedge\langle\!\langle f_i,f_j\rangle\!\rangle\Diamond(v\leq_i U_i))\wedge\wedge_{f_i\in d_i(q),f_j\in d_j(q)}\langle\!\langle f_i\rangle\!\rangle\bigcirc(Rat(j,f_j)\rightarrow\langle\!\langle f_i,f_j\rangle\!\rangle\Box\neg(v\leq_i U_i)))$

理性参与者 j 选择策略 $f_j\in d_j(q)$ 时，参与者 i 为了最大化自己的知识 $v\leq_i U_i$，最小化参与者 j 的知识，会选择最佳策略 f_i。根据定义 1，所以 $S_r,\lambda\vdash Rat(i,f_j)\bigcirc BR_i(f_i,f_j)$。但是理性参与者 j 也会出于最大化自己知识的目的，希望最小化参与者 i 的知识。因此，$S_r,\lambda\vdash(Rat(j,f_j)\rightarrow\langle\!\langle f_i,f_j\rangle\!\rangle\Box\neg(v\leq_i U_i))$。所以基于 rATEL-A，关于理性参与者的形式化描述是正确的。

(2)理性安全协议形式化建模

假设两方理性安全协议的通信是可靠的，即传输的信息不会发生延迟、丢失，并且参与者以同步的方式发送信息，且每轮只有一个参与者发送信息，另一个参与者接收信息。

基于新提出的 rCEGS S_r，运用 11 元组 $S_r=\langle S,(U_i)_{i\in\sum},(\leq_i)_{i\in\sum},\|\cdot\|_{s_r}(q)\rangle$ 来形式化描述理性安全协议，其中

·k：理性参与者个数，其集合 $\sum=\{A,B\}$。

·Q：有限状态集合，其中在状态 $q\in Q$ 处，关于每个参与者 $i\in\sum$，可执行程序 $L_i(q)=\langle d_i(q),M_i(q),r_i(q)\rangle$：

1) $d_i(q)$：参与者 i 在状态 q 处的可利用的行为；

2) $M_i(q)$：参与者 i 在状态 q 处的各种消息集合，其中 $m_i(q)\in M_i(q)$ 表示 $m_i(q)$ 是与 $M_i(q)$ 兼容的消息；

3) $r_i(q)$：在状态 q 时协议执行的轮数。

·Π：命题的有限集合，包括协议中每个状态 q 处的消息 M_q 以及物品 $item$、协议执行的轮数，以及参与者对物品 $item$ 效用函数值的偏好关系。

·π：解释函数，对于每个状态 $q\in Q$，$\pi(q)\subseteq\Pi$ 是真命题集合。

·ACT：表示参与者 $i\in\sum$ 的行为集合，并且 $ACT=\{send_i(m_q),rec_i(m_q),idle_i(q),quit_i(q)\}$，其中 $send_i(m_q)$，$rec_i(m_q)$，$idle_i(q)$，$quit_i(q)$ 分别表示参与者 $i\in\sum$ 在状态 q 处向参与者 $j\in\sum\backslash\{i\}$ 发送消息 $m_q\in M_q$，在状态 q 处收到参与者 $j\in\sum\backslash\{i\}$ 向 i 发送的消息 $m_q\in M_q$，在状态 q 处什么也不做，在状态 q 处终止协议。

·d：$d_i(q)\subseteq ACT$，$D(q)=d_1(q)\times\cdots\times d_n(q)$。其中：

1)若参与者 $i\in\sum$ 在状态 q 处执行行为 $idle_i(q)$，那么每个参与者 $j\in\sum\backslash\{i\}$ 仍然处于状态 q 处，也就是说 $S_r,q\vdash\langle\!\langle idle_i\rangle\!\rangle\bigcirc(L_j(q,idle_i)=L_j(q))$；

2)若参与者 $i\in\sum$ 在状态 q 处执行行为 $quit_i(q)$，那么对于每个参与者 $j\in\sum\backslash\{i\}$，则有：

$S_r,q\vdash\langle\!\langle quit_i(q)\rangle\!\rangle\bigcirc\perp$

$S_r,q\vdash\langle\!\langle quit_i\rangle\!\rangle\bigcirc(L_i(q,quit_i)=L_i(q))$

$S_r,q\vdash\langle\!\langle quit_i\rangle\!\rangle\bigcirc(r_i(q,quit_i)=r_i(q))$

$S_r,q\vdash\langle\!\langle quit_i\rangle\!\rangle\bigcirc(L_j(q,quit_i)=L_j(q))$

3)若参与者 $i\in\sum$ 在状态 q 处执行行为 $send_i(m_q)$，那么对于每个参与者 $j\in\sum\backslash\{i\}$，则有：

$S_r,q\vdash\langle\!\langle send_i\rangle\!\rangle\bigcirc\top$

$S_r,q\vdash\langle\!\langle send_i\rangle\!\rangle\bigcirc(L_i(q,send_i(m_q))=L_i(q)\cup rec_i(m_q))$

$S_r,q\vdash\langle\!\langle send_i\rangle\!\rangle\bigcirc(r_i(q,send_i(m_q))=r_i(q)+1)$

·δ：状态 $q\in Q$，联合行为 $a\in D(q)$，也就是说 $\delta(q,a)\in Q$。

·$\sim_i$：对于参与者 i，若 q 和 q' 是不可区分的两个状态，要求 $q\sim_i q'$。

·U_i：对于有限状态计算 $\lambda=q_1\cdots q_n$，理性参与者期望的效用函数为 $U_i(\lambda)=U_i^+(\lambda)-U_i^-(\lambda)$，其中，$S_r,\lambda\vdash(rev_i(item_j))\bigcirc\top$ 表示参与者 $i\in\sum$ 获得 $item_j$，其中 $j\in\sum\backslash\{i\}$，相应的效用函数为 $U_i^+(\lambda)$；$S_r,\lambda\vdash(send_i(item_i))\bigcirc\top$ 表示参与者 $i\in\sum$ 失去对 $item_i$ 的控制，相应的效用函数为 $U_i^-(\lambda)$。

·$\leq_i$：对于有限计算 λ，命题 $(v\leq_i U_i(\lambda))\in\Pi$。

·$\|\cdot\|_{s_r}(q):f_\Gamma\rightarrow(\bigcup_{i\in N}S_i^q)$，表示在状态 $q\in Q$ 处，对于 S_r 中的每个策略组合 f_Γ，用 $\|f_\Gamma\|_r(q)$ 表示理性安全协议扩展式博弈 $G(q)$ 中策略组合 s。

(3)理性安全性建模

在构建的理性安全性式化模型基础上，如果理性安全协议是安全的，理性攻击者采取任何攻击行为都不能获得理性安全协议中传输的任何信息，也就是说理性攻击者所获得的效用函数值为 0。因此，运用 rATEL-A 形式化表示如下：

$S_r,q\vdash\langle\!\langle Attac,ACT\rangle\!\rangle\Diamond\neg(0<_{Attac}U_{Attac})$

其中，$Attac$ 表示理性攻击者，ACT 表示理性攻击者 $Attac$ 的任意攻击行为，其中 $\prec_{Attac}$ 表示理性攻击者 $Attac$ 的严格偏好关系。理性攻击者 $Attac$ 通过采取攻击行为 ACT 获得期望的消息或物品，但是理性安全协议是安全的，所以理性攻击者 $Attac$ 采取任意的攻击行为 ACT 都无法获得期望的消息和物品，即就是理性攻击者 $Attac$ 不能获得期望的效用函数值 U_{Attac}。因此在状态 q 处，下面理性安全协议的形式化模型 S_r 的满足关系成立：

$S_r, q \models \langle\langle Attac, ACT\rangle\rangle \Diamond \neg (0 \prec_{Attac} U_{Attac})$

(4)理性公平性建模

在构建的理性安全性式化模型基础上，需要形式化理性安全协议的公平性[27]。由于自利性，参与者都希望获得自己期望的物品，或者期望其他参与者都没有获得期望的物品。那么基于 rCEGS，可以对理性公平性建模，形式化如下：

定义 5(理性公平性) 在 S_r 中，形式化两方理性安全协议参与者的公平性，可描述为：

(i)若 (f_i, f_j) 是 S_r 的纳什均衡，若参与者都没有获得期望的物品，当且仅当 $S_r, q \models NE\langle\langle f_i, f_j\rangle\rangle \rightarrow \langle\langle f_i, f_j\rangle\rangle \bigcirc ((U_i = 0 \leq_i v) \wedge (U_j = 0 \leq_j v))$。

(ii)若 (f_i, f_j) 是 S_r 的纳什均衡，若参与者都获得了期望的物品，当且仅当 $S_r, q \models NE\langle\langle f_i, f_j\rangle\rangle \rightarrow \langle\langle f_i, f_j\rangle\rangle \bigcirc ((v \leq_i U_i = U_i^+ - U_i^-) \wedge (v \leq_j U_j = U_j^+ - U_j^-))$。

(5)理性安全协议形式化模型分析

对于理性安全协议的形式化模型，利用与 rCEGS 等价的扩展式博弈 $G(q)$ 进行分析。建立理性安全协议形式化模型 S_r, q 的扩展式博弈 $G(q)$，如图 1 所示。

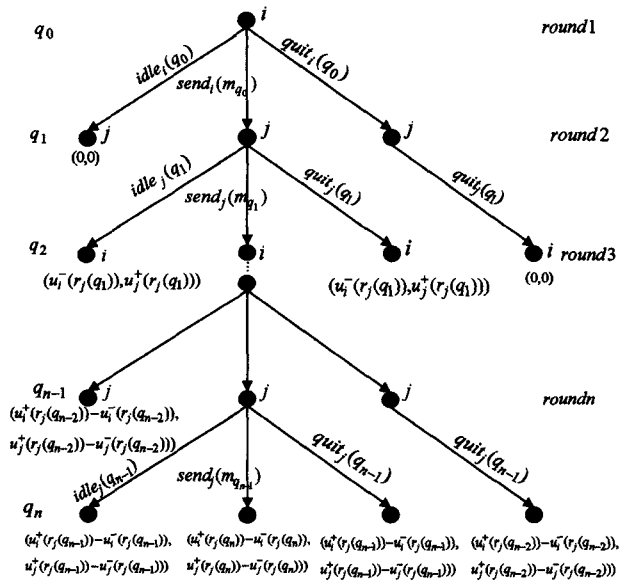

图 1 理性安全协议形式化模型的扩展式博弈

考虑参与者 i, j 的自利性，在扩展式博弈 $G(q)$ 中，要求理性安全协议交替执行 $r_j(q_{n-1}) = n$ 轮，参与者 i, j 才能获得期望的完整物品，即对于参与者 $i \in \sum$，协议在 $r_i(q_t)(1 \leq r_i(q_t) \leq n, 0 \leq t \leq n-1)$ 轮只能获得物品的一部分。因此，执行理性安全协议相当于交替执行 n 个分布式程序 $L_i(q_0), L_j(q_1), \cdots, L_{j-1}(q_{n-1})$。

在状态 q_0 处，参与者 i 执行程序 $L_i(q_0) = \langle d_i(q_0), M_i(q_0), r_i(q_0)\rangle$：

1) $d_i(q_0) = \{idle_i(q_0), quit_i(q_0), send_i(m_{q_0})\}, m_{q_0} \in M_{q_0}$；

2) $a_1 \in d_i(q_0), \delta(q_0, a_1) = q_1, r_i(q_0) = 1$；

3) $\| a_1 \|_{s_r}(q_0) = s_1$。

在状态 q_1 处，参与者 j 执行 $L_j(q_1) = \langle d_j(q_1), M_j(q_1), r_j(q_1)\rangle$：

1) $d_j(q_1) = \{idle_j(q_1), quit_j(q_1), send_j(m_{q_1})\}, m_{q_1} \in M_{q_1}$；

2) $a_2 \in d_j(q_1), \delta(q_1, a_2) = q_2, r_j(q_1) = 2$；

3) $\| a_2 \|_{s_r}(q_1) = s_2$。

依次类推，在状态 q_{n-1} 处，参与者 j 执行 $L_j(q_{n-1}) = \langle d_j(q_{n-1}), M_j(q_{n-1}), r_j(q_{n-1})\rangle$：

1) $d_j(q_{n-1}) = \{idle_j(q_{n-1}), quit_j(q_{n-1}), send_j(m_{q_{n-1}})\}, m_{q_{n-1}} \in M_{q_{n-1}}$；

2) $a_n \in d_j(q_{n-1}), \delta(q_{n-1}, a_n) = q_n, r_j(q_{n-1}) = n$；

3) $\| a_n \|_{s_r}(q_{n-1}) = s_n$。

在状态 q_n 处，由于理性安全协议在状态 q_{n-1} 处已交替执行完 n 轮，参与者 i, j 不再执行任何程序。

对应于理性安全协议的形式化描述，在每个状态 $q \in Q$ 处，对应于扩展式博弈 $G(q)$ 的第 $r_t(q) = round\Delta (t \in \sum, 1 \leq \Delta \leq n)$ 轮，其中 $round\Delta$ 表示博弈执行第 Δ 轮。

在 $round1$ 时，参与者 i 执行博弈 $G(q_0) = \langle p(\varepsilon), S_i^{q_0}(\varepsilon), h_1\rangle$：

1) $i = p(\varepsilon)$；

2) $S_i^{q_0}(\varepsilon) = \{idle(q_0), quit(q_0), send(m_{q_0})\}$；

3) $s_1 \in S_i^{q_0}(\varepsilon), h_1 = (s_1)$。

在 $round2$ 时，参与者 j 执行博弈 $G(q_1) = \langle p(h_1), S_j^{q_1}(h_1), h_2\rangle$：

1) $j = p(h_1)$；

2) $S_j^{q_1}(h_1) = \{idle(q_1), quit(q_1), send(m_{q_1})\}$；

3) $s_2 \in S_i^{q_1}, h_2 = (s_1, s_2)$。

类似地，在 $roundn$ 时，参与者 j 执行博弈 $G(q_{n-1}) = \langle p(h_{n-1}), S_j^{q_{n-1}}(h_{n-1}), h_n\rangle$：

1) $j = p(h_{n-1})$；

2) $S_j^{q_{n-1}}(h_{n-1}) = \{idle(q_{n-1}), quit(q_{n-1}), send(m_{q_{n-1}})\}$；

3) $s_n \in S_i^{q_{n-1}}, h_n = (s_1, s_2, \cdots, s_n)$。

首先如果参与者 i, j 在理性安全协议形式化模型中，出于理性的考虑，当参与者 i 执行策略 $quit_i(q_0)$ 时，那么参与者 j 执行策略 $quit_j(q_1)$，由定义 5(i)可知：

$S_r, q \models \langle\langle quit_i(q_0), quit_j(q_1)\rangle\rangle \bigcirc ((U_i = 0 \leq_i v) \wedge (U_j = 0 \leq_j v))$。

那么理性安全协议形式化模型满足正确性和公平性。

其次，在扩展式博弈 $G(q)$ 中，由于参与者 i, j 是理性参与者，在执行理性安全协议的分布式程序时，选择最大化自己知识的占优策略，都会按协议既定规则执行完所有程序。根据逆向归纳法，在协议执行轮数为 $r_j(q_{n-1}) = n$ 时，显然对于参与者 j 来说，其获得的效用函数值 $u_j^+(r_j(q_n)) - u_j^-(r_j(q_n))$，其中都大于所获得的效用函数值 $u_j^+(r_j(q_{n-1})) - u_j^-(r_j(q_{n-1}))$ 和 $u_j^+(r_j(q_{n-2})) - u_j^-(r_j(q_{n-2}))$，因此参与者 j 会选择策略 $send_j(m_{q_{n-1}})$，根据定理 4，以此逆向类推，参与者 i 会选择占优策略 $send_i(m_{q_{n-1}})$。根据定理 3，策略组合 $s = (send_i(m_{q_0}), send_j(m_{q_1}), \cdots, send_j(m_{q_{n-1}}))$ 是纳什均衡，那么在 S_r, q 中 $\| f_\Gamma \|_{s_r}(q) = s$，所以 $f_\Gamma = (send_i(m_{q_0}), send_j(m_{q_1}), \cdots, send_j(m_{q_{n-1}}))$。

因此根据定理 3 可得到均衡解，$S_r, q = NE\langle\langle send_i(m_{q_0}), send_j(m_{q_1}), \cdots, send_j(m_{q_{n-1}})\rangle\rangle$。那么对应的效用函数值组合 $(u_i^+(r_i(q_n)) - u_i^-(r_i(q_n)) \geqslant v, u_j^+(r_j(q_n)) - u_j^-(r_j(q_n)) \geqslant v)$ 是参与者 i, j 的认知目标，所以根据理性公平性定义 5(ii)可知：

$S_r, q = NE\langle\langle send_i(m_{q_0}), send_j(m_{q_1}), \cdots, send_j(m_{q_{n-1}})\rangle\rangle \bigcirc((v \leq_i U_i = U_i^+(r_i(q_n)) - U_i^-(r_i(q_n))) \wedge (v \leq_j U_j = U_j^+(r_j(q_n)) - U_j^-(r_j(q_n)))$

因此，由于参与者的自利性，根据最大化自己的知识，进而使得协议达到纳什均衡解的状态，因此参与者 i 和 j 通过执行策略组合 $(send_i(m_{q_0}), send_j(m_{q_1}), \cdots, send_j(m_{q_{n-1}}))$ 获得各自期望的物品，所以理性安全协议形式化模型满足正确性和公平性。

6 理性交换协议的形式化分析

基于 rATEL-A，根据理性安全协议形式化模型，对理性交换协议的公平性和安全性进行形式化分析。

6.1 Syverson's 理性交换协议

在 1998 年，Syverson 首次提出了理性交换协议，他利用了一种叫做弱比特承诺(Weakly Secret Bit Commitment，WS-BC)的密码技术设计了一个可用于小额支付的理性交换协议，如图 2 所示。

$A \rightarrow B: m_1 = (desc_A, enc(key, item_A), w(key), \sigma_1)$

$B \rightarrow A: m_2 = (item_B, m_1, \sigma_2)$

$A \rightarrow B: m_3 = (key, m_2, \sigma_3)$

$\sigma_1 = sig(k_A^{-1}, enc(key, item_A), w(key))$

$\sigma_2 = sig(k_B^{-1}, (item_B, m_1))$

$\sigma_3 = sig(k_A^{-1}, (key, m_2))$

图 2 Syverson's 理性交换协议

其中，A 和 B 表示理性参与者，$A \rightarrow B$ 表示参与者 A 向参与者 B 发送消息，反之亦然。m_1 和 m_3 是由 A 发给 B 的消息，m_2 是 B 发给 A 的消息。$item_A$ 和 $item_B$ 表示交换的物品。$desc_A$ 表示对 $item_A$ 的描述，因为该协议是一个支付交换协议，而 $item_B$ 在协议中实际上作为购买 $item_A$ 的支付款项，所以不需要对 $item_B$ 进行描述。key 是随机产生的秘密密钥，$enc(key, item_A)$ 表示用对称密钥 key 对 $item_A$ 进行加密的对称加密算法。弱比特承诺 $w(key)$ 是表示在可接受的时间之内，参与者可以获得秘密密钥 key。k_A^{-1} 和 k_B^{-1} 分别是 A 和 B 的私钥，对应的公钥分别为 k_A, k_B。$sig(k_i^{-1}, m)$ 表示用私钥 $k_i^{-1}(i \in \{A, B\})$ 对消息 m 进行数字签名。在此协议中所有发送的消息都是发送方的数字签名，以防止伪造和否认发生。因此，σ_1 和 σ_3 是参与者 A 对消息 m_1 和 m_3 的数字签名，σ_2 是参与者 B 对消息 m_2 的数字签名。

6.2 理性安全性分析

在执行理性交换协议的过程中，首先基于弱比特承诺密码技术，理性参与者 A 向理性参与者 B 发送消息 m_1，由于 m_1 包含物品 $item_A$ 的描述和用秘密密钥 key 对物品 $item_A$ 的加密，以及用私钥 k_A^{-1} 对它们的签名，因此 B 可以确认消息 m_1 是由参与者 A 所发送。其次，参与者 B 向 A 发送消息 m_2，m_2 包含消息 m_1 和物品 $item_B$ 以及用私钥 k_B^{-1} 对它们的签名，同样 A 确认消息 m_2 是由参与者 B 所发送，并且 A 获得物品 $item_B$。所以，执行完这两个过程后，参与者 A 和 B 实现相互认证。然后进行第三个过程，即 A 向 B 发送消息 m_3，消息 m_3 包括消息 m_2 和秘密密钥 key，使得 B 获得秘密密钥 key，进而解密密文 $enc(key, item_A)$，获得物品 $item_A$。

虽然理性交换协议可以实现相互认证，实现物品的交换，但是在协议执行的第一阶段存在重放攻击。假设理性参与者 A 和 B 都是诚实的，攻击者 $Attac$ 采取攻击行为 ACT 代替参与者 A 向 B 发送消息 m_1，参与者 B 对消息 m_1 进行认证，相信是 A 所发送的消息，由于弱比特承诺密码技术，参与者 B 必须向参与者 A 发送消息 m_2，由此理性攻击者 $Attac$ 获得期望的物品 $item_B$，所以有

$S_r, q \models \langle\langle Attac, ACT\rangle\rangle \Diamond (0 \prec_{Attac} U_{Attac})$

所以理性交换协议不满足理性安全性的模型。于是为了防止重放攻击，在理性交换协议的消息 m_1 和 m_3 中加入参与者 A 的身份标识 ID_A，在消息 m_2 中加入参与者 B 的身份标识 ID_B。

在理性交换协议执行过程中，由于弱比特承诺密码技术，理性参与者 B 必须向参与者 A 发送消息 m_2。但如果理性参与者 A 不是诚实的，参与者 A 在第一阶段可能会发送假消息，其中 $garbage(m_1)$ 表示消息 m_1 是假消息，这样就有

$S_r, q \models \langle\langle send_A(garbage(m_1), send_B(m_2)\rangle\rangle \Diamond ((v \prec_A U_A) \wedge (U_B \prec_B 0))$

于是，为了激励参与者 A 诚实地执行理性交换协议，防止其发送假消息，额外给参与者 A 一个惩罚值 F_A，并且要求 $F_A > U_A$，这样就保证了理性交换协议的正常执行。

6.3 正确性和理性公平性分析

对理性交换协议进行形式化描述，图 3 所示为理性交换协议的扩展式博弈。理性交换协议的执行可以看作 3 个分布式程序 $L_A(q_0), L_B(q_1), L_A(q_2)$ 的交替执行。

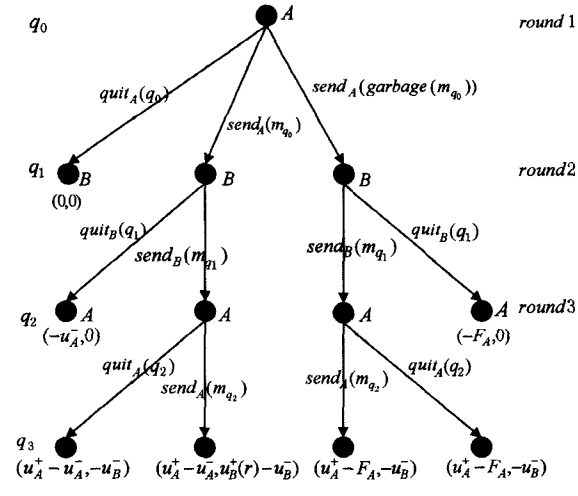

图 3 理性交换协议的扩展式博弈

相应地，在状态 q_0 处，参与者 A 执行程序 $L_A(q_0) = \langle d_A(q_0), M_A(q_0), r_A(q_0)\rangle$：

1) $d_A(q_0) = \{quit_A(q_0), send_A(m_{q_0}), send_A(garbage(m_{q_0}))\}$；

2) $a_1 \in d_A(q_0), \delta(q_0, a_1) = q_1, r_A(q_0) = 1$；

3) $\| a_1 \|_{S_r}(q_0) = s_1$。

在状态 q_1 处，参与者 B 执行程序 $L_B(q_1) = \langle d_B(q_1), M_B(q_1), r_B(q_1)\rangle$：

1) $d_B(q_1) = \{quit_B(q_1), send_B(m_{q_1})\}$；

2) $a_2 \in d_B(q_1), \delta(q_1, a_2) = q_2, r_B(q_1) = 2$；

3) $\| a_2 \| s_r(q_1)=s_2$。

在状态 q_2 处，参与者 B 执行程序 $L_A(q_2)=\langle d_A(q_2), M_A(q_2), r_A(q_2)\rangle$：

1) $d_A(q_2)=\{quit_A(q_2), send_A(m_{q_2}), send_A(garbage(m_{q_2}))\}$；

2) $a_3\in d_A(q_2), \delta(q_2,a_3)=q_3, r_A(q_2)=3$；

3) $\| a_3 \| s_r(q_3)=s_3$。

在状态 q_3 处，由于理性交换协议在状态 q_2 处已交替执行完第 3 轮，参与者 A,B 不再执行任何程序。

在理性交换协议的扩展式博弈中，博弈需要进行 3 轮，其中 $m_1=send_A(m_{q_0}), m_2=send_B(m_{q_1}), m_3=send_A(m_{q_2})$。那么对应于理性交换协议的形式化模型，每轮参与者 A,B 执行博弈如下。

在 *round*1 时，参与者 A 执行博弈 $G(q_0)=\langle p(\varepsilon), S_A^{q_0}(\varepsilon), h_1\rangle$：

1) $A=p(\varepsilon)$；

2) $S_A^{q_0}(\varepsilon)=\{idle_A(q_0), quit_A(q_0), send_A(m_{q_0})\}$；

3) $s_1\in S_A^{q_0}(\varepsilon), h_1=(s_1)$。

在 *round*2 时，参与者 B 执行博弈 $G(q_1)=\langle p(h_1), S_B^{q_1}(h_1), h_2\rangle$：

1) $B=p(h_1)$；

2) $S_B^{q_1}(h_1)=\{idle_B(q_1), quit_B(q_1), send_B(m_{q_1})\}$；

3) $s_2\in S_B^{q_1}, h_2=(s_1,s_2)$。

在 *round*3 时，参与者 A 执行博弈 $G(q_2)=\langle p(h_2), S_A^{q_2}(h_2), h_2\rangle$：

1) $A=p(h_2)$；

2) $S_A^{q_2}(h_2)=\{idle_A(q_2), quit_A(q_2), send_A(m_{q_2})\}$；

3) $s_3\in S_A^{q_2}, h_3=(s_1,s_2,s_3)$。

由于参与者在执行交换协议的过程中期望最大化自己的效用函数值，因此，基于 rATEL-A 的定义 5，形式化理性交换协议的所达到的理性公平性均衡解状态，即

$$S_r,q\vdash NE\langle\langle send_A(m_{q_0}), send_B(m_{q_1}), send_A(m_{q_2})\rangle\rangle\rightarrow\langle\langle send_A(m_{q_0}), send_B(m_{q_1}), send_A(m_{q_2})\rangle\rangle\bigcirc((v\leq_A U_A=U_A^{+}-U_A^{-})\wedge(v\leq_B U_B=U_B^{+}-U_B^{-}))$$

基于等价于 S_r,q 的扩展式博弈 $G(q)$，对理性交换协议的理性公平性均衡解状态进行分析。根据逆向归纳法，由定理 4 可知，在 *round*3 时，对于参与者 A 来说选择博弈树左边的策略 $quit_A(q_2)$ 和 $send_A(m_{q_2})$ 所获效用函数值比博弈树右边的效用函数值大；在 *round*2 时，对于参与者 B 而言，选择博弈树左边的策略 $send_B(m_{q_1})$ 所获得的效用函数值比选择其他策略的效用函数值都大；最后在 *round*1 时，因为只有参与者 A 执行了策略 $send_A(m_{q_0})$ 后，参与者 B 才能在 *round*2 时选择策略 $send_B(m_{q_1})$ 使得自己的效用函数值最大，直到 *round*3 结束时，根据定理 3，理性交换协议的扩展式博弈达到策略组合 $(send_A(m_{q_0}), send_B(m_{q_1}), send_A(m_{q_2}))$ 均衡状态，使得 A 和 B 都获得了期望的物品，所以理性交换协议满足正确性和理性公平性。

同样地，如果参与者 A 和 B 在协议执行过程中都选择 *quit* 策略，那么参与者 A 和 B 都没有获得所期望的物品，同样满足正确性和理性公平性，其中理性公平性形式化如下：

$$S_r,q\vdash NE\langle\langle quit_A(q_0), quit_B(q_1)\rangle\rangle\rightarrow\langle\langle quit_A(q_0), quit_B(q_1)\rangle\rangle\bigcirc((U_A=0\leq_A v)\wedge(U_B=0\leq_B v))$$

7 形式化分析方法比较

在文献[29]中，薛瑞等将安全协议的形式化分析方法分为 3 类：模态逻辑，模型检测，定理证明。这里把形式化分析方法 ATL、ATEL 和 rATEL-A 归为博弈逻辑类型，在表 1 中对各种类型的形式化分析方法进行了比较。由此可知，新的交替时序逻辑 rATEL-A 适合于理性安全协议的形式化分析。

表 1 形式化分析方法比较

类型	形式化分析方法	安全协议类型	形式化分析性质	优点	缺点
模态逻辑	BAN 逻辑 BAN 类逻辑	安全协议	认证性 认证性 保密性 非否认性	简单直观，易于掌握，命题与推理规则与自然语言相似	语义不完备，无法检测协议存在的某些安全缺陷
模型检测	Petri 网 有限状态机 SMV	安全协议	安全性	自动化验证技术，自动产生反例验证协议存在的缺陷	存在状态空间爆炸问题，协议参与者的数目受到限定
定理证明	Paulson 归纳法 串空间模型 SPI 演算	安全协议	正确性 安全性	证明安全协议满足安全属性，参与者数目不受限定，不存在状态空间爆炸问题	证明步骤多，过程复杂，对使用者水平要求高，自动化验证困难
博弈逻辑	ATL ATEL	安全协议	保密性 安全性 公平性 非否认性 适时终止性	形式化描述多方参与者博弈系统，参与者可以选择相应的策略行为，相应的模型检测工具为 Mocha	无法描述理性参与者的策略行为与知识之间的相互关系
	rATEL-A	理性安全协议	正确性 理性公平性 理性安全性	形式化描述多方参与者博弈系统，理性参与者根据效用函数和偏好关系知识，选择相应的策略行为	没有相应的模型检测和仿真工具，需要对模型检测工具 Mocha 作进一步改进

结束语 为了形式化分析理性安全协议，基于 ATEL，在 CEGS 中引入效用函数和偏好关系知识，提出新的并行认知博弈结构 rCEGS；通过在 ATEL 的合作模态算子《Γ》中引入策略参数 ACT，提出 rATEL-A；基于 rATEL-A 构建两方理性安全协议形式化模型，并用等价的扩展式博弈分析两方理性安全协议的形式化模型的安全性、正确性以及公平性。运用所构建的两方理性安全协议形式化模型，通过对具体的两方理性交换协议进行形式化，分析其理性安全性和正确性以及理性公平性。进一步分析所构建的两方理性安全协议的形式化模型，表明其可以扩展到对多方理性安全协议的形式化模型，进而可以运用所构建的多方理性安全协议形式化模型有效地形式化分析多方理性安全协议的理性安全性、正确性

和理性公平性。将博弈逻辑 rATEL-A 与现有的形式化分析方法进行对比，以此说明 rATEL-A 适合理性安全协议的形式化分析。下一步将探讨 rATEL-A 的公理化系统和模型检测和仿真工具，并用公理化系统来形式化分析与验证理性安全协议的理性安全性、正确性和理性公平性等性质，并对其进行模拟仿真。

参 考 文 献

[1] Syverson P. Weakly secret bit commitment: applications to lotteries and fair exchange[C]// Proceedings of 11th IEEE Computer Security Foundations Workshop. United States: IEEE, 1998: 2-13

[2] Halpern J, Teague V. Rational secret sharing and multiparty computation: extended abstract[C]// Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing (STOC'04). New York: ACM, 2004: 623-632

[3] Alur R, Henzinger T, Kupferman O. Alternating-time temporal logic[C]// 38th Annual Symposium on Foundations of Computer Science. United States: IEEE, 1997: 100-109

[4] Alur R, Henzinger T, Kupferman O. Alternating-time temporal logic[M]. Springer Berlin Heidelberg, 1998: 23-60

[5] Alur R, Henzinger T, Kupferman O. Alternating-time temporal logic[J]. Journal of The ACM(JACM), 2002, 9(5): 672-713

[6] Mahimkar A, Shmatikov V. Game-Based Analysis of Denial-of-Service Prevention Protocols[C]// Proceedings of the 18th IEEE Computer Security Foundations Workshop(CSFW'05). United States: Institute of Electrical and Electronics Engineers Computer Society, 2005: 287-301

[7] 文静华，张梅，李祥. 基于博弈的电子商务协议分析[J]. 通信学报，2006，27(3)：73-78
Wen Jing-hua, Zhang Mei, Li Xiang. Formal Analysis of E-commerce Protocols Based on Game[J]. Journal on Communications, 2006, 27(3): 73-78

[8] 张梅，文静华，张焕国. 基于 ATL 方法的电子商务协议 FONRP 分析[J]. 计算机工程，2008，34(3)：151-153
Zhang Mei, Wen Jing-hua, Zhang Huan-guo. Analysis of E-commerce Protocol FONRP Based on ATL[J]. Computer Engineering, 2008, 34(3): 151-153

[9] Long Shi-gong, Luo Wen-jun. Model Checking Alternating-time Temporal Logics of Knowledge[C]// 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008(WiCOM'08). United States: IEEE, 2008: 1-3

[10] Long Shi-gong. Protocol Analysis Through Alternating-time Temporal Logic and Timed Petri Net Models[C]// 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009 (WiCom'09). United States: IEEE, 2009: 1-4

[11] Zhang Ying, Zhang Chen-yi, Pang Jun, et al. Game-based Verification of Multi-party Contract Signing Protocols[M]// Formal Aspects in Security and Trust. Springer, 2010: 186-200

[12] Zhang Ying, Zhang Chen-yi, Pang Jun, et al. Game-based Verification of Contract Signing Protocols with Minimal Messages [J]. Innovations in Systems and Software Engineering, 2012, 8 (2): 111-124

[13] Jamroga W, Mauw S, Melissen M. Fairness in Non-Repudiation Protocols[M]// Security and Trust Management. Springer, 2012: 122-139

[14] Jiang Yun, Gong Hua-ping. Modeling and Formal Analysis of Communication Protocols Based on Game[J]. Information Technology Journal, 2012, 12(3): 470-473

[15] Van Der Hoek W, Wooldridge M. Tractable multiagent planning for epistemic goals[C]// Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 3(AAMAS'02). New York: ACM, 2002: 1167-1174

[16] Jamroga W. Some remarks on alternating temporal epistemic logic[C]// Proceedings of Formal Approaches to Multi-Agent Systems(FAMAS 2003). 2004

[17] Agotnes T. Action and knowledge in alternating-time temporal logic[J]. Synthese, 2006, 149(2): 375-407

[18] Buttyan L, Hubaux J, Capkun S. A formal model of rational exchange and its application to the analysis of syverson's protocol [J]. Journal of Computer Security-JCS, 2004, 12(3/4): 551-587

[19] Alcide A. Rational exchange protocols[D]. Leganés: Universidad Carlos III Department, 2008

[20] Van Otterloo S, Van Der Hoek W, Wooldridge M. Preferences in game logics[C]// Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'04). United States: IEEE, 2004: 152-159

[21] Van Benthem J, Van Otterloo S, Roy O. Preference Logic, Conditionals and Solution Concepts in Games[M]// Lindström S, Lagerlund H, Sliwinski R, eds. Modality matters. Festschrift for krister segerberg, University of Uppsala, 2005: 61-67

[22] Walther D, Van Der Hoek W, Wooldridge M. Alternating-time temporal logic with explicit strategies[C]// Proceedings of the 11th Conference on Theoretical Aspects of Rationality and Knowledge(TARK'07). New York: ACM, 2007: 269-278

[23] Goranko V, Van Drimmelen G. Complete axiomatization and decidability of alternating-time temporal logic [J]. Theoretical Computer Science-TCS, 2006, 353(1-3): 93-117

[24] Goranko V. Coalition games and alternating temporal logics [C]// Proceedings of the 8th Conference on Theoretical Aspects of Rationality and Knowledge (TARK'01). San Francisco: Morgan Kaufmann Publishers Inc, 2001: 259-272

[25] Van Der Hoek W, Jamroga W, Wooldridge M. A logic for strategic reasoning[C]// Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'05). New York: ACM, 2005: 157-164

[26] Van Der Hoek W, Wooldridge M. Cooperation, knowledge, and time: alternating-time temporal epistemic logic and its applications[J]. Studia Logica-An International Journal for Symbolic Logic-SLOGICA, 2003, 75(1): 125-157

[27] Buttyan L, Hubanux J. Toward a formal model of fair exchange——a game theoretic approach[R]. Switzerland: Swiss Federal Institute of Technology, 2000

[28] Canetti R, Rosen A. Cryptography and Game Theory[M/OL]. 2009. http://www.cs.tau.ac.il/~canetti/f09-cgt.html

[29] 薛瑞，冯登国. 安全协议的形式化分析技术与方法[J]. 计算机学报，2006，29(1)：1-20
Xue Rui, Feng Deng-guo. The Approaches and Technologies for Formal Verification of Security Protocols[J]. Chinese Journal of Computers, 2006, 29(1): 1-20

[30] 徐亮，余建平. 改进的验证正确性 ACTL 性质的限界模型检测方法[J]. 计算机科学，2013，40(6A)：99-102
Xu Liang, Yu Jian-ping. Improved Bounded Model Checking on Verification of Valid ACTL Properties[J]. Computer Science, 2013, 40(6A): 99-102

(下转第 143 页)

后于 Greedy、Ordinal 策略，通过分析可以认为是由于曲线(3)(4)带有预制计算节点的功能，其对负载的波动有一定的预判、吸收作用，因此当 PV 指标的斜率开始攀升时，策略(3)(4)仍可保持较好的适应能力，Finishedtime 指标几乎没有受到干扰。但 C 点之后，由于绝对数量的增大，负载量开始逼近系统所能承受的范围，导致预制量没有紧紧跟随任务量的增长，系统整体的响应时间被拉长。在图 4(b)中，曲线(3)(4)的绝对差值变大且拐点 D 出现的位置发生后移，这是由于增大系统单位时间有效部署计算节点的能力，可在应对绝对任务数的增大问题方面有积极的作用，可有效提升系统应对大任务量环境的能力。综合分析图 3、图 4 可以得出结论：AF-HW 模型对 Allocationspan、Finishedtime 指标的贡献均优于优化前的系统，该模型可有效地提升系统单点与整体的性能表现。

结束语 为了使云计算系统能有效地应对符合一定规律的海量并发任务请求给系统带来的冲击，在给用户带来良好 QoS 体验的同时满足与用户签订的 SLA，实现云计算出色的性能表现，本文提出一种基于 Holt-Winters 季节指数平滑模型预测的计算节点部署策略模型。模型通过加载系统历史请求数据预测下个单位时间段的任务请求量分布情况，并根据设计的 AF 算法判断系统是否应为本时段的任务请求数据量做出响应，及相应的部署数量、位置。AF-HW 模型还可自适应地调节系统实时响应请求的情况，充分利用冗余预制的计算节点，并可有效地根据请求量的分布状态自扩大或缩减预制周期，达到对请求变化的动态跟踪及降低系统能耗的目的。为了验证该模型的性能，设计了性能评估实验，针对模型的两个主要模块分别进行了实验。证明了 Holt-Winters 加法季节指数平滑模型在跟踪系统单日的任务请求量时拟合程度较高，说明其预测的准确及有效性；在对单个计算节点、系统整体响应性能指标评判时，设计了 5 种不同的环境强度进行模拟，证明在实际应用中相对于不添加预制功能的模型，该模型在响应性能方面有明显的优势，较适合类似于云计算等大规模的动态环境。

参 考 文 献

[1] Ioannis A M, Helen D K. Evaluation of gang scheduling performance and cost in a cloud computing system [J]. Journal of Supercomputing, 2012, 59(2): 975-992

[2] Anand R, Jeffrey D U. Mining of massive datasets[M]. London: Cambridge University Press, 2011

[3] Jerri L, Joe T, Mary E T. Google Analytics, 3rd Edition[M]. New Jersey: Wiley, 2009

[4] Qualcomm. The Wi-Fi evolution-an integral part of the wireless landscape[R]. USA: Qualcomm Incorporated, 2013

[5] Shiraz M, Abolfazli S, Sanaei Z, et al. A study on virtual machine deployment for application outsourcing in mobile cloud computing[J]. The Journal of Supercomputing, 2013, 63(3): 946-964

[6] 陈彬. 分布环境下虚拟机按需部署关键技术研究[D]. 长沙：国防科学技术大学，2010
Chen Bin. Research on key technologies of on-demand deployment of virtual machines in distributed environments [D]. Changsha: National University of Defense Technology, 2010

[7] Samer A K, Dinesh S, Prasenjit S, et al. VMFlock: Virtual Machine Co-Migration for the Cloud[C]// Proceedings of the 20th international symposium on High performance distributed computing(HPDC'11). New York: ACM, 2011: 159-170

[8] 罗晶. 嵌入式虚拟机系统镜像存储的研究[D]. 武汉：华中科技大学，2012
Luo Jing. Research on system images storage in embedded virtualization system[D]. Wuhan: Huazhong University of Science and Technology, 2012

[9] Jonathan R C. A Distributed and Collaborative Dynamic Load Balancer for Virtual Machine[C]// Euro-Par 2010 Parallel Processing Workshops. Berlin Heidelberg: Springer, 2010: 641-648

[10] Mankiw N G. Principles of Economics 6th Edition [M]. USA: Cengage Learning, 2011

[11] Sarah G, Roland F, Christophe C. Robust Forecasting with Exponential and Holt-Winters Smoothing[R]. Belgium: Katholieke University Leuven, 2007

[12] Hung L H. Hype Cycle for the Internet of Things[R]. USA: Gartner, Inc., 2013

[13] Rodrigo N C, Rajiv R, Anton B, et al. CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms [R]. Cloud Computing and Distributed Systems Laboratory, Australia, 2010

[14] Baidu Inc [OL]. 2013-10-05. http://tongji.baidu.com/web/5473605/overview/~mult

[15] Tai J Z, Waleed M, Zhang J M, et al. ARA: Adaptive Resource Allocation for Cloud Computing Environments under Bursty Workloads [R]. Boston: Northeastern University, 2011

[16] Ning F M, Giuliano C, Ludmila C, et al. Burstiness in multi-tier applications: symptoms, causes, and new models[R]. Willamsburg: College of Willian and Mary, 2008

[17] 王健宗，谌炎俊，谢长生. 面向云存储的 I/O 资源效用优化调度算法研究[J]. 计算机研究与发展，2013, 50(8): 1657-1666
Wang J Z, Chen Y J, Xie C S. Research on I/O resource scheduling algorithms for utility optimization towards cloud storage [J]. Journal of Computer Research and Development, 2013, 50(8): 1657-1666

(上接第 126 页)

[31] Jamroga W, Bulling N. A logic for reasoning about rational agents[M]// Computational Logic in Multi-Agent Systems-CLIMA. Berlin: Springer, 2007: 42-61

[32] Bulling N, Jamroga W. Rational play and rational beliefs under uncertainty[C]// 8th International Joint Conference on Autonomous Agents&Multiagent Systems/Agent Theories, Architectures, and Languages. 2009: 257-264

[33] Andreas H, Emiliano L, Dirk W. Logic, Reasoning about Actions Meets Strategic Logics[M]// Logic, Rationality, and Interaction: 4th International Workshop(LORI 2013). Hangzhou, China: Springer Verlag, Tiergartenstrasse 17, Heidelberg, D-69121, Germany, 2013: 162-175

[34] Nils B, Wojciech J. Comparing variants of strategic ability: how uncertainty and memory influence general properties of games [J]. Autonomous Agents and Multi-Agent Systems, 2014, 28(3): 474-518