第 36 卷 第 2 期 计 算 机 工 程 2010 年 1 月
Vol.36 No.2 Computer Engineering January 2010
·开发研究与设计技术· 文章编号：1000—3428(2010)02—0252—02 文献标识码：A 中图分类号：TP393

面向社会 Agent 的网络监测系统框架

王 维[1]，黄 敏[2]，孙 禾[3]
(1. 西南科技大学计算机科学学院，绵阳 621010；2. 西南科技大学网络信息中心，绵阳 621010；3. 辽宁科技学院自动控制系，本溪 117022)

摘 要：在社会 Agent 理论的基础上，提出面向社会 Agent 的网络监测系统框架。结合软件复用的思想，根据网络监测数据，将该框架分为自治功能层、个体意识层和社会意识层的 3 层监测系统抽象模型。基于该框架设计的网页内容访问监测软件开发速度快、资源复用率高和鲁棒性强。

关键词：社会 Agent；网络监测；框架

Social Agent Oriented Network Monitor System Framework

WANG Wei[1], HUANG Min[2], SUN He[3]
(1. School of Computer Science, Southwest University of Science and Technology, Mianyang 621010;
2. Center of Network Information, Southwest University of Science and Technology, Mianyang 621010;
3. Department of Automatic Control, Liaoning Institute of Science and Technology, Benxi 117022)

【Abstract】This paper proposes a social Agent oriented framework of network monitor system base on the theory of social Agent. According to the idea of network monitor data and software reuse, this framework is divided into three layers monitor system abstract model, it comprises self-function layer, individual consciousness layer and social awareness layer. A Web page content access monitor software based on this framework has the advantages of quick development speed, high resource reuse rate and strong robustness.

【Key words】social Agent; network monitor; framework

1 概述

根据国际电信联盟(ITU)和国际标准化组织(ISO)合作制定的网络监控系统架构的描述分为网络资源监测、网络行为监测和桌面行为监测 3 大部分。对各种商业监测软件的调查发现，目前各大类的监测范围还要包括一些实际的子类别。网络资源的监测包括对路由器、交换机、服务器等网络上的固有硬件资源的监测。其中，该监测数据包括各种网络设备的利用率、数据吞吐量、网络设备的各层协议比例的统计等。网络行为的监测包括 Web 访问监测、邮件监测、BT/FTP 监测、QQ/MSN 监测、流量监测、打印监测等。桌面行为的监测包括安装软件检查、禁止游戏、非法内容审查、文件拷贝、文件加密等。

上述各类监测具有一定共性。按照数据获取方式大致分为本地监测和远程监测 2 种，且原始数据均为网络消息和本地消息 2 种，网络消息的获取分为 SNMP 报文方式和网络数据嗅探方式。由于采集原始数据的方式较少，且各种监测方式都是基于这些数据，因此构造各种监测 Agent 的核心功能后，可以基于不同监测目的从逻辑上指定监测角色。这为本文提出的面向社会 Agent 的网络监测系统框架打下基础。

2 基于角色的社会 Agent

2.1 智能 Agent 的 BDI 思维模型

基于角色的社会 Agent 模型是基于文献[1]的 BDI 模型，即一个解释器 M 是一个元组：$M=<W,E,T,\prec,U,B,G,I,\Phi>$，其中，$W$ 是世界集；E 是原子事件类型集；T 是时间点上的集合；$\prec$ 是时间点上的一个二元关系；U 是论域；Φ 是对任何已知世界和时间点从一阶实体到 U 中元素的映射；关系 B、关系 G、关系 I 将主体当前的处境分别映射到它的信念可达世界、目标可达世界和意图可达世界，且 $B\subseteq W\times T\times W$, $G\subseteq W\times T\times W$, $I\subseteq W\times T\times W$。用 R 表示这些关系中的任意一个，并用 R_t^w 表示在时刻 t 从世界 w 可达的世界集合。

$Bel(a,\Phi)$ 表示主体 a 在时刻 t 内具有一个信念 Φ，当且仅当主体 a 在时刻 t 的所有信念可达世界里都为真。

语义为 $M,v,w_t \models Bel(a,\Phi)$ iff $\forall w' \in B_t^w, M,v,w_t' \models \Phi$

$Goal(a,\Phi)$ 表示主体 a 在时刻 t 具有一个目标 Φ，当且仅当主体 a 在时刻 t 的所有目标可达世界里 Φ 都为真。

语义为 $M,v,w_t \models Goal(a,\Phi)$ iff $\forall w' \in G_t^w, M,v,w_t' \models \Phi$

$Int(a,\Phi)$ 用于映射主体当前处境到所有它的意图可达世界。主体在时刻 t 试图使 Φ 为真，当且仅当 Φ 使主体 a 在时刻 t 的所有意图可达世界里都为真。

语义为 $M,v,w_t \models Int(a,\Phi)$ iff $\forall w' \in I_t^w, M,v,w_t' \models \Phi$

$Att(a,\Phi)$ 表示主体 a 的思维属性，即主体 a 在时刻 t 具有一个信念(目标或意图)使 Φ 为真。

2.2 基于角色的社会 Agent 思维方式

本文所指的社会 Agent 是文献[2]提出的基于 Agent 角色的思维模型。它包括角色信念、角色目标和角色意图在内的承担它的智能 Agent 行为的思维状态，而承担角色的智能 Agent 以该角色的思维状态进行思维。基于角色的思维状态表示为 $Role(r,\Phi)$，即承担角色 r 的 Agent 具有信念(目标或意图) Φ。

基金项目：四川省教育厅自然科学科研基金资助项目(2006ZD034)
作者简介：王 维(1982－)，男，硕士研究生，主研方向：网络安全，数据库；黄 敏，副教授；孙 禾，讲师、硕士
收稿日期：2009-05-11 **E-mail：**vvaw@qq.com

智能 Agent 通过承担角色成为社会 Agent，可以用二元谓词 *Play*(*a*, *r*)表示智能 Agent *a* 承担角色 *r*。*Commit*(*a*, *b*, *r*)表示智能 Agent *a* 对智能 Agent *b* 承诺承担角色 *r*。智能 Agent 承担角色意味着智能 Agent 对角色的承诺，因此，$Play(a,r) \supset Commit(a,b,r)$。

智能 Agent 一旦承担角色，就以基于角色的思维属性进行思维。因此，有 $Paly(a,r) \wedge RoleAtt(r,\Phi) \supset Att(a,\Phi)$，表示智能 Agent *a* 承担角色 *r*，并且基于角色 *r* 的思维属性为 $RoleAtt(r,\Phi)$，智能 Agent *a* 具有的思维属性为 $Att(a,\Phi)$。

3 面向社会 Agent 的网络监测系统框架

经研究认为，实现可面向社会 Agent 设计的框架，关键是以脚本语言中闭包的方式整合上述思维模型中的各种属性。本文基于社会 Agent 理论，按照软件设计功能复用的思想，利用 LUA[3]是易整合语言(glue language)的特性，参考并改进文献[4]将 MAS 分为社会意思层和个体意识层的思想，提出一个抽象模型，如图 1 所示。

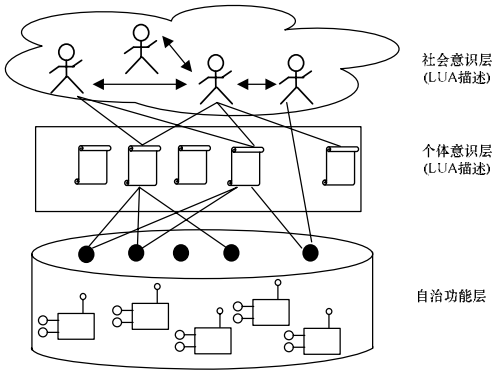

图 1　面向社会 Agent 的抽象框架

在图 1 中，自治功能层包含可复用的基本单位，在本框架中包括网络数据包抓取的 COM 组件，网络流量监测的 COM 组件、负责基于 TCP/IP 通信的服务动态链接库、面向 SQL Server 的数据库通信中间件、面向 Agent 的语言解释器组件动态链接库、以及上述某些功能所需要的基于完成队列的 I/O 控制程序中间件等。个体意识层是 Agent 静态属性的描述层。不但定义了各种角色的 Agent 的能力，还定义了它们的名称、目标描述、权限、能向外界提供的服务描述以及其他与 Agent 有关的对象。本框架中使用 LUA 脚本定义 Agent 的个体意识。社会意识层根据上一层所提供的接口进行 Agent 的角色定义，它是一个动态的开放框架，框架使用 LUA 脚本配置 Agent 的社会意识信息，在该层上定义各个 Agent 之间的角色关系即实现系统功能需求。社会意识层依赖于一种类似于 P2P 服务的抽象模型，如图 2 所示。

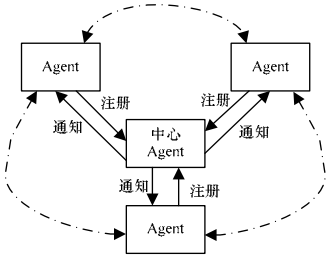

图 2　社会意识层的交互协议模型

中心服务器通过各 Agent 的注册情况，在读取角色配置信息后向各 Agent 发送通知以完成 $Play(a,r) \supset Commit(a,b,r)$ 操作，然后使各 Agent 可以根据角色配置情况完成所承担的任务。

4 基于本文框架的网页内容访问监测软件

为积极配合党和政府提出的“服务型政府”建设，某机关单位进行内部网络的监管，了解员工利用上班时间的上网内容。本文基于该框架开发了一个网页内容访问监测软件。为保证不影响软件的性能和拓扑结构，监测单元采用 TAP 接入的方式部署，选用设备为 DATACOM 的 10/100/1000-TAP。为了监测网页访问情况，需要对 Http 协议进行分析。而 Http 协议是基于 TCP 协议的，且协议数据是基于文本的。因此，只要分析 Http 请求的 Host 和 Path 就可以知道用户是在什么网站。

设 *A*, *B* 为 2 个 Agent，有 *A*=*B* 或 *A*≠*B*，*A* 需要 *B* 提供 Http 协议头的数据，在社会意识层上可描述为

B.PlayRole(A, “Sniffer.Http”)

在个体意识层可配置 *B* 的 LUA 脚本为

```
RoleAbility={Proto=Sniffer.Http, FilterAdapter=XMLAdapter,
Filter="options.xml", MessageAdapter=comm}
RoleBel=RoleAbility
RoleAction=function()
{
//解析消息的闭包
…
}
RoleGoal=RoleAction
RoleInt=LOCAL_ADAPTER
```

在个体意识层可配置 *A* 的脚本为

```
function MessageCallBack(httpHead, userIP)
httpHead=string.lower(httpHead)
//内容格式化的回调接口，使用 LUA 的模式匹配功能找到网页
//访问路径
…
end
```

在使用 VC++开发的面向 LUA 配置的 UI 层表现如图 3 所示。

图 3　过滤规则配置为 Nil 软件运行时的截图

与以往针对某应用层协议的网络监测软件的开发过程所用的时间和复杂度对比，如表 1 所示。

表 1　2 种方法开发的软件对比

	直接构建软件开发	基于本文框架开发
开发周期/天	≈10.0	<0.5
调试方法	单一、定位慢	可分层调试、定位快
资源利用率	高	非常高(使用 IOCP 核心对象)
分布式开发	不容易	容易(借鉴 P2P 模型)
可扩展性	低	高(基于 COM，且可分层扩展)
智能性开发	慢(修改规则即需编译)	快(规则基于解释)
鲁棒性	低	高

(下转第 259 页)