

基于层次时间自动机的动态行为取证建模方法

金仙力^{1,2,3}, 孙国梓^{1,2,3}, 杨 庚^{1,2,3}

(1 南京邮电大学 计算机学院, 江苏 南京 210003; 2 江苏省无线传感网高技术研究重点实验室, 江苏 南京 210003;
3 宽带无线通信与传感网技术教育部重点实验室, 江苏 南京 210003)

摘 要: 提出一种新的动态行为取证层次化模型. 首先介绍层次时间自动机的概念, 接着详细阐述动态行为的层次时间自动机形式化模型及其组合模型, 然后分析组合模型中可能存在的非法行为.

关键词: 层次时间自动机; 取证模型; 动态行为; 形式化方法

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2012)11-0018-04

The Methods of Forensic Model for Dynamic Behavior Based on Hierarchical Timed Automata

JIN Xian-li^{1,2,3}, SUO Guo-zhi^{1,2,3}, YANG Geng^{1,2,3}

(1 College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2 Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;
3 Key Lab of Broadband Wireless Communication and Sensor Network Technology,
Ministry of Education Jiangsu Province, Nanjing 210003, China)

Abstract: This paper proposes a new hierarchical forensic model for dynamic behavior. Firstly, it introduces the concept of hierarchical timed automata. Then, the formal model and its composition model for dynamic behavior are detailed. It also analyses the illegal behaviors in the composed model.

Key words: hierarchical timed automata; forensic model; dynamic behavior; formal method

1 引言

当前,随着信息技术的飞速发展,计算机和网络在现代社会中所扮演的角色日益重要^[1].同时,计算机犯罪也以惊人的速度增长,犯罪手段也呈现多样化和复杂化.为有效打击计算机犯罪,一方面要建立起一套健全的法律体系,另一方面由于计算机犯罪和计算机数据证据的特殊性,计算机数据取证必须遵循严格的过程和程序,建立一个从调查准备至证据呈现各个阶段均有效的取证模型^[2-3].目前,计算机取证研究除在传统技术方法上进一步发展外,计算机动态取证技术^[4]和形式化取证分析技术已成为主要的研究方向.本文针对动态取证技术,提出一种

基于层次时间自动机^[5]的动态行为形式化模型,以精确的语义为后续的动态行为取证工具的开发奠定可信的理论基础.

2 动态行为取证模型

2.1 层次时间自动机

层次时间自动机(Hierarchical Timed Automata, HTA)^[5]是一种层次状态机,它以层次方式对时间自动机进行了扩展.它与平面时间自动机的区别在于层次时间自动机的状态既可以是简单状态(在层次时间自动机中称为基本状态)也可以是组合状态(在层次时间自动机中称为超级状态,它包含子状态),而平面时间自动机不存在子状态.超级状态,它

收稿日期: 2012-05-04; 修回日期: 2012-06-08

基金项目: 江苏省高校自然科学研究计划项目(09KJD520007); 江苏高校优势学科建设工程项目(yx002001); 南京邮电大学引进人才计划(NY208007)

本身就是一个(层次)时间自动机,其子状态既可以是“异或”的组合也可以是“与”的组合。在“异或”组合中,每个子状态之间是互斥的,也就是说,当这个组合处于激活状态,那么其中有且仅有一个子状态是激活的。反之,如果一个“与”组合处于激活状态,则它所有的子状态都是激活的。需要注意的是,“与”组合的子状态不能是简单状态。

为了便于给出一个清晰的语义形式分析,层次时间自动机引入“入口”点和“出口”点来表示不同层次间的转换。每个超级状态都有一个“入口”集,它是外界进入超级状态的“入口”点的集合,一般用符号“●”或“—”表示。而“出口”点是离开超级状态的过渡状态,一般用符号“—”表示。

下面是层次时间自动机的语法定义:

定义 1 (层次时间自动机 HTA). 一个层次时间自动机是一个九元组 $\langle S, S_0, \delta, \sigma, V, C, Ch, Inv, T \rangle$, 其中

- S 是一个有限位置状态集,用于描述系统中的不同位置状态;
- $S_0 \subseteq S$ 是初始位置状态集合;
- $\delta: S \rightarrow 2^S$ 是一个从位置 l 到 l' 的所有可能的子状态的映射函数;
- $\sigma: S \rightarrow \{\text{AND, XOR, BASIC, ENTRY, EXIT, HISTORY}\}$ 对应每个位置状态的一个类型;
- V, C, Ch 分别是变量,时钟和通道的集合;
- $Inv: S \rightarrow \text{Invariant}$ 对应每个位置状态的一个不变量;

• $T \subseteq S \times (\text{Guard} \times \text{Sync} \times \text{Reset} \times \{\text{true, false}\}) \times S$ 是位置转移规则集,用于表述系统在接收不同输入下从一个位置状态转移到另外一个位置状态的规则。其中 Guard 是卫条件的集合, Sync 是同步信号的集合, Reset 是重置(包括时钟重置和数据赋值)的集合。一个转移 $t = (l, g, s, r, u, l')$ 连接两个位置 l 和 l' , 伴随卫条件 g 、同步信号 s 、赋值 r 和紧急标记 u , 用符号 $l \xrightarrow{g, s, r, u} l'$ 表示。转移 t 表示当满足卫条件 g 时,在同步信号 s 的驱动下,从位置状态 l 转移到位置状态 l' , 同时时钟重置和数据赋值。如果转移 t 伴随紧急标记 u 为 true 的时候,转移立即进行。如果 u 为 false, 则转移 $t = (l, g, s, r, u, l')$ 中 g, s, r, u 可以省略。关于层次时间自动机的详细语法可参阅文献[5]。

2.2 行为模型

本文中,行为事件是指某一实体单元在某一段时间段发生了一系列具有逻辑规则的行为动作,每一个行为动作将对本实体单元和该实体单元所在的外界环境(其他实体单元)产生影响^[6]。

基于层次时间自动机的行为事件形式定义如下:

定义 2 (行为事件的层次时间自动机模型). 行为事件 P 的层次时间自动机模型可以表示一个五元组:

$$\langle ID_P, A_P^I, A_P^O, A_P^H, B_P \rangle.$$

其中:

(1) ID_P 是行为事件 P 的标识;

(2) A_P^I, A_P^O, A_P^H 是互不相交的三个集合,分别表示行为事件 P 输入动作集合、输出动作集合和内部(隐藏)动作集合:输入动作用来表示由外界环境产生的对本实体单元产生影响的行为动作,输出动作用来表示由本单元实体发出的影响外界环境的行为动作;内部动作是发生在本实体单元内容的行为动作,对外界不产生任何影响;

(3) B_P 是行为事件 P 的行为语义描述,刻画行为事件的动态变化。从外界环境来看,它代表 HTA 中的一个超级状态;从行为事件本身来看,它是一个 HTA $\langle S, S_0, \delta, \sigma, V, C, Ch, Inv, T \rangle$ 。

图 1 是基于层次时间自动机的一个简单行为事件的形式模型实例。图中,我们将层次时间自动机封装在一个虚线框中,虚线框边缘表示行为动作。箭头代表行为事件与外界环境的动作交互方向。

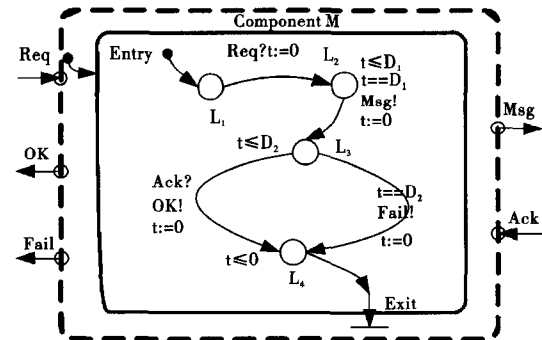


图 1 行为事件的形式模型举例

如图 1 所示,行为事件 M 是某一实体单元在某一个时间点由外界触发后发送了一条消息信号 Msg 并判断在规定时间内是否收到响应信号 Ack 。当自动机收到外界的请求动作信号 Req 后,发送消息信号 Msg ,网络传送延迟为 D_1 ,之后开始等待响

应信号. 如果自动机在 D_2 时间内收到响应信号, 则向环境返回成功信号 OK, 否则返回失败信号 Fail. 行为事件 M 对应的超级状态包括六个子位置状态: 入口点 Entry(事件开始), L_1, L_2, L_3, L_4 和出口点 Exit(事件结束).

由定义 2, 行为事件 M 的输入动作、输出动作和内部动作集合可分别描述如下:

$$A_M^I = \{\text{Req}, \text{Ack}\}, A_M^O = \{\text{Msg}, \text{OK}, \text{Fail}\}, A_M^H = \emptyset.$$

2.3 行为组合

行为事件组合是由多个行为事件按照一定的时间关系和方式复合而成的更加复杂的行为事件, 复合后, 多个实体单元组合成一个更大的实体单元, 原有的多个行为事件成为组合后行为事件的子行为事件. 这些子行为事件既可以是简单行为事件, 也可以是复合行为事件.

如果两个行为事件是可组合的, 那么首先必须满足动作之间不存在冲突, 即行为事件语法可组合:

定义 3 (语法可组合). P 和 Q 两个行为事件接口是语法可组合的当且仅当:

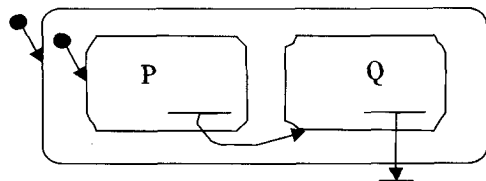
- (1) $A_P^H \cap A_Q = \emptyset$
- (2) $A_Q^H \cap A_P = \emptyset$
- (3) $A_P^O \cap A_Q^O = \emptyset$
- (4) $A_P^I \cap A_Q^I = \emptyset$

我们将 P 和 Q 共有的动作表示为: $\text{shared}(P, Q) = A_P \cap A_Q$.

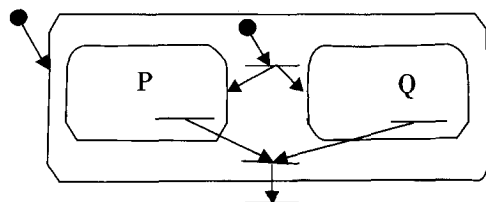
如果 P 和 Q 是语法可组合的, 那么

$$\text{shared}(P, Q) = (A_P^I \cap A_Q^O) \cup (A_P^O \cap A_Q^I)$$

两个行为事件的语法可组合表示两个行为事件都执行了各自的行为动作. 组合方式如图 2 所示.



(1) 顺序组合



(2) 并行组合

图 2 组合方式

定义 4 (行为组合). 行为事件 P, Q 的行为组合是以顺序或并行方式连接两个有交互动作的 ($\text{shared}(P, Q) \neq \emptyset$) 实体单元复合成一个新的更为复杂的行为事件, 记为 $P \parallel Q$. 将 $P \parallel Q$ 用五元组 $\langle \text{ID}_{P \parallel Q}, A_{P \parallel Q}^I, A_{P \parallel Q}^O, A_{P \parallel Q}^H, B_{P \parallel Q} \rangle$ 表示如下:

- (1) $\text{ID}_{P \parallel Q}$ 是新行为事件 $P \parallel Q$ 的标识
- (2) $A_{P \parallel Q}^I = (A_P^I \cup A_Q^I) - \text{shared}(P, Q)$
- (3) $A_{P \parallel Q}^O = (A_P^O \cup A_Q^O) - \text{shared}(P, Q)$
- (4) $A_{P \parallel Q}^H = (A_P^H \cup A_Q^H) \cup \text{shared}(P, Q)$
- (5) $B_{P \parallel Q}$ 是一个新的层次时间自动机, 是 P, Q

对应的自动机 B_P, B_Q (视为 $B_{P \parallel Q}$ 的子状态) 的顺序组合或并行组合.

如图 3, 行为事件 N 行为逻辑为: 等待接收信号 Msg , 如果收到则向外界环境返回响应信号 Ack , 传输延迟为 D_3 . 行为事件 N 的输入动作、输出动作和内部动作集合可分别描述如下:

$$A_N^I = \{\text{Msg}\}, A_N^O = \{\text{Ack}\}, A_N^H = \emptyset$$

行为事件 N 与图 1 中行为事件 M 组合后, 共享动作 $\text{shared}(M, N) = \{\text{Msg}, \text{Ack}\}$ 成为复合行为事件 $M \parallel N$ 的内部动作, 三种动作集合为:

$$A_{M \parallel N}^I = \{\text{Reg}\}, A_{M \parallel N}^O = \{\text{OK}, \text{Fail}\}, A_{M \parallel N}^H = \{\text{Msg}, \text{Ack}\}$$

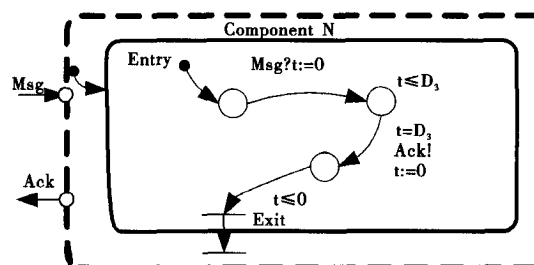


图 3 行为组合举例

2.4 非法行为取证

两个行为事件组合满足语法可组合性并不代表实体单元中的每一个行为动作是按正确的规则交互的, 可能存在两个行为事件间的动作不一致. 为此, 我们引入非法行为状态用于描述这种不一致性.

定义 5 (非法行为状态). 复合行为事件 $P \otimes Q$ 的非法行为状态集合定义为:

$$\text{Illegal}(P, Q) = \{(m, n) \in S_P \times S_Q \mid \exists a \in \text{shared}(P, Q), (a \in A_P^O(m) \wedge a \notin A_Q^I(n)) \vee (a \in A_Q^O(n) \wedge a \notin A_P^I(m))\}$$

其中:

- (1) S_P, S_Q 分别代表行为事件 P, Q 的状态集合.

(2) $A_P(m)$ 、 $A_Q(n)$ 分别表示行为事件 P 、 Q 中各自从位置状态 m 、 n 为源点的位置转移上的动作集合。

(3) 上标 I 和 O 分别表示该集合中的元素是属于输入动作和输出动作。

非法状态表明当前一个行为事件中的活动状态的输出动作发生时另一个行为事件的活动状态不存在与之对应的输入动作。

以行为事件 M (图 1)和行为事件 L (图 4)为例,两个行为事件满足语法可组合性,但当 $D_4 > D_1$ 时,它们之间的组合并不是按照正确的交互协议,因为存在动作 $\text{SendMsg} \in \text{shared}(M, L)$,使得 $(L_2, S_1) \in S_M \times S_L$ 满足 $\text{Msg} \in A_M^O(L_2)$ 并且 $\text{Msg} \notin A_L^I(S_1)$,即至少存在一对非法状态 $(L_2, S_1) \in \text{Illegal}(M, L)$,不为空。

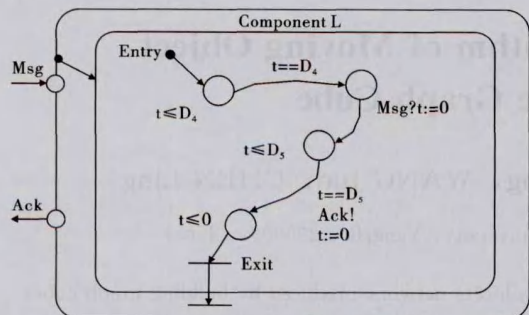


图 4 行为事件 L

3 结束语

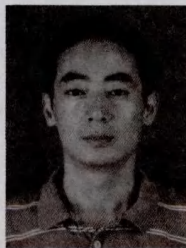
本文提出了基于层次时间自动机的动态取证形式化模型。该模型可以从不同粒度的实体单元分析行为的动态变换,从而大大降低取证过程的复杂性,同时有利于快速捕捉和定位非法行为动作。下一步的工作将研究行为组合的非法行为状态的检测算法和计算机动态行为取证工具的开发。

参考文献:

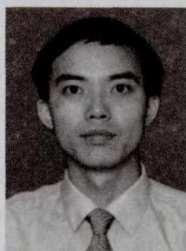
- [1] 李炳龙,王鲁,陈性元. 数字取证技术及其发展趋势[J]. 信息网络安全, 2010 (10): 52-55.

- [2] 陈威兵. 数字视频真实性和来源的被动取证[J]. 通信学报, 2011 (6): 177-183.
- [3] 孙国梓. 基于可信概率的电子数据取证有效性模型[J]. 计算机学报, 2011, 34(7): 146-152.
- [4] 鄢喜爱,杨金民,常卫东. 基于蜜罐技术的计算机动态取证系统研究[J]. 微电子学与计算机, 2010, 27(1): 135-137.
- [5] David A, Oliver Möller M. From HUPpaal to Uppaal: A translation from hierarchical timed automata to flat timed automata [R]. Research Series RS-01-11, BRICS, Department of Computer Science, University of Aarhus, 2001.
- [6] Delp E, Memon N, Wu M. Digital forensics [J]. IEEE Signal Process Magazine, 2009 (3): 14-15.

作者简介:



金仙力 男, (1978—), 博士, 讲师, 硕士生导师。研究方向为形式化方法、信息安全和软件工程。



孙国梓 男, (1972—), 博士, 教授, 硕士生导师。研究方向为信息安全、计算机网络。



杨庚 男, (1961—), 博士, 教授, 博士生导师。研究方向为云计算服务、传感器网络、信息安全等。