doi:10.3969/j.issn.1673-9833.2012.04.019

基于可信级度量的智能终端安全模型研究

郭德彪，陈卫兵，王金燕，周　颖，彭志香

（湖南工业大学 计算机与通信学院，湖南 株洲 412007）

摘　要：为解决开放环境下智能终端无法提供有效保护用户隐私及通信实体之间的信任问题，提出一种基于可信级度量的stTLM智能终端安全模型。该模型基于一种轻量级可信级度量机制，通过对任务安全分级及集成奖惩机制，可提供细粒度的安全访问授权性能。模型评估结果表明，stTLM模型具有优异的环境适应性及动态性能。模型容易实施，可有效增强开放环境下智能终端的安全性。

关键词：访问控制；安全模型；可信级度量；智能终端

中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1673-9833(2012)04-0081-07

Study on Security Model of Smart Terminal Based on Trusted Levels Measure

Guo Debiao，Chen Weibing，Wang Jinyan，Zhou Ying，Peng Zhixiang

（School of Computer and Communication，Hunan University of Technology，Zhuzhou Hunan 412007，China）

Abstract：A security model for smart terminal based on trusted levels measure named stTLM is proposed for effective solving user privacy protection and trusted communication between entities. Based on a lightweight trust levels metrics mechanism, the model can provide a fine-grained security access authorization performance by grading tasks and integrating reward-punishment mechanism. The evaluation result shows that the stTLM model has an excellent environment adaptability and dynamic performance. The model is easy to implement and be able to enhance the safety of the smart terminal effectively in open environment.

Keywords：access control；security model；trusted levels measure；smart terminal

1　背景知识

开放环境下，智能终端系统用户变动频繁、无法事先获得用户的身份，给用户身份安全管理及隐私保护带来巨大挑战。在系统资源紧张的智能终端中（例如分布嵌入式系统），复杂的安全策略及可信度量方法限制了这些系统的应用范围。针对这些问题，国内外诸多学者使用不同方法扩展了基于角色的访问控制（role-based access control，RBAC）模型[1-6]，以增强开放式环境下基于传统RBAC模型[7-8]的平台安全性。

一些学者提出使用基于证书的访问控制模型增强平台的安全管理[9-12]，但基于证书的机制不保证在证书发布期间载体行为和功用的一致性，也无法保障证书本身的获得途径合法；同时，基于访问控制的证书机制不记录用户行为，它根据证书呈递的一个特殊会话给予相应权限，具有二值性的缺陷。因此，有学者提出基于可信的访问控制模型，此模型通过信任度量动态升降用户权限克服了基于证书的访问控制模型的上述缺点，信任度量值的计算根

收稿日期：2012-05-12

作者简介：郭德彪（1986-），男，江苏徐州人，湖南工业大学硕士生，主要研究方向为嵌入式系统，
E-mail：ek_guoarm@126.com

据终端对自身度量及第三方声誉[13]。

J. W. Woo 等人[14] 提出了一个扩展的 RBAC 模型，通过判断用户可信值是否大于预先设定的阈值来决定是否授予权限。H. Takabi 等人[15]定义了用户可信度及角色需求可信度，并定义只有当用户可信度大于或等于角色需求可信度时才能分配角色。Qureshi Basit 等人[16]给出了一种可信度量机制，该机制避免了因网络中节点间的第三方信誉造假而模型容易被攻陷的现象。Sudip Chakraborty 等人[17]将可信关系集成在 RBAC 中，并提出了 TrustBAC 模型，该模型先给用户分配可信级，然后根据可信级与角色映射并分配权限，用户只有通过提升可信值才能提升角色集权限。TrustBAC 模型能够动态地对角色进行分配，克服了RBAC模型的动态性及监管性不足的缺陷。Li Lei 等人[18]提出用一种模糊回归可信度量方法预测用户的可信性关系，该方法可以避免基于可信分级的环境适应性带来的误导问题。Carles Martinez-García 等人[19]基于一种类似角色扮演的访问控制机制提出了 FRBAC 模型，模型内部角色是可进化的，因而增强了模型的安全性。A. El Husseini 等人[23]结合EC-SAKA 协议提出一种适用于智能环境下低资源系统使用的可信度量机制，具有信任度量简单的优点。

上述模型及所用度量机制，或用户角色不可进化，动态性差[13−15,23]，或未考虑用户信任需求[17,19]，或度量机制复杂[16,18,20−22]，均不适合在资源紧张的智能终端上使用。因此，为解决上述问题，本文提出一种基于轻量级可信度量机制的智能终端安全模型 stTLM，该模型通过对任务安全分级及集成奖惩机制，可提供细粒度的安全访问授权性能，具有优异的环境适应性及动态性能。

2 stTLM 安全模型

2.1 形式化说明

stTLM 安全模型如图 1 所示。

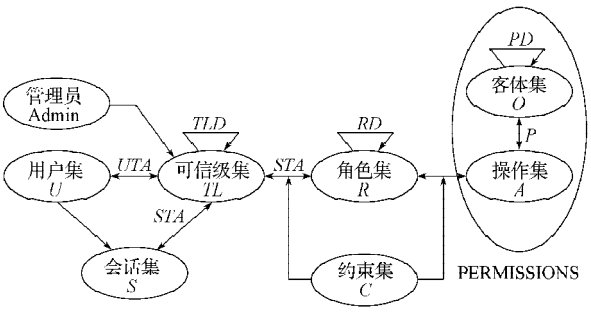


图 1 stTLM 模型

Fig.1 Model of stTLM

stTLM 模型定义了元素集及元素集之间的关系。元素包括下列类型：用户、可信级、角色、会话、操作、客体、权限及约束。

定义 1 stTLM 模型元素的形式化定义如下：

1）用户 $USERS=\{user_1, user_2, \cdots, user_n\}$，用户的概念是指具有自主能力的实体，包括其它系统、有自主能力的程序及自然人。

用户集 U 指正获取系统服务的用户集合。集成在模型中的管理员 Admin 是一个特殊的用户，拥有所有权限。

2）可信级 $TRUST\_LEVELS=\{TL|TL[0,1]\}$，是[0,1]之间的一个动态可变的实数。一个用户在特定时刻根据会话拥有一个可信级。

3）角色 $ROLES=\{role_1, role_2, \cdots, role_n\}$，系统根据用户的可信级赋予角色集，角色 R 是指相同语义职责关联的工作职能。

4）会话 $SESSIONS=\{session_1, session_2, \cdots, session_n\}$，会话 S 对应于一个用户和一组可信级，表示用户获取可信级的过程。

一个用户可进行多次会话，在每次会话中获得不同可信级。拥有不同的可信级意味着拥有不同的访问权限。

5）客体 $O=\{object_1, object_2, \cdots, object_n\}$，客体是一个可操作的数据集合，是系统可支配资源的一部分。

6）操作 $A=\{read, write, execute, \cdots\}$，是程序操作的一个镜像。

7）约束 C 定义为施用于模型元素之间的断言，返回一个接受与否的量。可将其视为施用元素关系或元素分配的条件。

8）权限 $P=2^{(O\times A)}$，在系统中执行特定任务的授权。权限总是和角色联系在一块，即权限赋予角色特定的权利。权限类型取决于应用系统，模型本身并不作任何假设。

定义 2 stTLM 模型元素之间的关系定义如下。

1）sua 定义了根据一个用户 u 属性 P 分配会话 s 的关系，$sua(u, P, s)=s^P$。在一次访问过程中，用户 u 可能会发起多次会话 s。

2）$UTA\subseteq USERS\times TRUST\_LEVELS$ 定义了用户信任级的分配关系。这是一个多对多关系，因为每个用户可能同时激发多个会话而具有多个可信级。

3）$STA\subseteq SESSIONS\times TRUST\_LEVELS$ 定义了会话信任级的分配关系。这是一个一对多的关系。每个会话都对应一个可信级。

4）$RTA \subseteq ROLES \times TRUST_LEVELS$定义了角色信任级的分配关系。这是一个多对多关系，同一可信级可被分配给多个角色，而一个角色可能具有多个可信级。

5）$TLD \subseteq TRUST_LEVELS \times TRUST_LEVELS$为可信级的支配关系（或称为偏序关系），表示为≤。对于任何$(TL_1, TL_2) \in TLD$，当$TL_1 \in TL_2$时，称为$TL_2 \leqslant TL_1$，即可信级集合TL_1是可信级集合TL_2的子集。

6）$RD=ROLES \times ROLES$为角色的支配关系，表示为≤。对任何$(r_1, r_2) \in RD$，仅当Assigned_Permissions$(r_1) \subseteq$Assigned_Permissions(r_2)时，称为$r_2 \leqslant r_1$。

7）$PD=PERMISSION \times PERMISSION$，为权限的支配关系，表示为≤。对于任何$(p_1, p_2) \in PD$，Assigned_TrustLevels$(p_1) \subseteq$Assigned_TrustLevels (p_2)时，称为$p_2 \leqslant p_1$。

8）Assigned_Roles函数　$TRUST_LEVELS \rightarrow 2^{ROLES}$指定可信级与角色之间的映射关系。形式表示为Assigned_Roles$(TL)=\{r \in ROLES \mid (r, TL) \in RTA\}$。

9）Assigned_Permission函数　$ROLES \rightarrow 2^{PERMISSIONS}$指定角色与权限之间的映射关系。形式表示为Assigned_Permission$(r)=\{p \in PERMISSIONS \mid (p, r) \in PA\}$。

约束 *constraints* 除了对分配函数进行限制外，也对访问控制策略及可信度量策略进行限制，系统可以根据具体需求对模型约束进行适当扩展及细化。本文提出的轻量级可信度量机制中，可以对任务安全因子及奖惩因子进行约束。这样做的目的是，既保证了任务安全的细粒度，同时增强了度量机制的动态性。

2.2　访问控制管理

stTLM 模型综合授权函数、访问控制策略以及可信度量策略，决策一个访问用户是否被允许访问相关客体。

当访问发生时，模型会根据被严密保护的访问历史记录和推荐，计算出访问用户的可信值。用户的可信值将传递给访问控制管理，以作为决策的依据。访问控制管理根据访问控制策略及约束服务，使用授权函数为用户分配角色和权限。用户在系统中的行为会被记录，非法行为会使用户的可信级降低。根据访问控制策略，当更新后的用户可信级很低而无法获得访问权限时，将导致用户正在进行的或后续的访问请求被拒绝。因此，模型的安全性均及动态性可以得到保障。模型访问控制管理框架如图 2 所示。

访问控制机制的本质是通过限制用户动作以保护系统资源，即只允许用户在限定的访问控制策略下实施特定任务。使用 stTLM 安全模型用作访问控制时，用户每次访问被允许前会先进行授权，授权依据是用户可信级值是否大于规定值。可信级值只有大于规定值，访问才被允许。同样，在会话过程中访问控制策略会动态验证授权及存取函数是否满足条件。若不满足这些条件，访问将被立刻禁止。用户被允许访问后，系统将为一个用户立即激活一个会话。在会话期间，用户拥有一个动态可信级，能够使用与之关联的角色。一个角色可以被多个用户使用，这些用户的权限相同。因此，用户可以通过可信级度量获得一个角色，执行该角色限定权限内的操作。

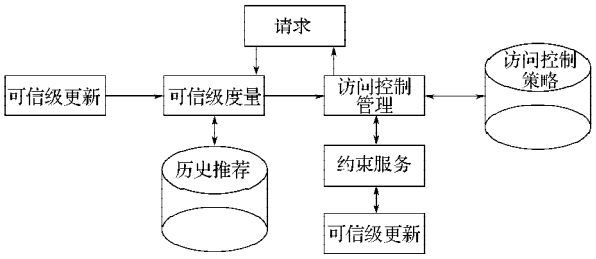
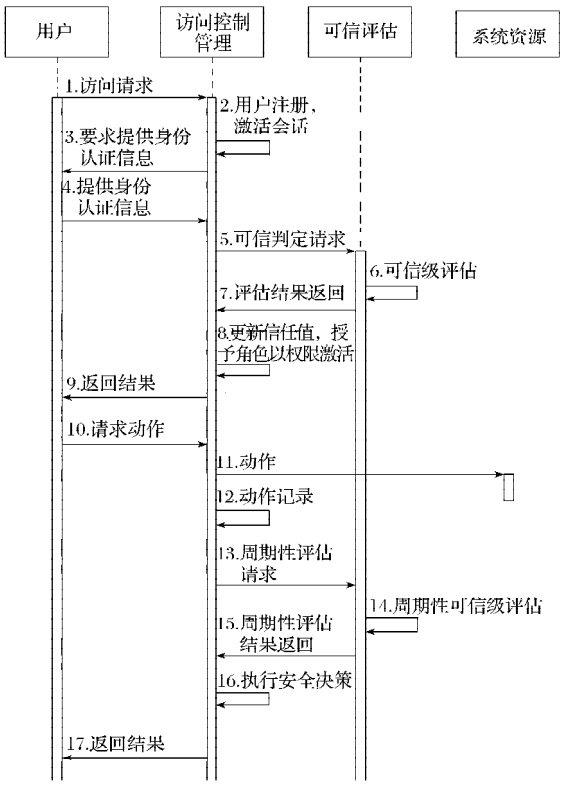


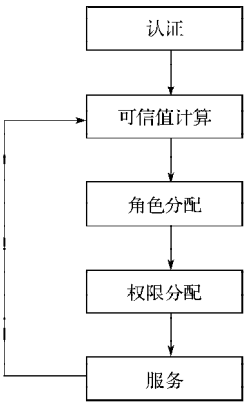
图2　模型访问控制管理过程

Fig. 2　Management process of access control in stTLM

从用户角度分析，stTLM 模型工作流图的基本过程如图 3 所示。



a）stTLM 模型工作时序图



b）stTLM模型工作流程

图3 stTLM模型工作流图

Fig. 3 Workflow diagram of stTLM model

用户（user）第一次接入系统（system）时，系统注册用户并生成会话实例（session）。系统根据用户提供的公开属性P，使用sua函数启用会话s^p并激活对用户u可信关系度量。系统根据计算的可信级值$T(system \rightarrow user)=tl$，使用函数Assigned_Roles确定用户$user$可以使用的角色$role$。$role$可以有多个，对任意一个角色$rolei$，$user$都有一个对应的权限集$p_j$，即$\forall j,(p_j, r_i)\in PA$。因此，在会话session中，用户$user$拥有权限集$\cup_i$Assigned_Permissions($role_i$)= $\cup 1 \leqslant i \leqslant n\{p_{ij} \mid (p_i, role_i)\in PA\}$。用户$user$被限定只能在权限满足条件下才能对客体$O$执行操作$A$，即$\forall(o,a)\in O \times A,(o,a)\in p_{ij}$。用户$user$对被允许的客体上动作会被记录在会话$session$中。对可信级重新评估时，动作历史会作为评估信息来源，更新的可信级值tl'会重新保存在$session$中。模型集成一个超级管理员system_admin，它能根据预定义的访问控制策略及可信度量策略对模型进行管理，可禁止类似拒绝服务攻击（DoS）的访问请求。

3 可信级度量

由图2可知，在stTLM模型中，可信级的度量是一个核心机制。为适应在资源紧缺的智能终端中使用模型，提出了一个具有细粒度安全特性的轻量级度量机制——sTrust。该机制度量组件构成如表1所示，可信级TL的度量包括直接可信DT及间接可信IT两部分。与其它度量机制[20-23]不同的是，直接知识和间接知识组件允许扩展。直接知识是节点根据历史对自身的直接推测，不仅包括信誉组件RE还包括直接不确定性组件DU。同理，间接知识是节点对历史和推荐的间接推测，包括趋势组件TR和间接不确定性组件IU。

表1 可信度量机制组件sTrust

Table1 Component of sTrust scheme

可信级 Trust Levels(TL)	度量构件
直接可信 Direct Trust(DT)	经验 Experience（E） 直接知识 Direct Knowledge（DK），包括信誉RE及直接不确定部分DU。
间接可信 Indirect Trust(IT)	推荐 Recommence（RC） 间接知识 Indirect Knowledge（IK），包括奖惩RP及间接不确定部分IU。

使用sTrust评估实体间的可信关系过程中始终遵循准则1和定义3，可信（不可信）的概念与Sudip Chakraborty等[17]给出的定义相同。

准则1 与可信关系度量时刻间隔越小，对可信关系度量值的权重影响越大。

定义3 可信（不可信）定义为在特定上下文中实体安全可靠动作的（不）胜任能力。

在特定的上下文c中，实体A对B的信任度量用$T_{(A\rightarrow B)}=(DT_{(A\rightarrow B)}, IT_{(A\rightarrow B)})$表示，其中，$DT_{(A\rightarrow B)}$为直接可信度量值，$IT_{(A\rightarrow B)}$为间接可信度量值。可信度量值可用式（1）表示

$$T_{(A\rightarrow B)}=\boldsymbol{T}_{(A\rightarrow B)}\times \boldsymbol{W}_{(A\rightarrow B)}=\left(DT_{(A\rightarrow B)}, IT_{(A\rightarrow B)}\right)\begin{pmatrix} w_{DT} \\ w_{IT}\end{pmatrix}=$$
$$w_{DT}\times DT_{(A\rightarrow B)}+w_{IT}\times IT_{(A\rightarrow B)}, w_{DT}+w_{IT}=1。 \quad (1)$$

$T_{(A\rightarrow B)}\in[0,1]\cup\{\perp\}$，0表示完全不可信，1表示完全可信，$\perp$表示无定义。无定义意味着在度量时间间隔内，系统没有可度量的事件发生。

权值向量$\boldsymbol{W}$元素分别为直接可信和间接可信权重。可信度量的基础是对事件性质的判定，事件性质由定义4确定。令a^i_k表示在第i个时间间隔内第k个事件，若$a^i_k\in LT$,则$p^i_k=0$；若$a^i_k\in HT$，则$p^i_k=1$。$I_i=\sum_{k=1}^{n}p^i_k$表示在第i个时间间隔内的所有的事件和值，令n_i，la_i，ha_i分别表示在第i个时间间隔内度量事件总数（一般可信事件不参与度量）、低可信事件个数及高可信时间个数，显然$n_i=la_i+ha_i$。特别地，当$n_i=0$时，$T\in\{\perp\}$。

定义4 $T_{(A\rightarrow B)}\in(0, 0.5)$表示低可信级$LT_{(A\rightarrow B)}$；$T_{(A\rightarrow B)}=0.5$表示一般可信级$MT_{(A\rightarrow B)}$；$T_{(A\rightarrow B)}\in(0.5,1)$表示高可信级$HT_{(A\rightarrow B)}$。

为表述方便，除特殊说明外，下文中对度量关系的表述均指实体A对实体B的度量关系，例如$T_{(A\rightarrow B)}$将简化描述为T。直接可信是实体根据经验E和直接知识DK对自己的度量。在本文中，直接知识主要指信誉RE。

$$DT = w_E \times E + w_{DK} \times DK。\tag{2}$$

权值 w_E, w_{DK} 满足关系 w_E+w_{DK}=1。经验的度量值由式（3）确定：

$$E = \begin{cases} \dfrac{\sum_{i=0}^{n} w_i p_l}{n_i}, & n_i \neq 0; \\ 0, & n_i = 0。 \end{cases}\tag{3}$$

在一个特定时间间隔里，第 i 个事件的权重由 $w_i = \dfrac{i}{S}, \forall i \in 1,2,\cdots,n$ 决定，并满足 $S = \dfrac{n(n+1)}{2}$。若 n_i=0，则 w_E=0。

直接知识包括信誉及直接不确定两部分

$$DK = w_{RE} \times RE + w_{DU} \times DU, w_{RE} + w_{DU} = 1。$$

信誉是对客体以往访问的一个记录评价，当对任务的安全需求较高时对信誉评估更加严格。信誉值的评估定义为式（4）：

$$RE = \frac{\sum_{i=0}^{n} ha_i}{\sum_{i=0}^{n} [n_i + (sl-1)la_i]}。\tag{4}$$

sl 为对任务分配的安全因子，这样做是为了满足不同任务的细粒度安全需求。当 sl=1 时，不考虑安全特性。此处限制 $sl \in [1,100]$ 且满足 $sl \in \mathbf{Z}^+$。显然，sl 越大，任务对安全的需求越高。DU 难以进行量化，应根据实际应用扩展。

间接可信部分包括推荐（RC）和间接知识（IK）两部分，推荐来自直接关联实体（推荐者）。间接可信值的度量方法用式（5）表示：

$$IT = w_{RC} \times RC + w_{IK} \times IK, w_{RC} + w_{IK} = 1。\tag{5}$$

设直接关联的节点个数 m，每个关联节点都作为一个推荐者给出一个推荐值 DT_i（相关推荐者的可信级值），则度量推荐值 RC 是所有这 m 个推荐者的推荐值的平均值，用式（6）式表示：

$$RC = \begin{cases} \dfrac{1}{m}\sum_{i=1}^{m} DT_i, & m \neq 0; \\ 0, & m = 0。 \end{cases}\tag{6}$$

间接知识包括奖惩及间接不确定两部分

$$IK = w_{RP} \times RP + w_{IU} \times IU, w_{RP} + w_{IU} = 1。$$

奖惩机制基于近期历史事件性质判定是否奖惩，并对后续事件进行直观预测。用式（7）表示：

$$RP = \left(\frac{ha_i}{n_i}\right)^2 \mathrm{e}^{-1/\left(1+ha_i^2\right)}。\tag{7}$$

对趋势的度量仅在策略间隔时间到时更新，采用类似式（3）的计算方法。IU 难以进行量化，应根据实际应用扩展。对历史可信级，采用式（8）的计算方法[23]。显然，它们均遵循规则 1。

$$TL^{[t_1,t_n]} = \frac{\sum_{i=1}^{n} w_{t_i} T^{(t_i)}}{\sum_{i=1}^{n} w_{t_i}}, w_{t_i} = \alpha^{t_n - t_1}, 0 < \alpha \leqslant 1。\tag{8}$$

4　模型评估及分析

在编写的模拟器上验证 stTLM 模型的有效性，模拟器遵循 sTrust 机制的度量规则。为方便验证，仿真要素设置如表 2 所示。为 $user_1$、$user_2$ 及 $user_3$ 分配的可信级初始值为0.20, 0.50及0.80；令 D={D_1, D_2, D_3, D_4}为实验数据集，实验数据的 0 代表违规事件，1 代表合法事件，空格代表一个时间间隔；假设与终端直接关联的终端有 3 个，它们的推荐值集为 R={R_1, R_2, R_3, R_4}；规则部分为用户可信级与用户权限之间的映射关系，仿真时参考，此处不对权限 P 作具体定义。

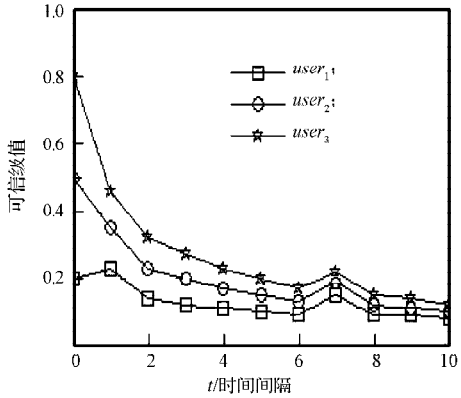
仿真结果如图 4 所示，分别为 stTLM 模型在不同仿真数据下可信级的度量结果。由图 4 可知，违规事件拉低了关联用户的可信级，合法事件提升了相关用户的可信级值。对于拥有不同初始可信级的用户，相同的事件将使用户可信级趋于一致。

表 2　仿真设置

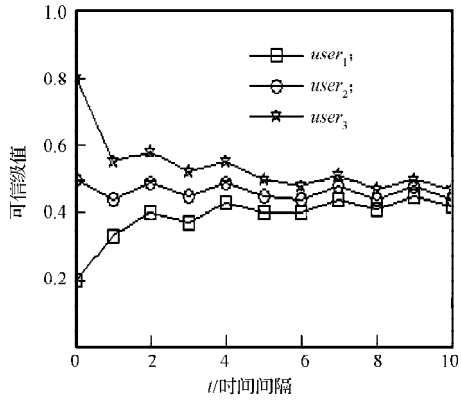
Tabel 2　Simulation settings

初 始 条 件	仿 真 数 据	规　则
TL_{u1}=0.2, TL_{u2}=0.5, TL_{u3}=0.8,sl=1, α=0.6 $\mathbf{W}_{TL}$=(w_{DT},w_{IT})=(0.50,0.50), $\mathbf{W}_{DT}$=(w_E,w_{DK})=(0.75,0.25) $\mathbf{W}_{IT}$=(w_{RC},w_{IK})=(0.75,0.25)	D_1={ 01010 00000 00000 00000 00000 00000 01010 00000 00000 00000}, R_1={0.1, 0.1, 0.1}; D_2={01010 10101 01010 10101 01010 01010 10101 01010 10101 01010}, R_2={0.4, 0.5, 0.6}; D_3={ 11111 10101 10101 10101 11111 11111 10101 10101 10101 11111}, R_3={0.5, 0.7,0.8}; D_4={ 10101 11111 11111 11111 11111 11111 10101 11111 11111 11111}, R={0.7,0.9,0.9};	$TL_{[0,0.19)} \in P_1 = \{\varphi\}$ $TL_{[0.20,0.39)} \in P_2 = \{p_1\}$ $TL_{[0.40,0.59)} \in P_3 = \{p_1,p_2\}$ $TL_{[06,0.79)} \in P_4 = \{p_1,p_2,p_3\}$ $TL_{[0.80,1.00]} \in P_5 = \{p_1,p_2,p_3,p_4\}$

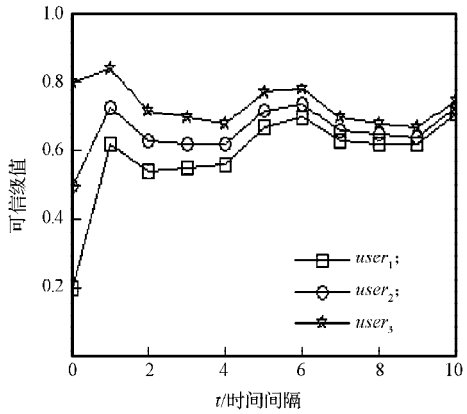
由图4a可知，在第1个和第7个时间间隔，少数合法事件减慢了用户的可信级的下降趋势。但大量的违规事件最终致使 TL_{user}<0.2，根据规则用户将不能获得系统任何权限；由图4d可知，在第1个和第7个时间间隔，违法事件立即拉低了可信级。但通过大量合法事件积累，最终 TL_{user}>0.8，根据规则用户将获得系统所有必要权限；由图4b，4c的度量结果可知，在各个时间间隔用户可信级可快速动态地反应事件性质。综上所述，stTLM模型有效，且具有优异的动态性及细粒度安全特性。



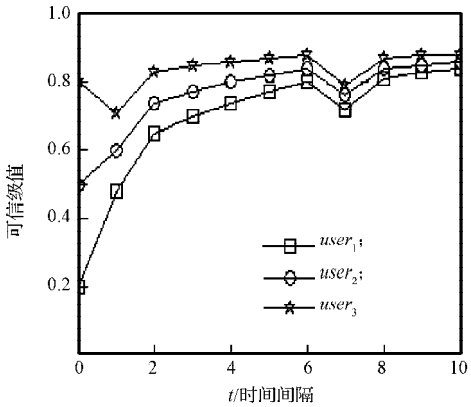
a）数据集1度量



b）数据集2度量



c）数据集3度量



d）数据集4度量

图4 stTLM模型有效性仿真结果

Fig. 4 The simulation result for the effectiveness of stTLM model

5 结语

本文提出了一种基于可信级度量的智能终端安全模型stTLM。模型集成了一种轻量级可信度量机制，通过任务安全分级策略和奖惩机制提供更细粒度的访问授权。模型有效性分析结果表明，本文所给出的模型具有优异的环境适应性及动态性能，且容易实施。

参考文献：

[1] Chen Liang，Jason Crampton. Risk-Aware Role-Based Access Control[C]//7th International Workshop on Security and Trust Management. Berlin：Springer，2012：140-156.

[2] Subhendu Aich，Shamik Sural，Majumdar A K. STARBAC: Spatiotemporal Role Based Access Control[C]// International Conference on OTM Part II. Berlin：Springer，2007：1567-1582.

[3] Tang Zhuo，Wei Juan，Salam Ahmed，et al. A New RBAC Based Access Control Model for Cloud Computing[C]//7th International Conference on Advances in Grid and Pervasive Computing. Berlin：Springer，2012：279-288.

[4] Huang Yong. Reputation and Role Based Access Control Model for Multi-Domain Environments[C]//International Symposium on Intelligence Information Processing and Trust Computing. Huanggang：[s.n.]，2010：597-600.

[5] Covington M J，Moyer M J，Ahamad M. Generalized Role-Based Access Control for Securing Future Applications [C/OL].[2012-04-12]. http://hdl.handle.net/1853/6580.

[6] Aljnidi Mohamad，Leneutre Jean. ASRBAC: A Security Administration Model for Mobile Autonomic Networks (MAutoNets)[C]//4th International Workshop on Data Privacy Management and Autonomous Spontaneous

Security. Berlin：Springer，2010：163-177.

[7] Sandhu R S，Coyne E J，Feinstein H L，et al. Role-Based Access Control Models[J]. IEEE Computer，1996，29(2)：38-47.

[8] Ferraiolo D F，Sandhu R S，Gavrila S I，et al. Proposed NIST Standard for Role-Based Access Control[J]. ACM Transactions on Information Systems Security，2001，4(3)：224-274.

[9] Chadwick D，Otenko A，Ball E. Role-Based Access Control with X.509 Attribute Certificates[J]. IEEE Internet Computing，2003，7(2)：62-69.

[10] Blaze M，Feigenbaum J，Lacy J. RFC 2704：The KeyNote Trust Management System Version 2[S]. Internet Society：Network Working Group，1999：1-37.

[11] Liang Jianmao，Shun Zhenyao，Kai Zhang，et al. Design and Implementation of Document Access Control Model Based on Role and Security Policy[C]//Second International Conference on Trusted Systems. Berlin：Springer，2011：26-36.

[12] Li N H，Winsborough W H，Mitchell J C. Beyond Proof-of-Compliance: Safety and Availability Analysis in Trust Management[C]// IEEE Symposium on Security and Privacy. Oakland：IEEE Computer Society Press，2003：123-139.

[13] Bonatti P，Duma C，Olmedilla D，et al. An Integration of Reputation-Based and Policy-Based Trust Management[C/OL].[2012-04-15]//http://rewerse.net/publications/download/REWERSE-RP-2005-116.pdf.

[14] Woo J W，Hwang M J，Lee M J，et al. Dynamic Role-Based Access Control with Trust-Satisfaction and Reputation for Multi-Agent System[C]//24th International Conference on Advanced Information Networking and Applications Workshops. Perth：Conference Publishing Services，2010：1121-1126.

[15] Takabi H，Amini M，Jalili R. Trusted-Based User-Role Assignment in Role-Based Access Control[C]//International Conference on Computer Systems and Applications. Amman：[s.n.]，2007：807-814.

[16] Qureshi Basit，Min Geyong，Kouvatsos Demetres. Countering the Collusion Attack with a Multidimensional Decentralized Trust and Reputation Model in Disconnected MANETS[J]. Multimed Tools Application. 2011，doi：10.1007/sl 1042-011-0780-7.

[17] Sudip Chakraborty，Indrajit Ray. TrustBAC-Intergrating Trust Relationships into the RBAC Model for Access Control in Open Systems[C]//International Symposium on Access Control Models and Technologoes. NewYork：Association for Coputeing Machinery，2006：49-59.

[18] Li Lei，Wang Yan，Varadharajan Vijay. Fuzzy Regression Based Trust Prediction in Service-Oriented Applications[C]//6th International Conference on Autonomic and Trusted Computing. Berlin：Springer，2009：221-235.

[19] Carles Martinez-Garcí a，Guillermo Navarro-Arribas，Joan Borrell. Intra-Role Progression in RBAC: An RPC-Like Access Control Scheme[C]//6th International Workshop on Data Privacy Management and Autonomous Spontaneus Security. Berlin：Springer，2012：221-234.

[20] Li Lei，Wang Yan. The Study of Trust Vector Based Trust Rating Aggregation in Service-Oriented Environments[J]. World Wide Web，2012，15(5/6)：547-549.

[21] Ray Indrajit，Chakraborty Sudip. A Vector Model of Trust for Developing Trustworthy Systems[C]//9th European Symposium on Research in Computer Security. Berlin：Springer，2004：260-275.

[22] Zhou R，Hwang K. Vectortrust: The Trust Vector Aggregation Scheme for Trust Management in Peer-to-Peer Networks and Networks[C]//18th International Conference on Computer Communications and Networks. San Francisco：CA USA，2009：1-6.

[23] Husseini A El，Abdallah M'Hamed，Bachar EL Hassan，et al. A Noval Trust-Based Authentication Scheme for Low-Resource Devices in Smart Environments[J]. Procedia Computer Science, 2011，5：362-369.

（责任编辑：申 剑）