# 基于Seal演算的分布式系统安全模型

黄 勇 吴尽昭

(广西民族大学信息科学与工程学院 南宁 530006) (中国科学院成都计算机应用研究所 成都 610041)

**摘 要** 针对目前分布式计算安全模型存在的不足,以能有效描述位置和移动性的形式化模型Seal演算为工具,将系统安全属性的刻画归结为系统进程在给定计算环境下的位置互模拟等价,提出一种无干扰安全模型,其可以方便地刻画不同的安全性质。为满足实际安全需求,提出了一种可复合的安全属性,并给出了相应的证明。最后,通过实例分析表明了模型的有效性。

**关键词** 分布式系统,Seal演算,位置互模拟,安全模型

**中图法分类号** TP393.8 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.039

## Security Model for Distributed System Based on Seal Calculus

HUANG Yong WU Jin-zhao

(College of Information Science and Engineer, Guangxi University for Nationalities, Nanning 530006, China)

(Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu 610041, China)

**Abstract** To address the weaknesses of the current security model for distributed computation, this paper proposed a non-interference security model, which is described in the setting of Seal calculus. The new model reduces the characterization of systems security to the location bisimulation equivalence of certain processes in which the position and mobility of systems have been taken into consideration. This paper also proved that the model can define a composite security property according to the security requirements of distributed systems. Finally, a case study was illuminated to show the practical application of this model.

**Keywords** Distributed system, Seal calculus, Location bisimulation, Security model

随着计算机技术和网络通信技术的高速发展,一方面,以并发性、分布性、自治性和移动性为主要特征的云计算[1]、物联网[2]等新技术与应用已成为目前业界研究的热点;另一方面,针对这些应用的病毒侵害、网络蠕虫、特洛伊木马等恶意攻击层出不穷。由于这类分布式系统规模庞大、功能复杂,设计之初缺乏安全理论的指导或安全原则未能贯穿始终,各种各样的软件漏洞对系统的安全构成潜在的致命威胁。因此,如何保证分布式系统的安全性始终是开放系统中的一个核心问题。

要解决分布式系统的安全问题,利用形式化方法是一种可行的途径。其中,无干扰(Noninterference)模型是实现多级安全系统(Multi-level Security System)的重要参考模型,为分析系统中隐蔽信息流提供了一种比较直观的定义和方法。最早的无干扰模型是由Goguen与Meseguer[3]基于自动机理论框架提出的,主要是面向确定性系统。由于多数实际应用系统都是非确定性系统,Sutherland[4]以及Wittbold等人[5]提出了更适合非确定系统的无干扰模型。在上述工作的基础上,文献[6-8]对无干扰模型相关问题进行了更深入的研究,利用安全进程代数刻画无干扰安全模型,将系统安全性的验证归结为特定系统进程的弱互模拟等价关系。在文献[10]中,王立斌等人基于π演算给出了移动系统的无干扰安全模型框架,以广泛应用于移动系统的安全分析。然而他们使用的形式化工具限制了模型的表达能力,不具备刻画位置和客观移动机制,因而无法描述在位置失效的情况下移动系统的安全性[9]。在分布式系统安全模型中,位置是一个非常重要的安全要素[11],当我们对同一位置的资源提出内部和外部资源访问请求时,系统应该进行不同的安全检查。然而,文献[11]提出的安全模型无法刻画大型复杂系统的组合安全特性。

针对上述问题,本文综合考虑分布式系统位置失效情况和进程移动性,使用可描述位置和移动进程的形式化工具Seal演算,将系统的安全属性定义为系统进程在给定计算环境中的位置互模拟关系,提出一种新的无干涉安全模型,该模型可以很好地反映位置失效对分布式系统安全性的影响,可以方便刻画不同的无干涉安全性质;同时,针对大型分布式系统的安全分析需求,提出了一种可复合的安全属性,并结合实例进行分析讨论。

到稿日期:2014-08-06 返修日期:2014-11-24 本文受国家自然科学基金(11371003,11461006),广西自然科学基金(2011GXNSFA018154),广西高等学校优秀人才资助计划项目(桂教人[2011]40号),广西高校科学技术研究重点项目(2013ZD021),广西可信软件重点实验室开放课题(kx201122)资助。

黄 勇(1979-),男,博士,副教授,主要研究方向为网络与信息安全、可信软件验证、形式化方法,E-mail:gxunhy@163.com;吴尽昭(1965-),男,博士,教授,博士生导师,主要研究方向为形式化方法、自动推理、验证技术。

## 1 Seal 演算及其定义

Seal 演算[12]是一种描述进程移动和系统安全机制的分布式进程演算，是可清晰描述位置嵌套、程序移动和资源访问控制特性的计算模型。与其他分布式形式工具 π 演算[13]、Ambient 演算[14]相比，Seal 演算在 π 演算的内核上扩展了同步机制和客观移动机制，具有如 portal 边界、父子交互等特殊安全性质，因此非常适合作为探索具有移动进程的分布式系统的安全分析工具。

在标准 Seal 演算中，符号 $m,n,\cdots,x,y,z$ 表示名字，位置 $\eta::=*\mid\uparrow\mid n$，其中 $*$，$\uparrow$ 和 $n$ 分别表示当前 seal，父 seal 和名字为 $n$ 的子 seal；动作 $\alpha::=\overline{x}^{\eta}\langle y\rangle\mid x^{\eta}\langle\lambda y\rangle\mid\overline{x}^{\eta}(y)\mid x^{\eta}(y)\mid open_{\eta}x$，其中 $\overline{x}^{\eta}\langle y\rangle$ 表示在位于 seal $\eta$ 的通道 $x$ 输出不同的名字 $y$，$x^{\eta}\langle\lambda y\rangle$ 表示在位于 seal $\eta$ 的通道 $x$ 输入不同名字 $y$，$\overline{x}^{\eta}(y)$ 表示在位于 seal $\eta$ 的通道 $x$ 发送 seal $y$，$x^{\eta}(y)$ 表示在位于 seal $\eta$ 的通道 $x$ 等待接收一个 seal 并开始名字向量 $y(y_1\cdots y_n)$ 的 $n$ 个复制，$open_{\eta}x$ 表示 seal $\eta$ 的一个 portal 是开放的。进程 $P,Q,R,S::=0\mid P\mid Q\mid(\nu x)P\mid\alpha.P\mid n[P]\mid n[X]$，其中 0 表示不做任何动作的进程，$P\mid Q$ 表示并行组合，$(\nu x)P$ 表示名字 $x$ 被限制在进程 $P$ 范围内使用，$\alpha.P$ 表示执行动作 $\alpha$ 后继续执行进程 $P$，$n[P]$ 表示体为 $P$ 的 seal $n$，$n[X]$ 表示体为 $X$ 的 seal $n$。

本文使用 Seal 演算的标准语法和标准语义，同时不加说明地使用在文献[9]中定义的所有结构同余规则、加热(Heating)关系以及标记转移系统(Labelled Transition System)。为便于描述，将系统中所有名字的安全级别分为高($H$)、低($L$)两个级别，记为 $H\geqslant L$，有如下定义。

**定义 1** 进程的函数 $Res_H:\varepsilon\to\varepsilon$，使得 $\forall P\in\varepsilon,Res_H(P)=(\nu\vec{H})P$，其中 $\varepsilon$ 是所有进程的集合，$\vec{H}$ 为所有高级别名字的向量。

直观上，对于进程 $P$，函数 $Res_H(P)$ 限制了进程中高级别的行为，使得高级别行为只能作为系统的内部操作，无法与外部环境交互，从而可获得进程 $P$ 的高安全级约束。

**定义 2** 函数 $Low_H:\varepsilon\to\varepsilon$，使得 $\forall P\in\varepsilon,Low_H(P)$ 对进程作如下操作，$\forall\alpha$，如果 $lev(\alpha)=H$，则将 $\alpha$ 替换成 $\tau$，其中 $lev(\alpha)$ 表示获取动作 $\alpha$ 的安全级别。

这里，函数 $Low_H(P)$ 把进程 $P$ 中所有高级别操作替换为内部操作 $\tau$，直观上，它表示低级别用户的观察视图，也就是说低级别用户观察到的高级别操作都是 $\tau$。

**定义 3**(上下文 $C()$) 一个上下文 $C()$ 是一个包含零个或多个孔(hole)的进程，孔与 $C$ 的其他部分是并发关系。把一个孔写作()。$C(P)$ 是指进程 $P$ 填充上下文 $C$ 的每个孔后的结果。这里上下文的语法为 $C()::=()\mid C()\mid P\mid C()\mid(\nu x)C()\mid x[C()]$。

## 2 基于位置的无干扰安全模型

本文使用 Seal 演算建立分布式系统的无干扰安全模型，考虑位置是实际分布式系统的一个重要安全属性，我们可以将系统的低安全级别行为不依赖于高安全级别行为的安全性质归结为验证基于位置的进程行为互拟等价，即进程是行为安全的，当且仅当将低级别用户无法区别进程有高级别操作的行为与没有高级别操作时的行为。进一步分析，根据位置的不同，还可以得出该进程的不同安全属性。

**定义 4**(基于位置的无干扰安全模型) 对任意基于位置的进程等价关系 $\mathcal{R}$，在任意给定的上下文环境 $C$，称进程 $P$ 在 $C$ 下是 $\mathcal{R}$ 行为安全，记为 $P\in NNI^{C}_{\mathcal{R}}$，当且仅当 $\forall P\in\varepsilon$，都有 $(C[Low_H(P)],C[Res_H(P)])\in\mathcal{R}$。

这里，上下文环境对进程 $P$ 来说是一个外部环境，当一个进程进入一个外部环境时，如果进程与下上文环境中的其它任意进程(含恶意进程)进行交互时，低安全级别用户都无法观察进程高安全级别行为在交互后发生的变化，即没有任何恶意进程能够影响低级别用户的观察视图。定义 4 在引入位置的概念后，也同样要求不能影响低级别用户的观察视图，如果上述关系成立，则进程 $P$ 是安全的。本文用下标 $l$ 表示基于位置的等价关系。

**命题 1** 对任意上下文环境 $C$，我们有 $NNI^{C}_{\sim_l}\subseteq NNI^{C}_{\dot{\sim}_l}\subseteq NNI^{C}_{\approx_l}\subseteq NNI^{C}_{\overset{*}{=}_l}$，其中 $\sim_l$ 是基于位置的 Barbed 等价，$\dot{\sim}_l$ 是基于位置的强 Barbed 互模拟等价，$\approx_l$ 是基于位置的弱 Barbed 等价，$\overset{*}{=}_l$ 是基于位置的弱 Barbed 互模拟等价。

证明：因为 $\overset{*}{\approx}_l$ 蕴涵 $\approx_l$，$\approx_l$ 蕴涵 $\overset{*}{\sim}_l$，$\overset{*}{\sim}_l$ 蕴涵 $\sim_l$，易得证。

该命题说明，基于位置的等价关系建立的无干扰传递安全性质是一种比基于计算上下文(环境、域)[9]等价关系更强的安全性质。显而易见，进程的安全性主要取决于分析进程所用的等价关系[11,15]，而非进程所处的上下文环境。同样，一定条件下安全的系统，在增加了安全要素后，该系统无法满足指定的安全属性，则可能被视为不安全的。从这种意义上说，系统安全性与所处的外部环境无关，而是取决于系统的某种无干扰安全性质，因为恶意攻击是任何系统都可能遇到的，如果仅仅考虑环境因素，就无法限制某些类型的恶意攻击，因此我们必须考虑针对某种类型的攻击建立合适的无干扰安全性质，用于检验系统在该约束条件下是否安全。

**命题 2** $\forall P,Q\in NNI^{C}_{\mathcal{R}}\not\Rightarrow(P\mid Q)\in NNI^{C}_{\mathcal{R}}$

证明：只需给出反例，取 $P=\overline{b}^{\eta}_{L}\langle x\rangle.a^{\eta}_{H}\langle x\rangle$，$Q=\overline{a}^{\eta}_{H}\langle y\rangle\cdot b^{\eta}_{L}\langle y\rangle+b^{\eta}_{L}\langle y\rangle$，在任意上下文环境 $C$ 下关于位置 $\eta$ 存在任意等价关系 $\mathcal{R}$，显然有 $P,Q\in NNI^{C}_{\mathcal{R}}$。由于 $Res_H(P\mid Q)\to a^{\eta}_{H}\langle x\rangle$，而 $Low_H(P\mid Q)$ 却没有与之对应的操作结果。

在动态恶意环境下，不仅系统运行时的进程会动态地改变，而且高级别恶意进程也是可以动态配置的。显然，系统的安全性质也会动态地发生变化，所以需要一种更强的安全属性来检查系统的所有可达状态。因此，本文提出了便于验证的强 $NNI^{C}_{\mathcal{R}}$(Strong $NNI^{C}_{\mathcal{R}}$，简称 $sNNI^{C}_{\mathcal{R}}$)安全属性，要求在动态环境下系统的每一个状态都满足 $NNI^{C}_{\mathcal{R}}$。

**定义 5**(可持续的强无干扰安全性质) 如果 $P\in NNI^{C}_{\mathcal{R}}$，则对任意由 $P$ 可达的状态 $P'$，都有 $P'\in NNI^{C}_{\mathcal{R}}$，则有 $P\in sNNI^{C}_{\mathcal{R}}$。

$NNI^{C}_{\mathcal{R}}$ 性质在选择算子和并行算子上都没有组合的性质，但是在验证一个大型复杂系统的安全性时，我们希望能够将其分解成许多小的简单子系统的组合，这时组合的性质就很重要了。而上面提出的 $sNNI^{C}_{\mathcal{R}}$ 就具备这一组合性质，下面给出相关命题和证明。

**引理 1** 如果 $(C[Low_H(E)],C[Low_H(F)])\in\mathcal{R}$，那么 $\forall P\in\varepsilon$，都有 $(C[Low_H(E\mid P)],C[Low_H(F\mid P)])\in\mathcal{R}$。

证明：事实上，我们可以通过可能的几种情况证明以上关系。

• 如果有 $Low_H(E|F)\xrightarrow{\tau}Low_H(E'|F')$，显然有 $E\xrightarrow{a}E'$和 $F\xrightarrow{\bar{a}}F'$，那么同样有 $Low_H(E)|Low_H(F)\xrightarrow{\tau}\xrightarrow{\tau}Low_H(E')|Low_H(F')$。因此我们可得$(C[Low_H(E|P)],C[Low_H(F|P)])\in\mathcal{R}$。

• 如果有 $Low_H(E|F)\xrightarrow{a}Low_H(E'|F)$，显然有 $E\xrightarrow{a}E'$，那么同样有 $Low_H(E)|Low_H(F)\xrightarrow{a}Low_H(E')|Low_H(F)$。因此可得$(C[Low_H(E|P)],C[Low_H(F|P)])\in\mathcal{R}$。

**命题 3** 如果 $E,F\in sNNI_{\Re}^{\zeta}$，那么有 $E|F\in sNNI_{\Re}^{\zeta}$。

证明：需要证明如下情况：如果 $E,F\in sNNI_{\Re}^{\zeta}$，那么对于它们的任何后续状态 $E'$和 $F'$，都有 $E'|F'\in NNI_{\Re}^{\zeta}$，例如$(C[Low_H(E'|F')],C[Res_H(E'|F')])\in\mathcal{R}$。根据定义 5 可知，任意 $sNNI_{\Re}^{\zeta}$进程的所有后续状态都是 $NNI_{\Re}^{\zeta}$。因此，实际上可以视如上关系为一弱位置互拟关系。

事实上，可以通过各种可能的情况证明以上关系。假设有$(C[Low_H(E|F)],C[Res_H(E|F)])\in\mathcal{R}$，由于 $C$ 中的空位与 $C$ 的其它部分是并发关系，为便于描述，我们将上述等价关系简化为$(Low_H(E|F),Res_H(E|F))\in\mathcal{R}$，下面首先考虑最感兴趣的情况：$Low_H(E|F)$的迁移。

• 如果有 $Low_H(E|F)\xrightarrow{\tau}Low_H(E'|F')$，显然有 $E\xrightarrow{a_H^{\eta}\langle x\rangle}E'$和 $F\xrightarrow{\overline{a_H^{\eta}\langle x\rangle}}F'$，那么有 $Res_H(E|F)\xrightarrow{\tau}Res_H(E'|F')$。因此可得$(C[Low_H(E'|F')],C[Res_H(E'|F')])\in\mathcal{R}$。

• 如果 $Low_H(E|F)\xrightarrow{\tau}Low_H(E'|F)$且 $E\xrightarrow{a_H^{\eta}\langle x\rangle}E'$，同时由于$(Low_H(E),Res_H(E))\in\mathcal{R}$，那么存在 $E_1$ 使得 $Low_H(E)\overset{\tau}{\Rightarrow}Low_H(E_1)$和$(Low_H(E_1),Res_H(E_1))\in\mathcal{R}$、$(Low_H(E_1),Res_H(E'))\in\mathcal{R}$，这里的 $E_1$ 显然是 $sNNI_R^{\zeta}$。因此，我们也可以得到 $Low_H(E|F)\overset{\tau}{\Rightarrow}Low_H(E_1|F)$。现在我们可以证明$(Low_H(E'|F),Res_H(E_1|F))\in\mathcal{R}$。因为$(Low_H(E_1|F),Res_H(E_1|F))\in\mathcal{R}$显然是成立的。结合引理 1，可得$(Low_H(E'|F),Res_H(E'|F))\in\mathcal{R}$。

• 如果 $Low_H(E|F)\xrightarrow{\alpha}Low_H(E'|F)(\alpha\notin Act_H)$，显然有 $Res_H(E|F)\xrightarrow{\alpha}Res_H(E'|F)$。于是有$(Low_H(E'|F),Res_H(E'|F))\in\mathcal{R}$。

• 如果 $Low_H(E|F)\xrightarrow{\alpha}Low_H(E'|F')(\alpha\notin Act_H)$。显然有 $Res_H(E|F)\xrightarrow{\alpha}Res_H(E'|F')$。于是有$(Low_H(E'|F'),Res_H(E'|F'))\in\mathcal{R}$。

类似地，我们可以按照相同的方法证明 $Res_H(E|F)$迁移后所保持的关系。

• 如果 $Res_H(E|F)\xrightarrow{\tau}Res_H(E'|F')$，显然有 $E\xrightarrow{\alpha}E'$和 $F\xrightarrow{\bar{\alpha}}F'(lev(\alpha)\neq H)$，那么同样有 $Low_H(E|F)\xrightarrow{\tau}Low_H(E'|F')$，因此可得$(C[Low_H(E'|F')],C[Res_H(E'|F')])\in\mathcal{R}$。

• 如果 $Res_H(E|F)\xrightarrow{\alpha}Res_H(E'|F)(lev(\alpha)\neq H)$。显然有 $Low_H(E|F)\xrightarrow{\alpha}Low_H(E'|F)$。于是有$(Low_H(E'|F),Res_H(E'|F))\in\mathcal{R}$。

## 3 实例分析

在本小节，我们通过一个具体的实例来说明在实际移动应用中的策略表达与分析能力。本文以文献[6]中的访问控制器为实例，说明如何利用基于位置的无干扰安全属性分析实际系统的信息流安全，该系统本质上可以视为一个防火墙应用。下面给出访问控制器的 Seal 演算形式描述。

$$\text{Agent}\triangleq(\text{Server}_H[S]|\text{Server}_L[C])$$

$$S\triangleq r_{HH}^{\eta}(x)\cdot S|\overline{w}_{HH}^{\eta}(y)\cdot S|\overline{w}_{LH}^{\eta}(y)\cdot S$$

$$C\triangleq r_{HL}^{\eta}(x)\cdot C|r_{LL}^{\eta}(x)\cdot C|\overline{w}_{LL}^{\eta}(y)\cdot C$$

图 1 基于 Seal 演算的访问控制模型

这里我们将它抽象成一个拥有两个安全域的分布式 Agent系统，该系统满足无干扰多级安全，我们将这两个区域对象分别用 seal $Server_H$ 和 seal $Server_L$ 表示，$Server_H$ 模拟高安全级别的服务 Agent，$Client_L$ 模拟低安全级别的服务 Agent，高安全级别服务 Agent 的实体进程是 $S$，低安全级别服务 Agent 的实体进程是 $C$。$Server_H$ 通过输出动作 $r_{HH}^{\eta}(x)$传值给高级别用户，通过输入动作$\overline{w}_{HH}^{\eta}(y)$、$\overline{w}_{LH}^{\eta}(y)$分别与高级别、低级别用户交互更新数据。同样地，$Server_H$ 通过输出动作 $r_{HL}^{\eta}(x)$、$r_{LL}^{\eta}(x)$分别传值给高级别用户和低级别用户，通过输入动作 $\overline{w}_{LL}^{\eta}(y)$与低级别用户交互更新数据。其中，$r$ 通道表示读，$w$ 通道表示写，第一个下标表示用户的安全级别，第二个下标表示被访问对象的安全级别，$\eta$ 表示位置。在实例中，高级别行为包括 $r_{HH}^{\eta}(x)$、$\overline{w}_{HH}^{\eta}(y)$和 $r_{HL}^{\eta}(x)$，若 $\eta$ 取不同的值，我们易证$(C[Low_H(Agent)],C[Res_H(Agent)])\notin\mathcal{R}$，Agent 显然无法满足 $sNNI_{\Re}^{\zeta}$属性，因此，Agent 是不安全的。如果 $\eta$ 取同一位置，那么我们容易证明 Agent 满足 $sNNI_{\Re}^{\zeta}$属性，因此 Agent 是关于位置 $\eta$ 的无干扰安全。

**结束语** 本文使用 Seal 演算定义了一个可适用于分布式系统安全分析的无干扰安全模型，在定义中强调了位置的概念，形成对不干涉安全定义新的认识；提出了一种可复合的安全属性，并给出了相应的证明和实例分析。文献[6,10,11]也试图建立分布式系统安全模型统一框架，但他们的研究工作要么没有考虑位置对系统安全性的影响，要么所使用的形式化工具表达能力有限，无法显式描述系统的分布特性、位置概念和组合特性，因此很难分析验证实际分布式系统的安全性。而本文提出的模型具有很强的表达能力，可直观地体现分布和移动特性，具备位置概念，可灵活定义不同安全性质且具有组合特性，能更好地应用于分布式系统的安全分析中。我们下一步的研究工作将在模型中引入非传递无干扰安全策略，实现对信道过滤和安全降幂等安全问题的分析。

## 参 考 文 献


[1] Fernando N, Loke S W, Rahayu W. Mobile Cloud Computing: a Survey [J]. Future Generation Computer Systems, 2013, 29(1): 84-106

[2] Roman R, Zhou Jian-ying, Lopez J. On The Features and Challenges of Security and Privacy in Distributed Internet of Things [J]. Computer Networks, 2013, 7(10): 2266-2279

[3] Goguen J A, Meseguer J. Security Policies And Security Models [C]// Proc. IEEE Symp. on Security and Privacy. 1982: 11-20

[4] Sutherland D. A Model of Information [C]// Proc. National Computer Security Conf.. 1986: 175-183

[5] Wittbold J T, Johnson D M. Information Flow in Nondeterministic Systems[C]// Proceedings of IEEE Symp. on Security and Privacy. IEEE Computer Society Press, 1990: 144-161

[6] Focardi R, Corrieri R. Classification of Security Properties (Part

I:Information Flow)[J]. Foundations of Security Analysis and Design-Tutorial Lectures, Springer-Verlag, volume 2171 of LNCS,2001:331-396

[7] Focardi R,Rossi S. Information Flow Security in Dynamic Contexts [J]. Journal of Computer Security,2006,14 (1):65-110

[8] Oheimb D. Information Flow Control Revisited:Noninfluence= Noninterference+ Nonleakage [C]// Proceedings of European Symposium on Research in Computer Security 2004 (ESORICS' 04). Springer-Verlag, Vol. LNCS 3193,2004:225-243

[9] Riely J, Matthew H. Distributed Processes and Location Failures [J]. Theoretical Computer Science Archive, 2001, 266 (122): 693-735

[10] 王立斌,陈克非. 可移动系统安全模型统一框架[J]. 电子学报,2002,30(12A):2108-2110
Wang Li-bin, Chen Ke-fei. A Uniform Framework of Security Model for Mobile Systems [J]. Acta Electronica Sinica,2002,30 (12A):2108-2110

[11] 余万涛,胡光锐. 考虑位置失效的移动系统安全模型[J]. 计算机应用研究,2006,10:128-129
Yu Wan-tao, Hu Guang-rui. Security Model for Mobile Systems with Location Failures [J]. Application Research of Computers, 2006,10:128-129

[12] Castagnaa G, Vitekb J, Zappa Nardelli F. The Seal Calculus [J]. Information and Computation,2005,201(1):1-54

[13] Davide Sangiorgi, David Walker. The Pi-Calculus: A Theory of Mobile Processes [M]. Cambridge University Press,2002

[14] Cardelli L, Gordon A D. Mobile Ambients [J]. Foundations of Software Science and Computation Structures, LNCS, 1998, 1378:140-155

[15] Bugliesi M,Gallina L,Hamadou S,et al. Behavioral Equivalences and Interference Metrics for Mobile Ad-Hoc Networks [J]. Performance Evaluation,2014,73:41-72

(上接第 164 页)

由于两种方法实际采样的次数不一样,因此评价 Miss Ratio 不具有可比性,因而本文直接比较两种方法实际获取的事件数,结果如图 3 所示。

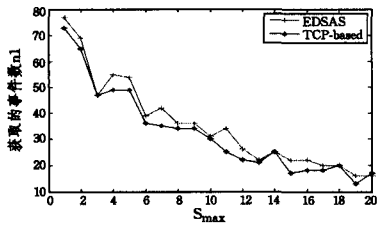


图 3 不同最大步长下获取的事件数对比

由图可见,基于 TCP 的方法获取的事件数与 EDSAS 方法基本一致,没有丢失重要的事件。接下来,衡量不同阈值对采样率和事件丢失率的影响。取 $S_{max}=8$ 的情况,基于不同的相对阈值得到的结果如图 4、图 5 所示。

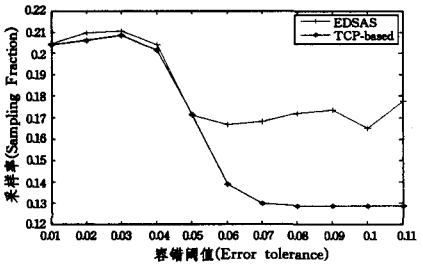


图 4 不同最大容错率下的采样率比较

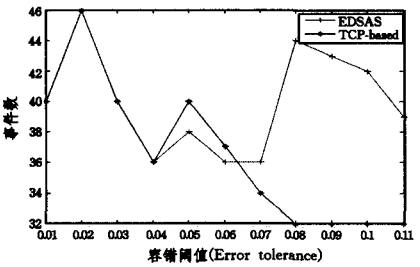


图 5 不同容错阈值下获取的事件数对比

当容错率增加时,采样率快速下降,在容错率从 0.05 增至 0.07 时,EDSAS 方法的采样率从 18%降至 17%,而基于 TCP 的采样方法的采样率则从 18%降至 13%,性能优于 EDSAS;在获取事件数方面,两种方法的性能仍基本一致。由此可见,容错率对于算法的影响比较大。针对不同的具体应用场景,需要通过实验来设置合理的参数。对于数据精度与能量损耗两个因素,从图中可以发现适合的参数取值。

**结束语** 算法的参数设置依赖于具体的应用需求,该算法针对场景选择合适的参数,能够很好地动态调整采样间隔并尽可能地获取重要信息。当预测误差低于阈值时,步长 $k$ 增大,这样可以让传感器节点避免对不需要的数据点进行采样。另一方面,如果预测误差超过了阈值,或者是检测到了事件,算法将降低 $k$ 的值,在较小的采样间隔上采样,以避免丢失重要的信息。改进后的算法参考 TCP 拥塞控制的思想,使得 $k$ 的调整能够快速响应变化。实验结果表明,该算法进一步提高了采样率调整的有效性。该算法计算简单,在资源受限的节点上易于实现。

## 参 考 文 献

[1] Gupta M,Shum L V,Bodanese E,et al. Design and evaluation of an adaptive sampling strategy for a wireless air pollution sensor network[C]// 2011 IEEE 36th Conference on Local Computer Networks (LCN). IEEE,2011:1003-1010

[2] Werner-Allen G, et al. Monitoring volcanic eruptions with a wireless sensor network[C]// Proceedings of the Second European Workshop on Wireless Sensor Networks,2005. 2005:108-120

[3] Alippi C,et al. Energy management in wireless sensor networks with energy-hungry sensors[J]. Instrumentation & Measurement Magazine,IEEE,2009,12(2):16-23

[4] Alippi C, et al. Adaptive Sampling for Energy Conservation in Wireless Sensor Networks for Snow Monitoring Applications [C]// IEEE International Conference on Mobile Adhoc and Sensor Systems(MASS 2007). 2007:1-6

[5] Alippi C, Roveri M. An adaptive CUSUM-based test for signal change detection[C]// Proceedings of 2006 IEEE International Symposium on Circuits and Systems(ISCAS 2006). 2006:5752-5755

[6] Wright D J. Forecasting Data Published at Irregular Time Intervals Using an Extension of Holt's Method[J]. Management Science,1986,32(4):499-510