

基于动态窗口的行为证据采集系统

肖 夏, 陈 岚, 李 莹

(中国科学院 微电子研究所, 北京 100029)

摘 要: 为了克服无线传感器网络中传统证据采集方式的滞后性和低精确性等缺陷, 采用基于窗口函数的动态采集方法, 利用窗口函数的快速响应、平缓恢复等特点, 设计了一套集证据指标、波动评估、动态窗口为一体的行为证据采集系统, 对网络中潜在的各类波动进行快速响应与追踪. 通过对窗口函数系数的数学推导和仿真测试, 证明了证据采集的实时性、准确性和有效性, 从而提高了行为证据采集的准确性, 为后续证据融合、可信分析提供了便利.

关键词: 无线传感器网络; 可信网络; 证据采集; 动态窗口技术

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2015)02-0010-05

An Evidence Collection System Based on Dynamic Window

XIAO Xia, CHEN Lan, LI Ying

(Institute of Micro-Electronics, Chinese Academy of Sciences, Beijing 100029, China)

Abstract: In order to conquer the high-latency and low-accuracy of traditional evidence collection method, we introduce a dynamic collecting mechanic, taking advantage of the rapid responsive, slow recovery characteristic of window function. We design a comprehensive evidence collection system, combining with evidence indicator, fluctuation evaluation, and dynamic evidence window, to rapidly follow the change of network. By math deduction and experimental testing, we verify the validity, accuracy and effectiveness of the system.

Key words: Wireless Sensor networks; Trusted Networks; Evidence Collection; Dynamic Evidence Window

1 引言

由于无线传感器网络应用广泛、环境复杂, 可信网络^[1]是确保无线传感器网络可靠性、安全性的关键技术之一. 证据是可信网络的基础组成部分. 证据分为身份证据和行为证据. 以密码学为基础的身份证据理论不能够适应无线传感器网络的复杂环境、低计算资源、易失效和易遭受攻击等极端条件. 必须通过行为证据分析对节点进行综合评估. 当前证据采集技术的主要缺点有如下: 有效证据深度过长导致系统对波动响应延时过长; 历史证据对当前证据影响较大, 使信度计算结果不准确; 缺乏对无线传感器网络证据指标的量化定义; 未对采集证据进行筛选导致融合计算量较大等. 本文设计一套适用性广、采集精度高、实时性强的证据采集系统. 既能对证据

进行全面的评估, 又能适应动态变化的网络.

2 证据采集系统的设计

2.1 证据系统框架:

2.1.1 证据定义

证据观测域是节点能够通过软件或者硬件检测获得的能够定量描述的行为证据的集合, 集合的每一个元素称为行为证据. 每一个行为证据是由一个确定维度的互动观测矩阵量化的, 行为证据矩阵是对观测矩阵进行的平均量化评估.

2.1.2 观测矩阵(Observation Array, OA)

观测矩阵是施信节点与受信节点每次交互的结果集合. 每次交互结果都根据行为证据进行分类归一化量化, 并作为观测集合元素储存在交互双方节点中. 单次观测矩阵 (Single Observation Array,

收稿日期: 2014-04-11; 修回日期: 2014-06-01

基金项目: 中国科学院重点部署项目“规模化物联网应用系统开发与示范验证”(KGZD-EW-102-1)

SOA)的维度由行为证据的维度决定,观测矩阵(OA)的横向维度由证据生存时间决定。

设有某无线传感器网络中有 D 维行为证据,生存时间为 U ,单次观测矩阵定义为

$$SOA_i = [\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_D]^T \quad (1)$$

观测矩阵定义为

$$OA = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1U} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2U} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{D1} & \alpha_{D2} & \dots & \alpha_{DU} \end{bmatrix} \\ = [SOA_1 \quad SOA_2 \quad \dots \quad SOA_U] \quad (2)$$

2.1.3 行为证据(Behavior Evidence, BE)

行为证据是由观测矩阵获得的统计学结果。行为证据具有三个主要性质^[2]。第一,可观测性。行为证据可以被传感器节点的软件或者硬件检测,并且为了保证信任系统的普适性和可移植性,观测应当是普适性的观测,特别不能是以特殊的硬件为基础而得到的证据。第二,可量化性。行为证据可以用 $[0, 1]$ 区间的归一化形式进行量化,不可是自然语言表述的、模糊的。第三,客观性。行为证据必须是客观评价的,是网络普适的,不以观测节点的个体需求而改变。

在无线传感器网络中,行为证据为影响传感器网络可靠性与安全性的基础指标,包括且不仅限于以下几点。

(1)节点剩余能量。能量是无线传感器网络的重要制约因素,高能量节点可以承担较为繁重的工作,而低能量的通常会减少与其他节点的交互^[3],因此剩余能量是预测目标节点行为的重要指标。

(2)节点安全等级。节点安全等级为节点进行加密、认证、密钥分配、入侵检测的能力。在网络部署时,会有一些节点的计算、存储能力相对较高。高安全等级的节点能对报文进行更为可靠的加密和认证,因此安全等级计入基础指标。

(3)节点回应速度。该指标指示了节点反映的速度,如果快速响应,则说明节点相对空闲、信道质量较高;如果长时间无响应,则该节点可能发生了失效、位移、拥塞等情况。

(4)节点报文转发率。正常情况下具有路由功能的节点应正确对报文进行转发,但恶意节点、失效节点会不可预测地丢失报文,不应获得路由能力。因此,报文丢失率是一项重要指标。

(5)节点位置稳定性。传感器网络中,变化拓扑是一项极富挑战的课题。因为节点不断变化的位置

会导致重定位、路由变化、自动增益控制失效等危害。因此节点位置稳定性表征了节点的可靠程度,是节点稳定性的重要指标。

(6)交互频度。该指标反映了施信节点与受信节点单位行为时间内交互的次数。交互频度的高低反映了交互结果的可信程度。交互程度越高,则交互结果证据样本充分,结果相对可信。交互程度越低,则交互证据样本相对不足,可信度低。

(7)交互量级。该指标反映了节点间每次互动的重要程度。该指标主要用于两个方面:第一,当节点证据采集不充分时作为动态权值扩展的依据;第二,防止节点进行大量低量级交互而恶意抬高自身信度的攻击。

(8)交互成功率。反映了节点间报文转发、数据获取等行为的成功率,直接反映了受信节点配合行为的比率。

但是,任何单一的基础指标都不能作为直接判断依据。因为单一指标在不同环境下波动较大,特别是在传感器网络所处的恶劣环境下,以单一指标作为判断依据只能体现网络节点的绝对环境,而不能反映网络节点的相对环境。由于信任度具有相对性,因此需要综合利用以上证据获得更为精确的信度结果。

定义行为证据矩阵 BE :

$$BE \\ = \left[\frac{\sum_{i=1}^U \alpha_{1i}}{U} \quad \frac{\sum_{i=1}^U \alpha_{2i}}{U} \quad \dots \quad \frac{\sum_{i=1}^U \alpha_{Di}}{U} \right]^T \\ = [\beta_1 \quad \beta_2 \quad \dots \quad \beta_D]^T \quad (3)$$

2.1.4 生存时间(Survival Time)

普遍来说,在相对较近的互动具有更高的参考价值,因此观测集元素应存在一定的生存时间,在生存时间内的证据被视为有效证据,而超过生存时间的证据参考性较低,被视为无效证据。由于存储空间和计算能力的限制,定义有效证据时间 U ,在 U 之内的证据为有效证据,在 U 之外的证据为无效证据,将被系统删除以节省存储空间。有效时间 U 即为观测集深度,不需要对有效证据进行衰减。

2.2 波动评估和动态窗口

网络波动是指网络当前一段时间所处的状态与历史长期所处的稳定状态存在较大差异的情况。网络波动分为突发波动和持续波动。突发波动指网络状态由稳定突发改变到另一个稳定状态;持续波动指网络任一时刻的状态是随机不稳定的。本文采用波动评估机制结合动态证据窗口机制,对网络的波

动进行量化评估. 对处于波动中的网络, 通过降低证据的采集窗口提高近期证据所占据的比重, 对信任度计算产生较大影响, 加快网络对波动的响应速度和准确性.

2.2.1 波动评估模块

波动评估模块利用当前时刻可以采集到的信息, 对网络所处的状况进行评估, 并且量化确定网络的波动情况, 输出波动反馈系数 R .

首先定义波动评估深度 F , 在观测矩阵 (OA) 中提取最近 F 组观测结果组成近期证据矩阵 FOA , 定义 FOA 为

$$FOA = \begin{bmatrix} \alpha_{1(U-F+1)} & \alpha_{1(U-F+2)} & \cdots & \alpha_{1U} \\ \alpha_{2(U-F+1)} & \alpha_{2(U-F+2)} & \cdots & \alpha_{2U} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{D(U-F+1)} & \alpha_{D(U-F+2)} & \cdots & \alpha_{DU} \end{bmatrix} \quad (4)$$

接下来对矩阵 FOA 求均值, 获得近期行为证据矩阵 FBE , 定义为

$$\begin{aligned} FBE &= \left[\frac{\sum_{i=U-F+1}^U \alpha_{1i}}{F} \quad \frac{\sum_{i=U-F+1}^U \alpha_{2i}}{F} \quad \cdots \quad \frac{\sum_{i=U-F+1}^U \alpha_{Di}}{F} \right]^T \\ &= [\gamma_1 \quad \gamma_2 \quad \cdots \quad \gamma_D]^T \end{aligned} \quad (5)$$

由于矩阵间的欧氏距离在矩阵元素较多时可能会掩盖个别差异化元素, 而任何差异元素都可能预示着网络处于波动中, 因此, 定义波动评估参数 R 为行为证据矩阵 (BE) 和近期行为矩阵 (FBE) 元素距离的最大值通过检测波动最大的元素表征网络的波动情况. 定义:

$$\begin{aligned} R &= \max \{ D(FBE, BE) \} \\ &= \max \{ |\beta_1 - \gamma_1|, |\beta_2 - \gamma_2|, \cdots, |\beta_D - \gamma_D| \} \end{aligned} \quad (6)$$

2.2.2 动态证据采集窗口 (Dynamic Evidence Window DEW)

由于传感器网络具有不确定性, 通常会受到其他信号的干扰, 导致网络状态波动. 对于处于波动中的网络, 在生存时间之内, 其相对近期的有效证据 (低深度证据) 具有较高的参考价值, 而相对长期的有效证据 (高深度证据) 的参考价值较低. 例如, 当节点因被入侵而发生信任度突变时, 固定证据窗口会因大量的历史记录而导致目标节点的信任度变化缓慢, 从而使节点遭受大量的攻击; 或因历史记录过少导致目标节点信任度剧烈波动. 因此, 本文采用动态窗口技术, 通过当前信任度和上一节点信任度的变化来确定网络的波动情况, 并根据网络的波动情况相应地增长或者缩短证据窗口. 当网络波动相对平

缓时, 证据窗口长度趋向于生存时间 U (最大深度), 当网络波动剧烈时, 证据窗口长度趋向于最小值.

网络波动情况由决策反馈域的波动预测模块提供, 窗口大小的调整方式符合窗口函数:

$$DEW = DEW \times \left[1 + K \times \ln \left(\frac{2}{R+T} - 1 \right) \right] \quad (7)$$

函数在 $[0, 1]$ 区间内曲线如图 1 所示.

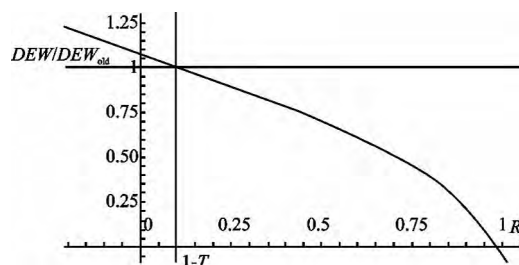


图 1 窗口函数

其中系数 K 为窗口系数, T 为阈值系数. 由图 1 可以看出, 动态窗口 DEW 是反馈系数 R 的凸函数, 因此当 R 小于阈值 ($R < 1 - T$), 网络波动可忽略, 窗口平缓增加; 当 R 较小时 ($R \approx 1 - T$), 网络波动较小, 窗口平缓减小; 相反的, 当网络波动剧烈导致 R 较大时 ($R \gg 1 - T$), 窗口迅速减小, 以适应网络的剧烈波动. 快速响应、平缓恢复的设计, 符合稳定性设计的一贯思路.

动态窗口 DEW 、波动评估深度 F 和生存时间 U 示意图如图 2 所示.

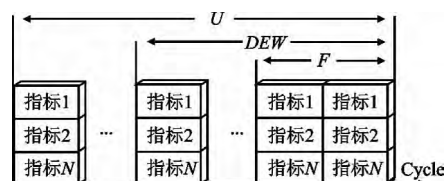


图 2 窗口示意图

与其他波动适应技术相比, 动态窗口技术不仅高度适应网络波动, 同时也没有完全清除历史记录, 当网络从突发扰动中恢复时, 长期证据的存在依然能够使节点获取相对完整的证据, 从而保证信任度计算的准确性.

2.2.3 相关系数的进一步讨论

(1) 动态窗口 DEW 和波动评估深度 F 的关系

系数 R 为波动评估系数, 具体反映了近期网络行为和长期网络行为的差异程度, 而 R 进而决定了证据窗口的大小, 证据窗口直接决定了近期结果对信任度的影响情况, 即网络对波动的响应情况. 近期

网络行为的深度是由参数 F 决定,因此 F 的大小决定了系统测量波动的能力. F 越大,则长期大幅度波动才能对波动评估参数 R 和信任度产生明显的影响;相反的, F 越小,短期的突发波动就会对波动评估参数 R 和信任度产生显著影响. 当系统当前证据窗口较大时,对近期证据不敏感,因此采用较小的波动评估深度 F 使得系统对短期波动敏感;当系统当前证据窗口较小时,对近期证据较为敏感,因此采用较大的评估深度 F 可以使系统保持相对稳定. 因而使 F 满足:

$$DEW \times F = C \quad (8)$$

且

$$DEW_{\min} > F_{\max} > F_{\min} \geq 2 \quad (9)$$

即可符合上述条件. 参数 C 的大小由实际存储容量决定. 由于 $F_{\min} = 1$ 时会导致网络在持续波动中产生不稳定的情况,因此取 $F_{\min} \geq 2$ 避免信任度的剧烈波动.

(2) 窗口系数 K 的选取与分析

首先讨论 DEW 窗口函数的定义域. 上文讨论的约束对变量 R 最初的取值范围为 $[0, 1]$, 但是, 由于上文讨论结果对其最大值产生一定的约束. R 最大时表示窗口 DEW 和 F 观测差异的最大值, 因此有

$$R_{\max} = \left| \frac{DEW - F}{DEW} \times a + \frac{F}{DEW} \times b - F \times b \right|, \quad a, b \in [0, 1] \quad (10)$$

最坏情况下, a, b 差值最大, 即 $a = 0$ 且 $b = 1$, 或 $a = 1$ 且 $b = 0$. 带入上式可得

$$R_{\max} = 1 - \frac{F}{DEW} \quad (11)$$

由式(8)可知, 当 F 最小时 DEW 取最大值, 此时系数 R 为最大值, 且对任何 $F > F_{\min}$, 都会使得 $R < R_{\max}$. 因此取 $F = 2$ 并将式(8) 带入式(11) 可得 DEW 窗口函数定义域为

$$R \in [0, \frac{4}{C}].$$

(3) 函数的值域

在 R 取值范围内, DEW 必须为正值, 因此在 R 定义域内, 必须使得 $DEW > 0$. 换言之, 根据函数单调性, 当 $DEW = 0$ 时, R 必须满足

$$\frac{4}{C} < R.$$

将上述条件带入式(7), 可得

$$0 < K < -\ln^{-1}\left(\frac{C}{C-2} - T\right) \quad (12)$$

即当 K 满足上式条件时, 函数取值均大于零.

从上式可知, 参数 K 的取值由常数 C 和阈值 T 共同决定, 且 C 和 K, T 呈负相关.

(4) 阈值系数 T . 阈值系数 T 为函数平移量, 反映了网络对波动的敏感程度. 当 $R > T$ 时, 窗口根据 $R-T$ 距离减小; 当 $R < T$ 时, 窗口根据 $T-R$ 距离增大. 因而 T 的取值决定了网络对何种程度的波动做出响应, 即网络对波动的敏感程度. T 的取值范围为 $[0, 1]$. 通常, 为了确保系统快速响应, 应取 $T > 0.6$.

3 仿真结果

本文对无线传感器网络中可能出现的几类具有代表性的情况进行仿真测试, 网络突发波动, 网络短时波动、和网络持续波动三类. 仿真中默认设置参数为 $K = 0.35, C = 32, DEW_{\text{init}} = 16, T = 0.9$.

3.1 网络突发波动测试

针对节点突发离网、长期失效、长期阻塞等情况进行测试. 假设节点初始工作正常, 各项指标均为 0.9. 在第十个周期突发波动后, 节点除第 2.1.3 节提出的第 2、5、6、8 几项指标基本保持不变外, 其余指标均跳变至 0. 测试观测 30 个互动周期后的结果, 如图 3、图 4 所示.

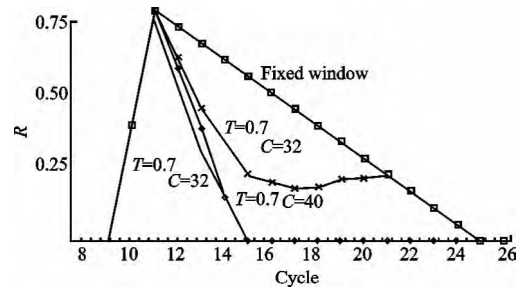


图3 波动系数变化图

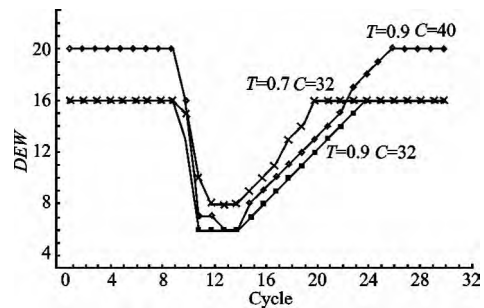


图4 窗口变化图

实验结果中非平滑折线是由于窗口取整引起的. 由于突变前后状态稳定, 可以认为突变后的 FBE 矩

阵为节点新的稳定值,因此波动系数 R 即反映了计算值和实际值的误差.图 2 显示,动态窗口机制相较于固定窗口,其响应速度大幅提高,能够在 4 到 5 个时间周期内将误差降低到 0.1 以下,而固定窗口需要 14 个周期才能实现.阈值 T 的减小使得波动系数降低较慢,但仍然能将波动系数在 5 个周期内降低至 0.2 以下.图 3 显示,本系统对突发波动响应迅速,在两个周期内将 DEW 降至最小值.之后随着网络状况的稳定, DEW 平稳恢复.阈值 T 的减小会使得网络对波动的敏感性降低,窗口减小速度和幅度都相对较小.参数 C 的大小对窗口的影响较小.

3.2 网络短时波动测试

针对节点突发离网、短期失效、短时阻塞等情况进行测试.假设节点初始工作正常,各项指标均为 0.9.第四个周期突发波动后,节点除第 2.1.3 节提出的第 2、5、6、8 几项指标基本保持不变外,其余指标均跳变至 0,经过 10 个周期后,各项指标均恢复至 0.9.本测试观测 35 个互动周期后的结果,如图 5、图 6 所示.

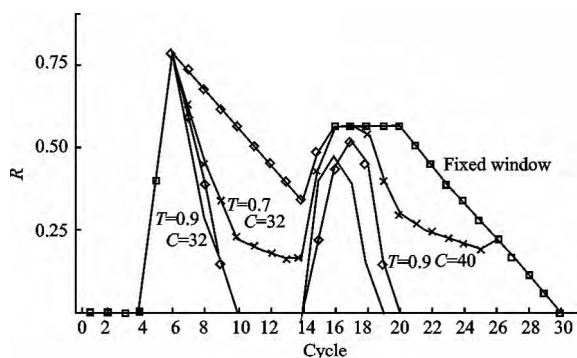


图 5 波动系数变化图

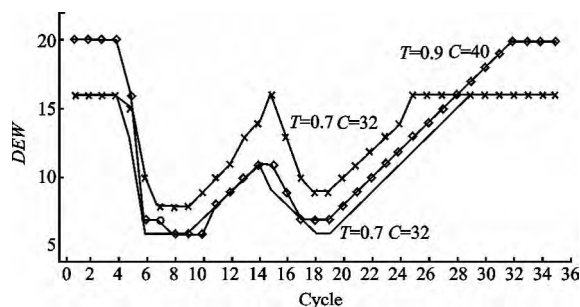


图 6 窗口变化图

短时波动可认为是有一定间隔时间的两次波动.图 5 显示,动态窗口能快速、有效地降低波动系数.对两次波动均迅速做出响应,降低波动系数.阈值 T 减小,使网络在第二次波动前未能将波动系数减小至最小值.图中在 $T=15$ 时,对于 $C=40$ 曲线,

由于其 F 较大导致第二次波动响应减慢了一个周期.因此, C 的大小影响处于波动中节点的响应速度.从图 6 中可以看出,窗口对两次波动十分敏感,第二次波动发生时,窗口均处于恢复过程中,便立即降至最小值,以捕捉网络波动.

3.3 网络持续波动测试

本节主要针对节点遭受持续性干扰的情况进行测试.假设节点初始工作正常,各项指标均为 0.9.第四个周期突发波动后,节点各项指标均发生持续性跳变.本测试观测 30 个互动周期后的结果,如图 7、图 8 所示.

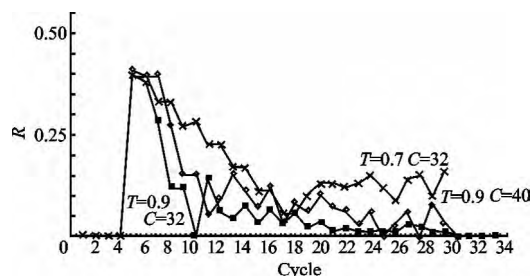


图 7 波动系数变化图

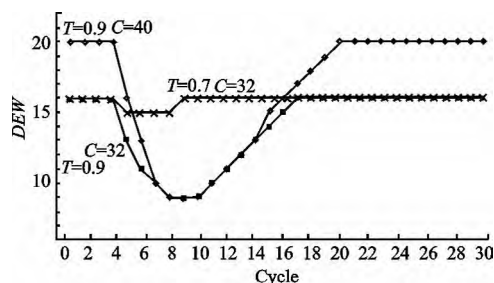


图 8 窗口变化图

对于持续波动,由于窗口 F 内数据取均值,导致其结果与 DEW 窗口结果差异减小,因此可以看到动态窗口减小速度和幅度均有所降低.图 7 中 $T=0.9$ 曲线波动系数在 5 到 6 个周期之后均降低至 0.1 以下,并持续波动,波动幅度较大. T 的减小会导致波动系数在 0.1 以上波动,即 DEW 窗口结果相对准确性较低,但波动幅度较小.应当注意,在持续波动条件下,窗口 F 的值并非为实际波动的数值,因此波动系数较大并不代表系统的误差较大.由图 8 可知, DEW 在一段时间后均恢复至最大值,通过增加采集深度最大限度的减小采集结果的误差.

3.4 与传统固定窗口的比较

根据以上三种情况,对固定窗口和动态窗口进行比较,结果如表 1 所示.

(下转第 19 页)

作为测试数据集运用到该 SSUT 分类后的安全态势评估训练模型中,通过模型的不斷自我学习即可得到态势评估的结果,从而告知网络管理员对标记为-1的不安全网络状态做出相应处理.可见,本文提出的支持扩展指标体系的 SSUT 网络安全态势评估模型对于提高网络安全性和辅助决策能力具有很好的指导作用.

5 结束语

从改进指标分类的角度出发,提出网络安全指标 SSUT 分类方法,建立支持扩展指标体系的 SSUT 网络安全态势评估模型,并结合 SVM 分类方法,将所选取相关指标元素构成的多维向量进行分类和态势评估,从而得到个性化用户对于网络安全态势评估的最佳结果.新模型与以往传统安全指标为基础的态势评估模型相比,在模型的有效性、准确性及扩展性方面有了很大改进;通过加入用户类型指标 User-Type 满足了不同网络用户的个性化网络安全需求,而指标影响因子的引入则对模型的自由度有了很大的提高,实验结果也验证了安全态势评估模型的优越性.

参考文献:

- [1] 龚正虎,卓营.网络态势感知研究[J].软件学报,2010,21(7):1605-1619.
- [2] Zhang Haoliang, Shi Jinqiao, Chen Xiaojun. A multi-level analysis framework in network security situation awareness [J]. Procedia Computer Science, 2013 (17): 530-536.
- [3] Cheng Xiaorong, Lang Su, Li Mingxuan. Research of network security situational assessment quantization based on mobile agent [J]. Physics Procedia, 2012 (25): 1701-1707.
- [4] 吴志军,杨义先.信息安全保障评价指标体系的研究[J].计算机科学,2010,37(7):7-10.
- [5] 丁世飞,齐丙娟,谭红艳.支持向量机理论与算法研究综述[J].电子科技大学学报,2011,40(1):2-10.
- [6] 梁海军.人工蜂群优化支持向量机算法在网络安全中的应用[J].微电子学与计算机,2013,30(2):95-98.

作者简介:

李纪真 男,(1986-),博士研究生.研究方向为计算机网络安全. E-mail:lijizhen1986@126.com.

孟相如 男,(1963-),教授,博士生导师.研究方向为宽带通信网络技术.

(上接第14页)

表1 动态窗口和固定窗口的比较

采用技术	响应速度	平均误差	收敛时间
固定窗口	无	0.5	15个观测周期
动态窗口	1~2个观测周期	<0.1	<5个观测周期

4 结束语

本文针对传感器网络中多证据的体系,设计了一种基于动态证据窗口的证据采集机制.仿真结果表明,对于三类典型的波动情形,动态窗口技术在线性复杂度条件下,其响应幅度、准确率、误差收敛速度上均优于传统固定采集窗口.本文设计的系统可代替传统的固定窗口技术,作为证据理论体系的前端采集模块.广泛适用于各类无线传感器网络.

参考文献:

- [1] 陆三兰,程铭东.基于D-S证据理论的组合数据融合算法[J].微电子学与计算机,2013,30(1):95-98.
- [2] 邓建春.可信网络的信任模型研究[D].成都:电子科技大学,2013.
- [3] 谭运宝,钟诚,张尊国.一种基于邻居合作检测的移动Ad Hoc网络信任模型[J].微电子学与计算机,2008,25(10):227-230.

作者简介:

肖夏 男,(1989-),硕士研究生.研究方向为无线传感器网络. E-mail:xiaoxia@ime.ac.cn.

陈岚 女,(1968-),博士,研究员,博士生导师.研究方向为超深亚微米芯片设计方法学、计算机体系结构及物联网关键技术.

李莹 女,(1982-),博士,副研究员.研究方向为物联网与嵌入式系统设计.