The Realization of Intrusion Detection Algorithm Based on Particle Filtering in WSN*

FENG Libo, LUO Guilan, YANG Cunji, LIAO Jing*

(*Institute of mathematics and computer, Dali University, Dali Yunnan* 671003, *China*)

Abstract: The security problem has become one of the obstacles about further development in wireless sensor networks. An intrusion detection algorithm is proposed which is based on particle filtering. The program used the LEACH algorithm to cluster the nodes in wireless sensor network. Then detected the nodes' data traffic used the particle filter algorithm in order to discover the abnormal node. Using the MATLAB simulate the responsiveness detection rates of the nodes. The simulation results show that the anomaly detection rate was maintained between 0.48 and 0.7 using the particle filter algorithm. The detection system maintains a more stable state. So the particle filter can be better applied to the intrusion detection system in WSN.

Key words: wireless sensor networks; network security; intrusion detection; particle filter; detection rate

EEACC: 7230; 7150P **doi**: 10.3969/j.issn.1004-1699.2013.11.019

WSN 中基于粒子滤波的入侵检测算法实现*

冯立波*, 罗桂兰, 杨存基, 廖 静

(大理学院数学与计算机学院, 云南 大理 671003)

摘 要: 安全问题已经成为无线传感器网络进一步发展和应用的障碍之一。提出了一种基于粒子滤波算法的入侵检测技术, 该方案利用 LEACH 算法对无线传感器网络节点进行分簇, 通过粒子滤波算法对簇内节点的数据流量情况进行检测, 以发现其中的异常节点, 并利用 MATLAB 仿真工具对节点的反应灵敏度及检测率进行仿真。算法计算得出的异常检测率维持在 0.48 到 0.7 之间, 检测系统处于一种较为稳定的状态, 粒子滤波能够较好地应用到 WSN 的入侵检测系统中。

关键词: 无线传感器网络; 网络安全; 入侵检测; 粒子滤波; 检测率

中图分类号: TP391; TN915 **文献标识码**: A **文章编号**: 1004-1699(2013)11-1573-06

安全问题已经成为无线传感器网络进一步发展和应用的障碍之一。无线传感器网络易遭受物理操纵、信息窃听、碰撞、拒绝服务、洪泛、丢弃性破坏等攻击。如何有效的检测和防范这些攻击, 保证传感器网络的正常运行已经成为当前研究热点。入侵检测是一种应用于计算机网络的为保证网络的安全而设计的能够及时发现并报告网络中未授权或异常现象的技术[1-2]。目前, 无线传感器网络中的入侵检测技术通过隐式马尔科夫模型来检测异常行为来进行的[3], 但是对于异常行为没有明确的定义。为了使得入侵检测系统的相关技术更好应用到无线传感器网络中, 文章提出了一种基于粒子滤波的算法, 使其能够适用于无线传感器网络通信质量较弱、传输数据功率较小、处理能力有限等情况。

粒子滤波是一种根据概率分布估算状态方差从而对目标物体进行跟踪的算法[4]。目前粒子滤波算法主要用于对目标进行跟踪, 以估算出运动轨迹[5-6]。文章在用 LEACH 算法[7]对节点进行分簇的前提下, 将这种粒子滤波跟踪算法应用到簇内节点对目标物体进行跟踪时节点状态的变化上, 通过对节点状态的跟踪估算出变化过程中传输的流量值。通过 LEACH 算法进行分簇, 可以使无线传感器网络获得更长的生命周期[8]。通过估算出的流量值与预定义的流量阀值相比较从而计算节点的检测率, 由检测率反应出节点受到攻击的情况以及当前网络的安全状态。

1 粒子滤波流量预测算法

1.1 流量估计预测

无线传感器网络节点在传输数据包时, 实际上

项目来源: 国家自然科学基金项目(11261002); 云南省教育厅科学研究基金项目(2012C065)

收稿日期: 2013-07-16 **修改日期**: 2013-10-09

是节点与节点之间进行流量的无线传输,入侵者可以根据对流量的控制达到攻击网络的目的。目前已有的流量估计算法有 Markov 线性流量预测模型、MAC 流量自适应算法、利用流量特征的 GIDS 保温分类优化算法等,这些算法都是根据流量的特征、性质进行计算[9-10]。但是这些算法计算出的值并不是很稳定,精确度也不高,而且在统计数值时误差较大,不容易检测出来入侵情况[11]。

粒子滤波技术是一种用于非线性、非高斯系统的滤波方法[12]。粒子滤波算法在无线传感器网络中有较广泛的应用,例如对节点进行跟踪,定位求精等方面,研究效果比较稳定[13]。本文将粒子滤波技术用在对目标进行跟踪,从而估算出流量,对节点是否受到攻击进行判断。利用该算法估算出的结果数值比较稳定,精确度较高。

1.2 基本原理

粒子滤波算法的核心是对重要密度函数的采样,通过概率分布计算加重权值,最终估算出流量的一种稳定且简单的算法。利用粒子滤波进行流量估计的算法过程如下:

(1)建立状态方程与观测方程

$$\boldsymbol{X}_k=\varphi_k(\boldsymbol{X}_{k-1},\boldsymbol{v}_k) \tag{1}$$

$$\boldsymbol{L}_k=f_k(\boldsymbol{X}_k,\boldsymbol{w}_k) \tag{2}$$

其中,$\boldsymbol{X}_k$ 是 k 时刻的状态向量;$\boldsymbol{L}_k$ 是 k 时刻的观测向量;$\boldsymbol{\omega}_k$ 和 $\Delta\boldsymbol{k}$ 分别为状态转移函数和观测函数;$\boldsymbol{\omega}_k$ 和 $\Delta\boldsymbol{k}$ 是状态噪声向量和观测噪声向量。

(2)初始化节点

当簇内中心节点检测到有目标进入时,为簇内第 j 个普通节点分配 nj 个粒子,并且这些粒子服从高斯分布。

(3)簇内普通节点粒子权值估计(重要性权值计算)

假设采样时刻为 k,且 $k-1$ 时刻节点的状态 $\boldsymbol{X}_k-1=$观测值 $\boldsymbol{L}_k$,条件概率 $p(\boldsymbol{X}_k\mid\boldsymbol{X}_{k-1})$ 为已知,通过式 3 预测 k 时刻的节点状态,当观测值可用时,计算粒子的权值:

$$\omega_k^{i,j}=\omega_{k-1}^{i,j}\frac{p(X_k\mid X_k^{i,j})p(X_k^{i,j}\mid X_{k-1}^{i,j})}{q(X_k^{i,j}\mid X_{k-1}^{i,j},X_k)}=\omega_{k-1}^{i,j}p(X_k\mid X_k^{i,j}) \tag{3}$$

其中,$\omega_k^{i,j}$ 表示簇内第 j 个普通节点的第 i 个粒子在 k 时刻的权值,第二个等号成立的条件是将 $p(X_k^{i,j}\mid X_{k-1}^{i,j})$ 作为重要密度函数。

(4)估计簇内普通节点的状态

第 j 个节点 nj 个粒子聚合状态(期望)估计:

$$X_k^j=\sum_{i=1}^{n_j}X_k^{i,j}\omega_k^{i,j} \tag{4}$$

第 j 个节点 nj 个粒子聚合权值估计:

$$\omega_k^j=\sum_{i=1}^{n_j}\omega_k^{i,j} \tag{5}$$

(5)簇内普通节点粒子更新(重采样)

通过估计的各粒子权值,判断此时的粒子是否已经偏离了状态转移轨道,即是否有效,若$\frac{\omega_k^{i,j}}{\omega_k^{1,j}}\leqslant\frac{3}{4}$,则表示该粒子测量结果无效,应重新为节点分配粒子,再进行重采样,估算权值及状态。

(6)用重采样的各估计值计算节点新的状态,直到估计值趋于稳定。

(7)估算流量

假设 B_0 是一个节点从状态 $k-1$ 到状态 k 单位长度内传输的数据量,而传输的总长度可以通过估计的节点权值得到:

$$S_{k-1,k}^j=\omega_k^j=\sum_{i=1}^{n_j}\omega_k^{i,j} \tag{6}$$

则节点从状态 $k-1$ 到状态 k 传输的总数据量为:

$$B_j=B_0\cdot S_{k-1,k}^j \tag{7}$$

式中:X_k:是 k 时刻的状态向量;L_k:是 k 时刻的观测向量;$p(X_k\mid X_{k-1})$:表示 k 时刻的条件概率;$\omega_k^{i,j}$:表示簇内第 j 个普通节点的第 i 个粒子在 k 时刻的权值;$S_{k-1,k}^j$:表示 $k-1$ 状态到 k 状态数据传输的总长度;B_0:表示一个节点从状态 $k-1$ 到状态 k 单位长度内传输的数据量,为已知;B_j:表示从状态 $k-1$ 到状态 k 传输的总流量。

粒子滤波流量估计算法的流程图如图 1 所示。

2 应用粒子滤波的入侵检测方法

2.1 检测方法原理

利用 LEACH 算法进行分簇,只是为了算法更好的性能和延长无线传感器网络的生命周期,本文中检测方法同样适合在其他分簇的网络拓扑结构中使用。

在用 LEACH 算法对节点进行分簇的前提下,将粒子滤波跟踪算法应用到簇内节点对目标物体进行跟踪时节点状态的变化上,通过对节点状态的跟踪估算出变化过程中传输的流量值。通过估算出的流量值与预定义的流量阀值相比较从而计算节点的检测率,由检测率反应出节点受到攻击的情况以及当前网络的安全状态。

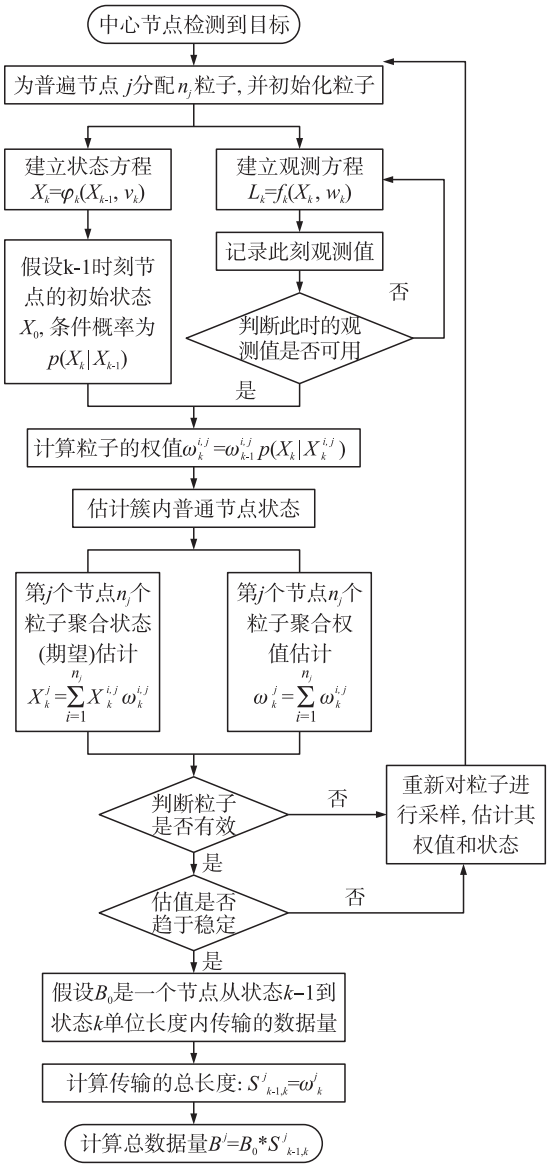

图 1　粒子滤波流量估计算法流程图

2.2　具体过程

将粒子滤波算法用在对 WSN 中节点流量的估计中,对数据包传输过程中节点状态变化中所产生的流量值,并通过估算出的流量值判断节点是否受到攻击。下面对整个检测过程作具体的描述。

算法的具体实现步骤如下:①首先确定待检测的区域 A;②假设节点个数为 n 个,对这些节点用 LEACH 分簇算法进行分簇;③待分簇结束后,簇头节点检测是否有目标物体进入检测区域,如果没有,则所有节点处于空闲状态,如果有目标进入,则执行第 4 步;④分配节点对目标进行检测,同时,粒子器分配一定量的粒子对该节点进行跟踪,并观测节点的状态变化;⑤根据粒子跟踪得来的数据判断当前节点是否有流量变化,若没有则返回第 4 步继续跟踪,如有则执行第 6 步;⑥记录当前估算出的流量值,并且输入预定义的阀值的最大值与最小值,将估算的流量值与阀值进行比较;⑦判断估算的流量值与阀值的比较结果,若估值大于最大值或小于最小值则判断该节点为异常节点,若估值在阀值范围内则将该节点标记为正常节点。

基于粒子滤波流量估计算法的入侵检测流程图如图 2 所示。

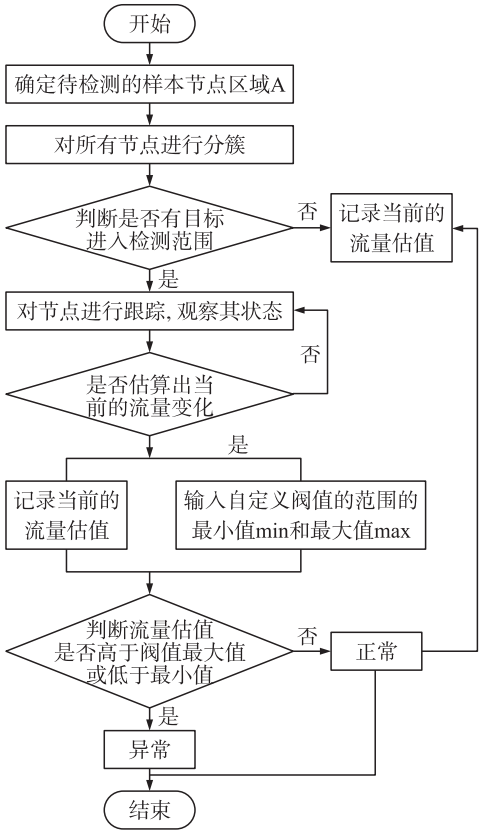

图 2　粒子滤波流量估计算法的入侵检测流程图

3　算法性能分析与仿真

通过数据包的检测率这一特征参数来预测无线传感器网络是否受到攻击。检测率指的是检测出来正确的攻击样本数量与总的攻击样本数量之比。使用粒子滤波算法时,输入的过程噪声和观测噪声方差值不同时,会影响检测效果。在本文提出的粒子滤波算法中,根据输入过程噪声和观察噪声可以得到不同的结果,并对结果进行分析。

3.1　仿真环境

假设粒子个数以及粒子的质量都处于比较好的状态。在仿真中假设有目标进入传感器网络节点检测范围,且目标在二维平面上做匀速运动,所有的节点在初始化时都能得到自己的真实位置,同时节点与节点之间都能直接通信,以及能够产生足够的粒子,每个节点都能够监视自己区域的目标物体。对仿真中要用到的参数作设置,每个节点运动的状态

方程和观测方程如下：

$$\boldsymbol{X}_k = \boldsymbol{A}\boldsymbol{X}k-1+\boldsymbol{B}v_k \tag{8}$$

$$\boldsymbol{L}_k = \sqrt{\boldsymbol{Y}_K^2+\boldsymbol{X}_K^2}+w_k \tag{9}$$

其中，$\boldsymbol{X}_k=(x,\dot{x},y\cdot\dot{y})_k^{\mathrm{T}}$；$\boldsymbol{v}_k=(w_x,w_y)_k^{\mathrm{T}}$；

$$\boldsymbol{A}=\begin{bmatrix}1&1&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{bmatrix};$$

$$\boldsymbol{B}=\begin{bmatrix}0.5&0\\1&0\\0&0.5\\0&1\end{bmatrix}$$

式中 x 和 y 为节点的平面直角坐标，v_k 和 w_k 为高斯白噪声，均值都为零；

在仿真过程中，过程噪声方差和观测噪声方差值都是随机输入值。并假设在整个仿真过程中，对每个节点分配的粒子数目能够满足要求。

表 1 粒子滤波流量预测仿真参数表

名称	设定值
样本区域范围	100 m×100 m
样本节点个数	100
粒子滤波器中的粒子个数	100
离子跟踪模拟长度	100
一个节点单位长度内传输的数据量	0.5
定义判断流量的阀值最大取值	20

3.2 可靠性分析

可靠性指的是传感器节点能够及时检测出节点异常并能够维持在稳定的水平。

粒子在对目标物体进行跟踪时所测量出来的数据比较稳定和精确。算法对估计值计算方差和均值，同时计算其收敛值。由统计理论知道，最优估计是可以由条件均值计算出来的，其均值的估值表示为：

$$E(\boldsymbol{X}_k|\boldsymbol{X}_{k-1})=\int \boldsymbol{X}_K p(\boldsymbol{X}_K|\boldsymbol{X}_{K-1})\mathrm{d}\boldsymbol{X}_K \tag{10}$$

式中 $\boldsymbol{X}_{k-1}$ 表示 $k-1$ 时刻的状态，$p(\boldsymbol{X}_k|\boldsymbol{X}_{k-1})$ 表示在已知 $k-1$ 时刻的状态求 k 时刻的状态的条件概率。

粒子滤波的核心思想是对粒子的重采样，在重采样过程中其均值可用式(11)计算：

$$E(\boldsymbol{X}_k|\boldsymbol{X}_{k-1})=\bar{\omega}_k(X_k^{(i)})X_k^{(i)} \tag{11}$$

式中，$\bar{\omega}_k$ 表示 k 时刻的加重权值，$X_k^{(i)}$ 表示第 i 个粒子在 k 时刻的状态。

算法由重要密度函数获得采样样本点，并随着测量值的依次到来，迭代求得相应的重点权值，最终以样本加权和表征后验概率密度得到状态的估计值[5]。重要密度函数的选择是粒子滤波实现的关键，通常将 $p(Xk|Xk-1)$ 作为重要密度函数。密度函数的选择也就确定了粒子滤波的可靠性程度，如果密度函数选择比较合理，则可靠性相对比较高，否则可靠性就会降低。本文中选择的密度函数是依据状态条件概率分布得出，所以可靠性相对比较稳定。

3.3 仿真结果

检测率反应的是在整个仿真过程中算法的精确度。由于无线传感器网络数据传输的随机性及不稳定性，仿真所采用的数据由随机函数产生并输出。下面就仿真过程中产生的过程噪声和观测噪声产生的结果进行比对分析。

图 3 是当输入不同的过程噪声方差值时检测率的比较图。

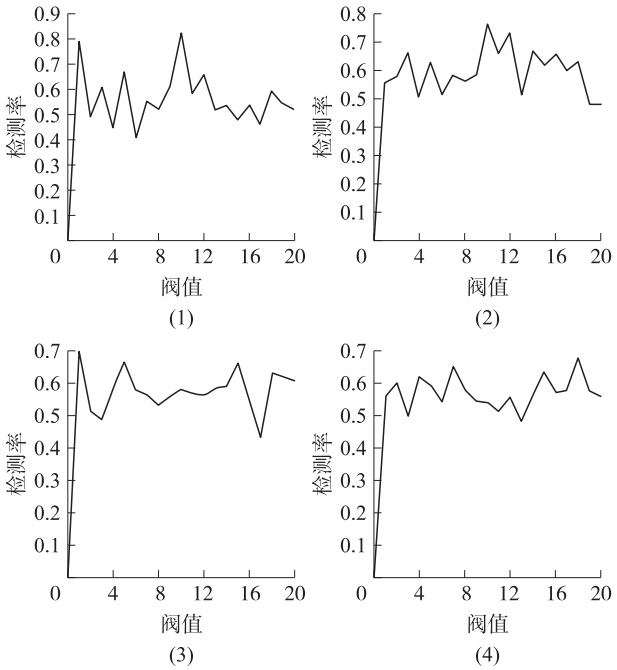

图 3 不同过程噪声方差值的检测率随阀值变化情况比较图

图 3 中子图(1)反应的是输入过程噪声方差值为 0.1 的检测率，阀值在 0 到 1 时节点的检测率波动比较大，当阀值从 1 到 20 时，节点检测率一直在 0.4 到 0.7 之间波动，平均检测率为 0.6153；子图(2)反应的是输入过程噪声方差值为 0.5 的检测率，阀值在 0 到 1 时节点的检测率波动比较大，从 0 一直呈直线到 0.58 左右，当阀值从 1 到 20 时，节点检测率一直在 0.5 到 0.72 之间波动，平均检测率为 0.6423；子图(3)反应的是输入过程噪声方差值为 100 的检测率，阀值在 0 到 1 时节点的检测率波动

比较大,从 0 一直呈直线到 0.5 左右,当阀值从 1 到 20 时,节点检测率一直在 0.5 到 0.7 之间波动,平均检测率为 0.6208;子图(4)反应的是输入过程噪声方差值为 1000 的检测率,阀值在 0 到 1 时节点的检测率波动比较大,从 0 一直呈直线到 0.58 左右,当阀值从 1 到 20 时,节点检测率一直在 0.48 到 0.7 之间波动,平均检测率为 0.6038。

由图 3 可知,不管过程噪声输入的值相差多少,节点的检测率都在 0.48 到 0.7 之间波动。由此可以得出结论:通过粒子滤波算法可以成功的检测出节点受到攻击的情况,而且估算出的值是比较稳定。在仿真过程中,输入的参数不同,存在一定的误差,这些问题在本文中没有得到解决,但是在以后的研究中,这将会作为重点问题研究。

图 4 是当输入不同的观测噪声方差值时检测率的比较图。子图(1)反应的是输入观测噪声方差值为 0.1 的检测率,由图可知,阀值在 0 到 1 时节点的检测率波动比较大,从 0 一直呈直线到 0.24 左右,当阀值从 1 到 20 时,节点检测率一直在 0.2 到 0.3 之间波动,当输入的观测方差值小于 0.1 时,检测率就在逐渐下降;子图(2)反应的是输入观测噪声方差值为 0.5 的检测率,阀值在 0 到 1 时节点的检测率波动比较大,从 0 一直呈直线到 0.58 左右,当阀值从 1 到 20 时,节点检测率一直在 0.47 到 0.65 之间波动;子图(3)和子图(4)分别反应的是输入观测噪声方差值为 100 和 1 000 的检测率,节点检测率超过了 1,即出现了异常现象。

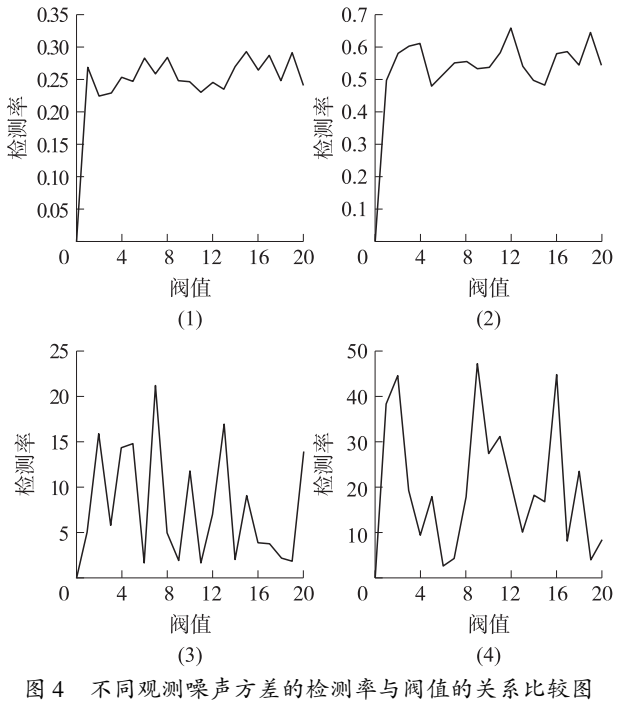

图 4　不同观测噪声方差的检测率与阀值的关系比较图

在过程噪声方差值固定,观测噪声方差值变化时,节点的检测率比较稳定,但是相对于在观测噪声方差值固定、过程噪声方差值变化的情况下检测率比较低。由此可见,在粒子滤波算法的仿真中,所输入的过程噪声方差值和观测噪声方差值对仿真结果的影响是不同的。由图 3 可知,过程噪声方差值输入任何数值时的检测率基本上不会有太大的波动,估算出的数值也比较稳定;从图 4 可知,输入的观测噪声方差值对仿真结果的影响就比较大,当输入的值太大或太小时检测率都可能出现异常现象。因此,在使用粒子滤波对无线传感器网络节点进行跟踪估算流量值时,必须考虑观测噪声方差值的输入,要选取合适的值进行仿真。

4　结论

在对无线传感器网络进行分簇的基础上,利用粒子滤波算法对节点的流量进行估算,并利用 MATLAB 仿真工具进行仿真,通过节点的检测率来反应无线传感器网络是否被攻击以及攻击的状况,并使得网络能够及时处理异常。通过粒子滤波算法估算出的结果比较稳定,适合应用在无线传感器网络中。

参考文献:

[1] 王颖,李国瑞. 基于分组的无线传感器网络入侵检测方案[J]. 传感技术学报,2009,22(6):878-882.

[2] 张永俊,牟琦毕,孝儒. 基于云模型的增 SVM 入侵检测方法[J]. 计算机应用与软件,2013,30(3):311-314.

[3] Doumit S, Agrawal D. Self-Organized Criticality and Stochastic Learning Based Intrusion Detection System for Wireless Sensor Network [C]//IEEE Military Communications Conference, Monterey, CA, USA, 2003:609-614.

[4] 夏克寒,许化龙,张朴睿. 粒子滤波的关键技术及应用[J]. 电光与控制,2005,12(6):1-4.

[5] 刘洋,李玉山,张大朴,等. 基于动态目标建模的粒子滤波视觉跟踪算法[J]. 光子学报,2008,37(2):375-379.

[6] 李红春,赵晓光,谭民. 无线传感器网络中基于粒子滤波的人员跟踪方法[J]. 传感技术学报,2012,25(6):807-813.

[7] 李芳芳,王靖. 一种基于 LEACH 协议的无线传感器网络路由算法[J]. 传感技术学报,2012,25(10):1445-1451.

[8] 林元乖. 能量高效的无线传感器网络分簇路由算法研究[J]. 计算机应用研究,2012,29(4):1529-1532.

[9] 彭青艳,赵勋杰,陈家波. 跟踪窗口尺寸自适应调整的粒子滤波跟踪算法[J]. 红外技术,2012,34(10):568-571.

[10] 方正,佟国峰,徐心和. 粒子群优化粒子滤波方法[J]. 控制与决策,2007,22(3):273-276.

[11] Zhang Miaohui. Adaptive Multi-Feature Tracking in Particle Swarm Optimization Based Particle Filter Framework [J]. Journal of Systems Engineering and Electronics, 2012, 23(5):775-783.

[12] 韩志杰,张玮玮,陈志国. 基于 Markov 的无线传感器网络入侵检测机制[J]. 计算机工程与科学,2010,32(9):27-30.

[13] 乔相伟,周卫东,吉宇人. 基于四元数粒子滤波的飞行器姿态估计算法研究[J]. 兵工学报,2012,33(9):1070-1074.

冯立波(1980-),男,河北邢台人,2008年毕业于北京邮电大学,获得硕士学位,现为大理学院数学与计算机学院讲师,主要研究方向为物联网,无线传感器网络,fengyibupt@126. com;

罗桂兰(1977-),女,四川绵阳人,2009年毕业于东北大学,获得博士学位,现为大理学院数学与计算机学院副教授,主要研究方向为物联网,无线传感器网络。