

基于聚类特征自适应机制的无线传感网 异常节点检测算法

戴春妮^{1, 2}

(1 华东师范大学 计算机科学与软件工程学院, 上海 200241; 2 上海建桥学院 信息技术学院, 上海 201306)

摘 要: 提出了一种基于聚类特征自适应机制的无线传感网节点检测算法. 首先, 基于节点聚类特征自适应机制, 通过特征采样, 不断获取异常节点的路由信息、链路抖动率以及数据分组传输率等关键参数信息, 从而计算节点特征值, 并联合矢量内积对异常节点进行识别, 提高对异常节点的感知能力; 随后, 采用分区聚类, 对可能的疑似异常节点进行聚合提纯, 降低网络对正常节点的误判, 提高了异常节点的检出效率; 最后, 定义异常节点检举规则, 通过对分区进行筛选, 有效降低了正常节点出现在异常节点集合中的概率, 从而提高了算法对异常节点的搜寻效率. 与当前 PSO 算法、SDR 算法相比, 此算法具有更高的异常节点检出率与更低的数据传输时延, 能够有效避免异常节点对传输数据的篡改.

关键词: 无线传感网络; 关键特征参数; 节点聚类; 聚类特征自适应机制; 异常节点检举规则

中图分类号: TP393.04

文献标识码: A

文章编号: 1000-7180(2017)04-0076-07

Anomaly Node Searching Algorithm of Wireless Sensor Networks Based on Adaptive Mechanism of Clustering Feature

DAI Chun-ni^{1, 2}

(1 College of Computer Science and Software Engineering, East China Normal University, Shanghai 200241, China;
2 Department of Information Technology, Shanghai Jianqiao University, Shanghai 201306, China)

Abstract: This paper presents a method based on the clustering of the abnormal nodes report mechanism of networking malicious behavior selection algorithm. On the basis of node clustering analysis, through the feature sampling construction characteristics of the node values, and according to the actual situation taken to increase the key characteristic parameters of malicious node behavior to carry on the accurate localization; then constructs the cluster mechanism, take the clustering partition continue to suspected nodes aggregate, to further reduce the misjudgment; rules for the prosecution of the definition of malicious nodes, the partition selection further reduces the normal nodes appear in the malicious node in the collection probability and improve the algorithm's perception of malicious nodes. Simulation results show that compared with the commonly used PSO algorithm and the SDR algorithm, the algorithm of the malicious node detection rate, and can effectively avoid tampering of malicious nodes to transmit data, has a strong practical value.

Key words: wireless sensor networks; key characteristic parameters; node clustering; clustering aggregation mechanism; abnormal node reporting rules

1 引言

为减少传感网异常行为对网络正常运行造成的

严重影响, 学者们提出了许多具有相应的算法, 如 Rodrigo. R^[1]等提出了一种基于区域交互特征刷新机制的传感网异常行为搜寻算法, 通过周期性特征采样

方式刷新区域特征,从而迅速提取到异常节点的攻击行为。然而,该搜寻算法仅仅能够对过往异常攻击方式进行递归,当节点更新频繁时易造成严重的误判现象,降低了该算法的适应性。Li. H. T^[2]等提出了一种基于异常行为隔离检测机制的传感网节点搜寻算法,该算法采取分区方式,一旦某区域内发生异常行为将迅速启动隔离机制,从而将异常行为造成的危害尽量控制在最小的范围内。但是该算法对节点密度分布情况考虑不足,当节点分布密集时极易造成大量正常节点被分割在隔离区域内部,导致网络出现大面积节点瘫痪现象。Ning. H. S^[3]等提出了一种基于数据水印辨析机制的传感网异常行为辨析算法,该算法通过向数据报文添加不可篡改的临时性水印的方式,降低了异常节点在中途窜入的可能性。但是,该算法需要对全部节点发送的数据报文进行水印添加,当网络数据流量较大时会提高算法复杂程度,并导致网络数据传输时延呈现增加的态势。

对此,本文提出了一种基于节点异常聚类特征自适应机制的传感网异常行为搜寻算法。

2 传感网络组网模型及节点聚类行为分析

2.1 传感网组网模型

考虑到当前最新的传感网在部署过程中往往采用基于无线数据交换方式的传感器作为网络节点,这些网络节点均采用布撒方式进行组网^[4],一旦中间发生异常情况,则可以通过自身携带的收发天线并采用无线感知方式实现对异常信息的感知。为简便起见,设整个传感网节点均分布在 $N \times N$ 的矩形区域内^[5],对任意传感网节点 i 而言,假设其在上述矩形区域内的感知位置为 (x_i, y_i) ,如图1所示,当该节点有异常行为时,不妨设中央节点 j 为检测节点(检测节点的坐标为 (x, y)),则异常节点 i 在满足式(1)时,即可被检测出来:

$$P(i, j) = 1, |i, j| < R \quad (1)$$

式中, $P(i, j)$ 为检测概率, $|i, j|$ 表示节点 i 和 j 之间的物理距离, R 表示中央节点 j 最佳感知半径:

$$|i, j| = \sqrt{|x_i - x|^2 + |y_i - y|^2} \quad (2)$$

结合模型(1)、(2)可以判断某节点 i 一旦发生异常行为时是否能够被探测到,若网络全部节点通过模型(1)处理之后,发现其相应的检测概率为1,则说明传感网处于整体可感知的状态。否则,需要通过分区的方式,通过在不同的分区中设置相应的检测节点,以便确保整体网络处于可感知的状态。

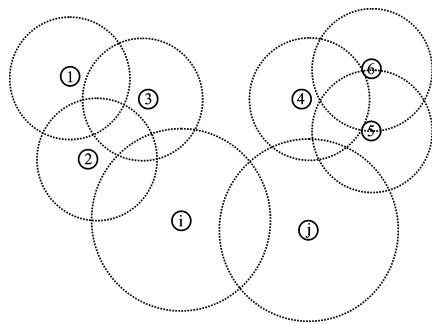


图1 传感网节点覆盖示意图

2.2 节点聚类行为分析

由于传感网节点在部署过程中,一般采用一次性部署成型的方式^[6],即组网节点均需要经过逐步检测并测试之后,方可进行组网。然而由于传感网在进行正常的数据传输过程中,一些伪装节点可能混入到正常节点中,且可能通过主动注入或被动监听的方式对网络的正常运行造成严重的破坏,因此,需要在行为上对整个网络节点进行聚类特征自适应,以便能够对不同的威胁行为作出相应的解决。

(1)以节点行为进行聚类,可以简单地将传感网中的全部节点划分为普通节点与外来节点两类,普通节点即能够进行正常的传感数据采集的节点,外来节点可分为两类:一类属于更新节点,即新更换的节点;或因需要新增加的传感节点;第二类属于异常节点,即通过混入方式进入传感网内部的节点,这些节点伺机进行数据窃听或进行其他破坏活动,往往会带来严重的安全隐患。

(2)潜伏节点,如图2所示,该种类型的节点与异常节点相比,往往具有更强的迷惑性,需要在具备一定的外界条件下方得以触发异常行为,触发过程可以采用时间触发、事件触发、单纯窃听三种方式进行。随着当前传感网技术的迅速发展,潜伏节点可以通过组网阶段、网络维护、主动侵入等多种形式注入到正常运行的网络中,在触发之前很难通过传统的检测方式进行检测,只能通过早触发-早发现的方式,将安全隐患控制在可控范围之内。

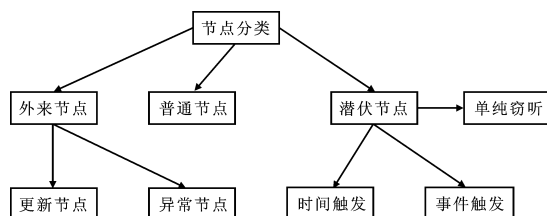


图2 节点聚类归类

(3) 节点数据特征值, 该特征值主要通过采样序列构成, 本文采取周期采样机制抽取得到: 不妨设节点 i 为网络中的任意节点, 采样周期为 T , 则节点 i 的节点数据特征值 i_t 将满足如下的序列:

$$i_t = \{i_1, i_2, \dots, i_n\} \quad (3)$$

式中, $\{i_1, i_2, \dots, i_n\}$ 分别为节点当前的数据路由信息、链路抖动率、数据分组传输率、数据报文解析率等关键特征参数构成, 通过增加关键特征参数, 能够有效增加采样的有效性。

考虑到传感网部署中, 全部网络信息均保存在中央节点上, 且中央节点上保存有全部节点信息的副本, 如图 3 所示, 本文采用匹配方式, 即一旦某节点的节点数据特征值与中央节点上参数保持一致, 则将判断该节点为异常节点。

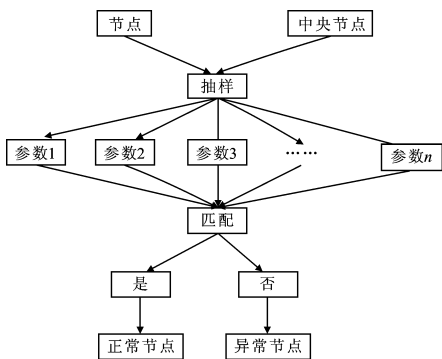


图3 节点数据特征匹配

考虑到实际过程中参数数量越多, 则准确程度越高, 然而由于实际部署中传感网节点密度往往极高, 且在一定的检测周期内即需要能够准确的检测出来, 因此, 本文采取矢量内积构造式对节点数据特征值进行处理,

设节点 i 的节点数据特征值 i_t 满足 $i_t = \{i_1, i_2, \dots, i_n\}$, 中央节点上对应的采样序列 $\tilde{i}_t$ 满足:

$$\tilde{i}_t = \{\tilde{i}_1, \tilde{i}_2, \dots, \tilde{i}_n\} \quad (4)$$

则两者的矢量内积 $R(i_t, \tilde{i}_t)$ 可构造如下:

$$R(i_t, \tilde{i}_t) = \sum (\|i_t\| - \|\tilde{i}_t\|) \quad (5)$$

式中, $\| \cdot \|$ 表示取对应的序列分量的运算, 当仅当 i_t 和 $\tilde{i}_t$ 对应的序列分量在允许的偏差之内时, $\|i_t\| - \|\tilde{i}_t\|$ 的结果取 1, 反之取 0. 结合模型(3)~(5)可得知, 矢量内积 $R(i_t, \tilde{i}_t)$ 累计总值越大, 则说明被抽样的节点 i 为异常节点的可能性也就越大。

此外, 由于模型(3)中的节点数据特征值均通过采样序列构成, 且该序列均通过周期采样机制获取, 若某个异常节点除了正常节点的全部特征参数, 然而由于本文采取的抽样方式获取特征参数, 随着采样序

列的不断增加, 异常节点与正常节点之间的特征值也会存在较大的差异, 因而通过模型(3)~(5)的过程即能将异常节点搜寻出来。

3 本文无线传感网异常节点搜寻算法

本文算法首先通过采样方式获取节点数据特征值, 并结合中央节点的数据副本构造矢量内积, 提高网络对异常节点的感知能力. 随后将不同的节点进行聚类处理, 形成完整的分类集合后, 通过搜寻规则进行异常节点搜寻. 整个算法由如下部分组成: 基于聚类特征自适应机制的节点特征值初始化、基于分区聚类机制的异常节点更新、异常节点检举。

3.1 基于聚类特征自适应机制的节点特征值初始化

由模型(3)可知, 对于任意节点 i 而言, 其节点特征值均可以通过抽样方式得到. 该特征值为一抽样序列, 序列分量由当前节点的各种关键特征参数所构成, 且选取的关键特征参数(数据路由信息、链路抖动率、数据分组传输率、数据报文解析率等)越多, 则抽样精度也就越高. 则节点 i 在进行节点特征值初始化过程中, 如图 4 所示, 首先需要将自身路由信息、数据传输信息等关键参数进行解析, 获取独立的关键参数, 然后将这些关键参数以 Hello 数据分组的方式发送到中心节点中. 当中心节点收取到节点 i 发送的 Hello 数据分组之后, 一方面从该数据分组中解析出节点 i 对应的关键参数, 另一方面也按照模型(3)的方式进行节点特征值抽样, 得到节点 i 的特征值副本, 此外, 中央节点也对自身进行抽样, 得到中央特征值序列。

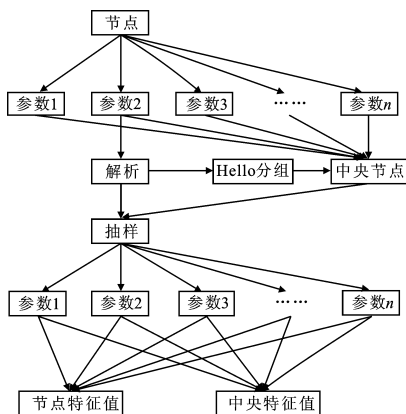


图4 节点特征聚类初始化

不妨设节点 i 的节点特征值为 i_t , 中心节点中获取的相应特征值副本为 $\tilde{s}_t(i)$, 中央特征值序列为 $\tilde{s}_t$, 按模型(5) 所示构造相应的矢量内积如下:

$$R(i_t, s_t(i)) = \sum (\|i_t\| - \|s_t(i)\|) \quad (6)$$

$$R(i_t, s_t) = \sum (\|i_t\| - \|s_t\|) \quad (7)$$

若节点 i 属于正常节点,则根据模型(5)分析,且满足如下条件:

$$\|i_t\| - \|s_t(i)\| = 0 \quad (8)$$

$$\|i_t\| - \|s_t\| = 0 \quad (9)$$

若节点 i 属于异常节点,则根据模型(5)分析,则满足如下条件:

$$\|i_t\| - \|s_t(i)\| = 1 \quad (10)$$

$$\|i_t\| - \|s_t\| = 1 \quad (11)$$

因此,若节点 i 经过矢量内积构造之后,若按模型(6)~(7)构造得到的数值越大,则说明该节点处于异常状态的可能性也就越高。构造节点 i 的联合矢量内积 R_i 如下:

$$R_i = \mu_1 R(i_t, s_t(i))^{1-\mu_2} + \mu_2 R(i_t, s_t)^{1-\mu_1} \quad (12)$$

式中, μ_1 和 μ_2 满足:

$$\mu_1 + \mu_2 = 1 \quad (13)$$

不妨设网络中处于活动状态的传感网节点的个数为 m ,则整个网络的联合矢量内积 R_{all} 满足:

$$R_{all} = \{R_1, R_2, R_3, \dots, R_m\} \quad (14)$$

由于模型(12)也可以提现为异常节点 i 的矢量内积,因此对于整个网络而言,异常节点修改网络参数的概率 P 满足:

$$P = \frac{\sum \mu_1 R_i(i_t, s_t(i))^{1-\mu_2} + \mu_2 R_i(i_t, s_t)^{1-\mu_1}}{\sum \mu_1 R(i_t, s_t(i))^{1-\mu_2} + \mu_2 R(i_t, s_t)^{1-\mu_1}} \quad (15)$$

相关参数同模型(12)~(14),该概率也是对于任意一个网络节点而言,被异常节点修改数据的概率。

模型(14)中对应的 R_i 构造方法同模型(12),且对于不同的节点而言, μ_1 和 μ_2 可根据实际情况不同的数值。由模型(8)~(11)可知,一旦某个节点处于异常状态,则其矢量内积构造过程中得到的“1”的数量将不断增多,该节点属于异常节点的可能性也将提高,需要重点进行监测;对于整体网络而言,按模型(14)即可判断网络中异常节点的存在性:若其对应分量 R_i 中,某个分量对应的矢量内积数值远远高于其他节点,则可初步将该节点搜寻为异常节点,若发现当前时刻该节点无明显异常行为时,则将重点监控该节点,并实时监控。

3.2 基于分区聚类机制的异常节点更新

通过模型(12)可以对某个节点是否处于异常状态进行初步判断,然而当网络中节点密度较大时将难以迅速的对节点同时进行构造及判断,特别是对于传

感网而言,一旦某个节点处于失效状态时,极易导致严重传染效应^[7],从而出现大面积数据瘫痪现象。因此,本文构建了聚类特征自适应机制,完成异常节点信息的更新。

考虑到传感网在实际部署中往往采取分区的方式^[8],不同分区内部的节点特征参数(数据路由信息、链路抖动率、数据分组传输率、数据报文解析率等)区别很大,如图5所示,本文算法以分区为单位,按如下步骤对全部节点进行聚类特征自适应。

Step 1:根据模型(12)构造得到全部可能的疑似节点,并设疑似节点组成的序列集合为 o ;

Step 2:按分区为单位,逐区构造节点特征值密度 $T(\alpha)$;

$$T(\alpha) = \{T(\alpha, H) \leq R \mid \mu \in o\} \quad (16)$$

式中, T 为节点 α 与相应的区头节点 H 之间的物理距离, R 为区域覆盖半径,

Step 3:再构造序列集合 o 的平均密度 p ;

$$p = \frac{\sum T(\alpha)}{n} \quad (17)$$

Step 4:根据模型(16),逐点对序列集合 o 中元素按模型(17)构造平均密度,并再次与模型(15)逐点进行比对,当仅当满足模型(18)的条件时,疑似节点才保留在序列集合 o 中,否则将该节点清除出集合。

$$p > T(\alpha) \quad (18)$$

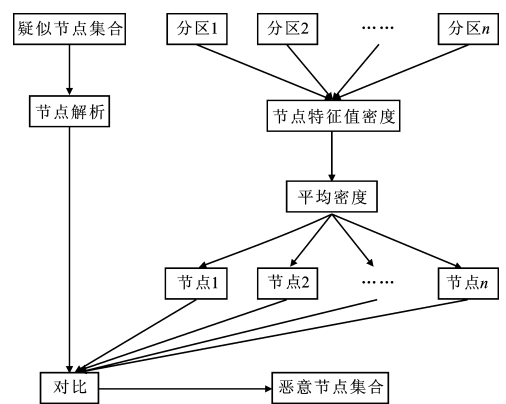


图5 分区聚类机制

3.3 异常节点检举

完成聚类特征自适应过程之后,显然序列集合 o 中节点均与其他传感网节点的关键特征参数有一定的不同,然而由于不同分区内节点的关键特征参数均有一定的差异性,单纯将序列集合 o 中节点判定为异常节点的话,将有不少正常节点会被误判。为降低误判可能,本文定义异常节点搜寻规则如下,其过程见图6,具体描述如下:

(1)首先获取聚类特征自适应流程中节点的全部信息,重新按照模型(12)构造联合矢量内积,并按模型(12)进行异常节点判断后,将不满足模型(8)成立条件的节点从序列集合 o 中删除;

(2)连续进行采样过程,直到序列集合 o 中的节点个数不再减少为止.

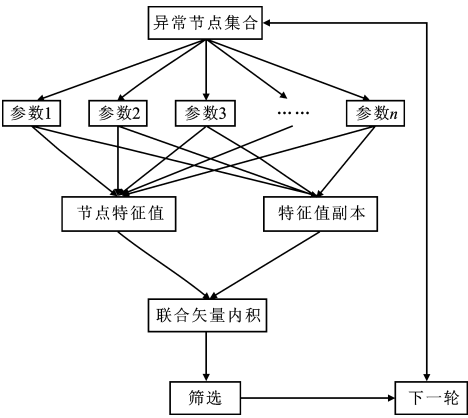


图 6 异常节点检举流程

4 仿真实验

为验证本文算法的优异性,本文将传感网领域常用的 PSO 算法^[9]、SDR 算法^[10] 视为对照组,采用 NS2 环境进行仿真实验,实验过程中基本仿真参数表如表 1 所示.

表 1 基本仿真参数表

参数	数值
网络部署区域面积	1 200 m×9 000 m
节点布置方式	平均分布
节点是否游走	是
节点密度/(个/m)	<12
节点最大初始能量/J	无定值,随用随补
数据传输率/(bit/s)	128
网络最大分区数量	128

实验过程中,采用分区方式部署无线传感节点,正文网络部署面积如表 1 所示;节点数据均采用无线方式进行采样及传输,信号调制方式为 8PSK;考虑到实际情况中异常节点往往从网络层与数据链路层两方面对网络进行入侵,因此特征参数分网络层与数据链路层两方面提取:网络层方面,取数据路由链路、链路抖动率、数据分组传输率、数据报文解析率 5 个特征参数;数据链路层方面,取信号频率波动、频率偏移量、信道抖动率 3 个特征参数;在 NS2 仿真环境中,上述 8 个特征参数均通过 NS2 相关函数进行周期性的

提取,采样周期为信号的发射周期. 由于信号调制方式为 8PSK,因此信号发射周期为 1 800 ms. 一旦检测发现区域内无线传感节点存在异常,则区域中的簇头节点将迅速把节点信息传输到 sink 节点中,以便进行进一步对比分析.

(1)异常节点检出率

图 7 显示了随着数据传输率的不断变动,本文算法的异常节点检出率变动情况. 由图 7 可知,当数据传输率不断增加时,本文算法的异常节点检出率在不断提高之后,逐步趋向稳定,这是由于随着数据传输率的不断增加,异常节点对应关键参数的强度也随之增加,因而检出率也随之提高;随着数据传输率的进一步提高,获取的异常节点序列集合将趋向稳定,因而异常节点检出率也呈现稳定状态. 此外,从图 7 中还可以看到,随着数据采样频率提高,本文算法的搜寻速度越快,单位时间能够匹配的关键参数也越多,使其收敛到最大检出率的速率提高,因而能够更快地检测出异常节点.

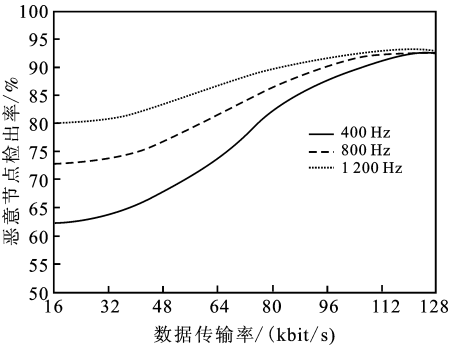


图 7 本文算法的异常节点检出率测试结果

图 8 显示了随着网络最大分区数量的不断变动,本文算法、PSO 算法及 SDR 算法的异常节点检出率测试结果,由图可知,随着网络最大分区数量的不断增加,本文算法的异常节点检出率最大,始终高于 PSO 算法及 SDR 算法. 这是由于 PSO 算法采用简单应答机制,当仅当异常节点对当前分区的数据传输产生影响之后,才能检测出异常节点,而 SDR 算法虽然能够通过分析网络数据报文对异常节点行为进行判定,然而由于 SDR 算法仅能够对节点路由信息进行解析,若异常节点的行为并不影响路由信息时,则 SDR 算法将处于失效状态,导致难以探测到异常节点. 而本文算法通过计算节点矢量内积,使其能够同时对多种节点特征参数(数据路由信息、链路抖动率、数据分组传输率、数据报文解析率等)进行解析,且可以根据需要追加更多的特征参数,并联合聚类特征自适应,进一步提高了对异常节点的感知能力,因而本

文算法的异常节点检出率要高于对照组算法。

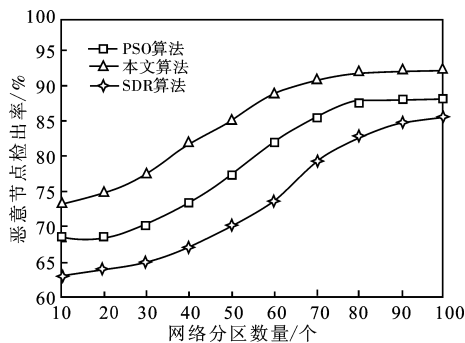


图8 三种算法的异常节点检出率测试结果

图9显示了随着网络工作时间的不断增加,本文算法与PSO算法及SDR算法的异常节点检出数量对比,由图可知随着网络工作时间的不断增加,三种算法的节点检出率均呈现不断上升的态势,然而本文算法检出率始终高于SO算法、SDR算法,且其检出率稳步提升。这是由于本文算法采取了聚类特征自适应机制,能够将疑似节点通过聚类机制进行集中,并利用异常节点检举机制不断对异常节点的信息进行探测优化,因而出现检出率稳步上升的态势。而PSO算法虽然能够对异常节点的反馈做出应答,然而单纯采取简单应答机制,当异常节点没有进行异常行为时,将难以探测到此类型的异常节点。SDR算法单纯从路由指标对异常节点进行探测,一旦异常节点并非在路由层面进行异常攻击时,该算法对异常节点的检测失败。

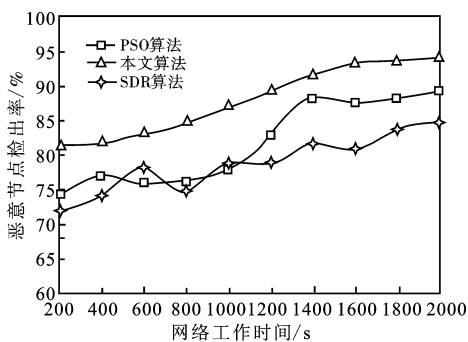


图9 不同网络工作时间下的三种算法的异常节点检出率测试

(2) 网络数据传输时延

由于在实际检测过程中,异常节点均是通过簇头节点进行数据监测,且检测过程中均与sink节点进行数据比对,因此数据网络传输时延与簇头节点的硬件质量密切相关;若无线传感节点的节点缓存越大、内部电路处理能力越强、收发天线的信号调制质量越高,则因检测而导致的数据网络传输时延也

将越低。图10显示了随着网络分区的不断增加,本文算法、PSO算法与SDR算法的数据传输时延测试结果。由图10可知,随着网络分区数量的不断增加,本文算法的数据传输时延始终处于较低的水平,且远远低于对照组算法。这是由于对任何异常节点检测算法而言,由于需要针对节点的行为进行实时监测,因此会导致出现一定的时延,然而本文算法能够通过多种参数,如数据路由信息、链路抖动率、数据分组传输率、数据报文解析率等同时进行并发检测,而PSO算法、SDR算法单纯采用一种检测机制,其中,PSO算法负责实时监听异常数据报文,SDR算法负责检测路由信息,因此,本文算法能够在较短的时间内完成检测过程,降低了检测过程中对正常数据发送过程的影响,因而本文算法的数据传输时延较低。

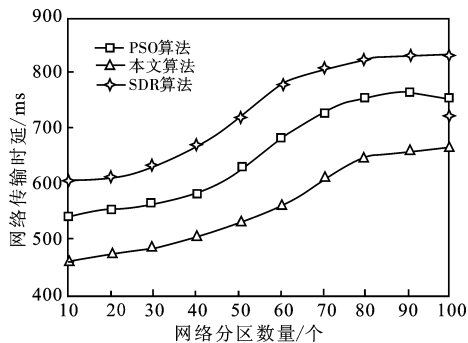


图10 三种算法的网络数据传输时延测试结果

(3) 数据传输质量

为直观显示异常节点对无线传感网数据的影响,在表1基础上,向网络中随机添加100个异常节点,并将灰度图像作为测试传输数据,其中,异常节点以一定的几率(本次实验设定为每个节点在同一传输周期内均以0.5%概率启动篡改行为)对传输数据进行攻击篡改。图11(a)为初始图像,图11(b)~(d)分别为本文算法、PSO算法、SDR算法经传感网传输后的数据质量。从仿真结果看,本文算法传输前后的图像质量失真较小,模糊程度较低,且无扭曲,见图11(b)。而PSO算法、SDR算法均出现了一定程度的模糊现象,且PSO算法甚至出现了一定程度的扭曲,见图11(d)。这是由于本文基于节点异常聚类特征自适应机制,能够通过节点特征值初始化、聚类特征自适应、异常节点检举三个过程,在进行异常行为发生前即可将绝大部分异常节点搜寻出来。PSO算法采用简单应答机制,仅当异常节点产生异常行为之后才能检测出来,导致传输数据出现严重的篡改现象,因而出现传输后的图像的失真度较大;

SDR 算法虽然能够对异常节点进行一定的解析,在一定程度上降低了传输数据被篡改的现象,然而由于该算法难以对不影响路由行为的异常节点进行搜寻,因而传输质量仍然要低于本文算法。



(a) 初始图像

(b) 本文算法



(c) SDR 算法

(d) SPO 算法(扭曲变形)

图 11 三种算法的在异常节点攻击下的传输输出图像质量

5 结束语

为解决当前传感网节点感知技术难以准确定位节点异常行为,且难以实现对实时异常行为的有效评估,导致出现严重的数据篡改现象等不足,本文提出了一种基于聚类特征自适应机制的无线传感网节点异常行为搜寻算法。通过构建节点特征值,联合矢量内积的方式提高对异常节点的感知能力,采取构建聚类特征自适应的方式降低误判情况的发生,最后定义异常节点搜寻规则,进一步提高了本文算法对异常节点的精确定位。仿真结果表明:与当前常用的 PSO 算法及 SDR 算法相比,此算法具有更高的异常节点检出率与更低的数据传输时延。

参考文献:

- [1] Wang H, Jin S. An energy-efficient framework for clustering based data collection in wsn [J]. Parallel and Distributed Systems, IEEE Transactions, 2011, 22(6): 1064-1071.
- [2] Li Z, Xi L, Hong J. Cross-layer adaptive resource allocation algorithm with diverse QoS requirements for single-cell OFDMA systems [J]. Journal of Harbin institute of Technology, 2015, 1(1): 15-22.
- [3] Ahme A, Abu B K, Cha N M. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks [J]. Frontiers of Computer Science, 2015, 12(7): 280-296.
- [4] 王翥, 王祁. 多约束容错性 WSN 中继节点搜寻算法的研究[J]. 电子学报, 2013, 1(2): 115-120.
- [5] 杨国宁, 冯秀芳, 樊刘娟. 一种基于最优融合集的多传感器数据搜寻算法 [J]. 软件学报, 2012, 23(11): 134-140.
- [6] Sichitiu. Cross-layer scheduling for power efficiency in WSN [J]. Proceedings of the IEEE INFOCOM, 2015, 6(9): 105-115.
- [7] Lin G M. Novel congestion control approach in wireless multimedia sensor networks [J]. The Journal of China Universities of Posts and Telecommunications, 2011, 18(2): 1-8.
- [8] Yang S, Qin B D. End-to-end rate-based congestion control with random loss: convergence and stability [J]. Journal of Systems Engineering and Electronics, 2008, 6(17): 1208-1214.
- [9] Zhen X L. A survey on data dissemination in wireless sensor networks [J]. Journal of Computer Science & Technology, 2013, 3(11): 470-486.
- [10] Cai Z X. Dynamic cluster member selection method for multi-target tracking in wireless sensor network [J]. Journal of Central South University, 2014, 2(11): 636-645.

作者简介:

戴春妮 女, (1977-), 博士, 副教授. 研究方向为网路通信、信号检测、模式识别. E-mail: shdaichuni1977jq@sina. com.