基于云模型的无线传感器网络恶意节点识别技术的研究

蔡绍滨[1,3],韩启龙[1],高振国[2],杨德森[3],赵 靖[1]
(1.哈尔滨工程大学计算机科学与技术学院,黑龙江哈尔滨 150001;2.哈尔滨工程大学自动化学院,黑龙江哈尔滨 150001;
3.哈尔滨工程大学水声工程学院,黑龙江哈尔滨 150001)

摘 要: 无线传感器网络(Wireless Sensor Network,简称 WSN)是一种没有基础设施的自组织无线网络.和其它网络一样,WSN 需要安全措施来保证网络通信的安全.但是,在无线传感器网络中,基于密码的安全体系不能有效处理来自网络内部的攻击,识别出恶意节点.因此,信任模型被用于无线传感器网络恶意节点识别.在信任模型和云理论的研究基础上,本文构建了一个基于云理论的无线传感器网络信任模型——云信任模型(CTM,Cloud-based Trust Model).实验结果表明,云信任模型能够有效识别恶意节点.

关键词: 无线传感器网络; 安全; 恶意节点; 信任模型; 云理论
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2012)11-2232-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.11.015

Research on Cloud Trust Model for Malicious Node Detection in Wireless Sensor Network

CAI Shao-bin[1,3], HAN Qi-long, GAO Zhen-guo[2], YANG De-sen[3], ZHAO Jing[1]
(1. *Department of Computer Science and Technology, Harbin Engineering University, Harbin, Heilongjiang* 150001, *China*;
2. *Department of automation, Harbin Engineering University, Harbin, Heilongjiang* 150001, *China*;
3. *Department of Underwater Acoustic Engineering, Harbin Engineering University, Harbin, Heilongjiang* 150001, *China*)

Abstract: WSN(Wireless Sensor Network)is formed by a large number of cheap sensors, and is used to collect information of sensed objects in assigned area. In most applications of WSN, security schemes are needed to guarantee the communication security. However, the security schemes based on key can not efficiently deal with the attacks from the inside of the network, and distinguish the malicious nodes. Therefore, trust models are applied to distinguish malicious nodes. Based on trust model and cloud theory, CTM (Cloud-based Trust Model) is proposed in this paper. The analysis and simulation results show that, CTM can distinguish malicious nodes efficiently.

Key words: wireless sensor network; security; malicious node; trust model; cloud theory

1 引言

无线传感器网络(Wireless Sensor Network,简称 WSN)是一种没有基础设施的自组织无线网络.它在军事、环境检测和预报、智能家居等诸多领域具有广泛的应用,已经引起了世界许多国家军界、学术界和工业界的高度重视.和其它网络一样,WSN 需要安全措施来保证网络通信的安全.尤其是,当 WSN 被部署到敌对的环境中时,它的安全是决定 WSN 是否能够正常工作的重要因素.

和有线网络相比,WSN 具有如下特点:(1)有限的存储空间和计算能力;(2)缺乏后期节点布置的先验知识;(3)布置区域的物理安全无法保证;(4)有限的带宽和通信能量;(5)不仅是点到点的安全,更是整个网络的安全;(6)应用相关性.因此,在无线传感器网络中,基于密码的安全体系不能有效处理来自网络内部的攻击[1].信任模型在解决无线传感器网络中内部攻击,识别恶意节点,提高系统安全性和可靠性有着显著优势.因此,信任模型[2]被用于无线传感器网络恶意节点识别.信任关系是一个很难度量的、抽象的心理认知,是不稳定的.在

收稿日期:2011-06-30;修回日期:2012-03-12
基金项目:国家自然科学基金(No.41176082,No.61073182,No.61073183);中央高校基本科研业务费专项资金(No.HEUCF1007,No.HEUCF100607)

信任模型和云理论的研究基础上,本文构建了一个基于云理论的无线传感器网络信任模型——云信任模型(Cloud-based Trust Model,CTM).

2　无线传感器网络信任模型

2.1　基于声誉的信任模型

2004 年,Ganeriwal Srivastava 提出了一个分布式对称模型 RFSN(Reputation-based Framework for Sensor Network)模型[3].RFSN 模型利用直接信誉和间接信誉来表示节点的信誉.其中,直接信誉是指节点自身保存的相邻节点信誉;间接信誉指节点通过相邻节点所获得的其他节点的信誉信息.

针对移动自组织网络的特点,文献[4]建立一个无核心节点的声誉评价机制.在该机制中,节点设定主动观测值(SR,Subjective Rating)来表示其监控的邻居节点是否正常处理其接到的包.在单位监控时间内,如果被监测节点错误行为较少,则 SR 值线性增加;如果被监测节点行为错误大于预定错误门限,则 SR 值指数减少.

在文献[5]提出的基于信誉的认证模型的基础上,文献[6]提出了基于声誉和信任组的实体认证模型(如图 1 所示).在该模型中,通过引入信任组来简化节点对信任度的计算,减少资源的消耗,提高网络的生命周期.但是,该方案是基于密钥的可信认证,若恶意节点获取了网络的密钥,则该模型的抵御能力将大大降低.

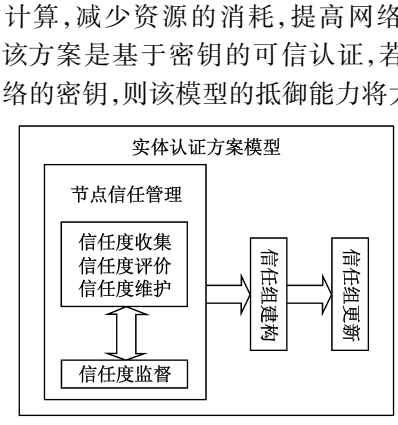

图1　实体认证方案模型

2.2　基于概率的信任模型

基于概率的信任模型[7,8]主要通过概率论和数理统计的方法建立传感器网络的信誉系统.目前,最多的是利用 Beta 概率分布建立 Beta 信誉系统,利用高斯概率分布建立高斯信誉系统,还有利用贝叶斯定理建立贝叶斯网络,或者将多种方法结合在一起.在基于概率分布的信任模型中,首先根据传感器节点的行为得到节点的信誉值,再通过信任值算法计算得到节点的信任值.信誉值对应概率分布的参数,信任值算法对应概率分布的数学期望.计算出节点的可信度后,节点只和信任值大于预设阈值的节点合作.

2.3　基于熵理论的信任模型

文献[9]提出了一种基于熵理论的信任模型,$T\{subject:agent,action\}$($T\in[-1,1]$)表示节点间的信任关系,$P\{subject:agent,action\}$ 表示节点 *agent* 从节点 *subject* 的观点来看可能对 *subject* 采取某一行为(*action*)的概率.因此,基于熵的信任值定义如下:

$$T\{subject:agent,actions\}=\begin{cases}1-H(p),0.5\leqslant p\leqslant 1\\ H(p)-1,0\leqslant p\leqslant 0.5\end{cases}$$

其中,$H(p)=-p\log_2(p)-(1-p)\log_2(1-p)$是熵函数,信任度 $p=P\{subject:agent,action\}$随着时间和行为上下文而变化.使用如下评估模型可计算 $subject:A$ 观察到 $agent:X$ 执行 *action* 的概率:

$$P\{A:X,action\}=\frac{1+\sum\beta^{t_c-t_j}k_j}{2+\sum\beta^{t_c-t_j}N_j}$$

其中 t_j 为统计时间,在时刻 t_j,A 统计到 X 执行 k_j 次 *action*,N_j 为要求执行 *action* 的次数,t_c 是当前时间,$0\leqslant\beta\leqslant 1$ 是遗忘因子.但是,基于熵理论的信任模型的实质还是基于概率的.

以上各个信任模型主要由节点对邻居节点的行为进行评估,并根据不同的方式建立节点的可信度.尽管他们建立的模型在一定程度反映了无线传感器网络节点的信任度的动态特性.但是,这些模型的信任描述的都是一个定性的概念,不能够很好地反映复杂环境中无线传感器网络的节点信任是一个根据环境变化的模糊问题.因此,在云理论的基础上,本文提出了云信任模型.

3　云理论

隶属云[10]是 20 世纪 90 年代李德毅院士在传统模糊数学和概率统计的基础上提出的定性定量互换模型,主要反映事物概念的两种不确定性:模糊性(边界的亦此亦彼性)和随机性.将二者结合起来,可以从语言值描述的定性问题中获得定量数据的范围和分布规律,或者将精确数值转换为适当的定性语言值.

设 Ω 是一个用精确数值表示的论域,T 是与 Ω 相联系的定性语言值.Ω 中的元素 x 对于 T 所表达的定性概念的隶属度 $C_T(x)$是一个在[0,1]上取值的,具有稳定倾向的随机数,隶属度在论域上的分布称为隶属云,简称云.云是从论域 Ω 到区间[0,1]的映射,即 $x\in\Omega$,$x\to C_T(x)$,$(x,C_T(x))$称为云滴[11].

云由云滴组成,一个云滴是定性概念在数量上的一次实现,单个云滴无足轻重,不同时刻产生的云的细节可能不尽相同.云用期望 *Ex*,熵 *En* 和超熵 *He* 三个数值来表示它的数字特征,来反映了定性概念上的定量特征[12].期望 *Ex* 是数域中最能体现这个定性概念的点,是将定性概念数值化的最佳样本点.在云图中体现

为云的峰值所处的位置.熵 En 是期望不确定性的度量,表示数域中可以被定性概念接受的取值范围,即模糊度,是定性概念亦此亦彼性的度量,通常熵越大概念越宏观.在云图中体现为云的宽度.超熵 He 是熵的不确定性的度量,反映云滴的离散程度,代表云滴出现的随机性,揭示了模糊性和随机性的关联.超熵越大,云滴离散程度越大,云图中云的厚度也就越大.

4 基于云理论的信任模型

隶属云模型把定性概念的模糊性、随机性和不确定性有机综合在一起,实现概念的定性和定量之间的转换.本文用云来描述一个时间段内传感器网络节点间通信态势以及节点收集数据的状态.因此,本文首先根据网络中绝大多数节点的通信态势和数据范围构建全局基准云.在此基础上,一个节点结合的自身局部环境特点来构建它自己的基准云,再通过邻居节点信任云和基准云的比较来判定邻居节点的行为是否和绝大多数节点行为相似.如果相似,则节点是一个正常节点;否则,节点是一个恶意节点.

但是,已有的云比较算法计算复杂度较高,不适合无线传感器网络.因此,我们提出了一个云相似度比较算法来降低计算复杂度[13],并在此基础上将云理论引入到无线传感器网络安全领域中,提出基于云理论的信任模型.

4.1 可信度的计算

网络中节点部署完毕后,各个节点开始进行数据的传输,节点同时在每个时间段 Δt 内对邻居节点的某些行为属性进行监听,将监听到的信息保存在一个矩阵中.在 n 个时间段后,节点 i 对节点 j 的行为属性监听矩阵为:

$$\boldsymbol{X}_{ij}=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \ddots & \cdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix}$$

其中,行数 m 为属性的个数,列数 n 为经历的时间段个数.

根据简化的逆向云生成器算法[14]计算出云的三个数字特征,对于某个属性上的信息集合 $\boldsymbol{X}_{ij}=\{x_1,x_2,\cdots x_n\}$,可以构造在这个属性上的信任云 $C(Ex,En,He)$,其过程如下:

(1)根据 $\boldsymbol{X}$ 求出样本均值 $\bar{X}=\frac{1}{n}\sum_{i=1}^{n}x_i$,一阶样本中心矩 $d=\frac{1}{n}\sum_{i=1}^{n}|x_i-\bar{X}|$,样本方差 $s^2=\frac{1}{n}\sum_{i=1}^{n}(x-\bar{X})^2$;

(2) $Ex=\bar{X}$;

(3) $En=\sqrt{\frac{\pi}{2}}\times d$;

(4) $He=\sqrt{s^2-En^2}$

在计算节点的直接信任度时,我们将相似云引入到信任领域中.首先根据经验构造信任基准云 $C_t(Ex_t,En_t,He_t)$,然后按照基于区间的云相似度比较算法,计算信任云与基准云的相似度,这个相似度就定义为该信任云的可信度,即节点 i 对节点 j 的直接可信度为:

$$t_{i,j}^{direct}=similar_{ij}$$

节点 i 对 j 进行可信度评估时,还需要从其他邻居节点处获得该节点对 j 的可信度,这样获得的可信度为间接可信度[15].在图 2 中,假设节点 k 和 m 为与节点 i 有交互行为的邻居节点,i 请求二者传递他们对节点 j 的可信度,其中 k 与 j 有直接交互行为,而 m 与 j 无交互历史,m 的邻居节点 n 和 j 有交互历史,故 m 先从 n 处获得 j 的可信度,然后在将这一可信度交给节点 i.在本例中,节点 i 获得的间接可信度如下式:

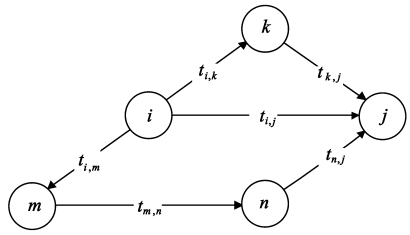

图2 间接可信度示意图

$$t_{i,j}^{indirect}=t_{i,k}^{direct}\times t_{k,j}^{direct}+t_{i,m}^{direct}\times(t_{m,n}^{direct}\times t_{n,j}^{direct})$$

将直接信任与间接信任加权相加即可得到总体可信度:

$$t_{i,j}=\omega_1\times t_{i,j}^{direct}+\omega_2\times t_{i,j}^{indirect}$$
$$(0<\omega_1,\omega_2<1,\omega_1+\omega_2=1)$$

4.2 可信度的更新

在一次可信度计算之后,节点 i 保留节点 j 的可信度.经过一段时间的交互,节点 i 从新计算和更新 j 的可信度.文献[16]定义的可信度更新函数为 $t_{new}=\omega t_1+(1-\omega)t_2,0<\omega<1$,其中,$t_1$ 为之前的可信度,t_2 为新计算得到可信度,ω 为时间衰减因子.所得到的 t_{new} 介于二者之间.当 ω 小于 0.5 时,历史记录的可信度所占权重较小,便形成了随时间衰减的可信度更新过程,符合日常人们对信任的理解.

当 $t_1\leqslant t_2$ 时,$t_1<t_{new}<t_2$,则可信度增值 $\Delta t=t_{new}-t_1=\omega t_1+(1-\omega)t_2-t_1=(1-\omega)(t_2-t_1)$;

当 $t_1>t_2$ 时,$t_2<t_{new}<t_1$,则可信度增值 $\Delta t'=t_1-t_{new}=t_1-\omega t_1-(1-\omega)t_2=(1-\omega)(t_1-t_2)$

因此,t_1、t_2 无论大小关系如何,只要增减幅度相同,即 $|t_1-t_2|=|t_2-t_1|$,则更新后得到的可信度的增减幅度也相同,这与日常生活中信任具有的“日久见人

心”的特征不符.通常,可信度应该在 $t_2 < t_1$ 情况下进行更新后降低幅度大,而在 $t_1 < t_2$ 情况下进行更新后的增长幅度小,即慢升快降机制.

现在我们将上升幅度变成原来的 $1/n$,下降幅度变成原来的 m 倍.

在 $t_1 \leqslant t_2$ 时,

$$t'_{new} = t_1 + \Delta t/n = t_1 + (\omega t_1 + (1-\omega)t_2 - t_1)/n$$
$$= [(n+\omega-1)t_1 + (1-\omega)t_2]/n$$

在 $t_1 > t_2$ 时,

$$t'_{new} = t_1 - m\Delta t = t_1 - m(t_1 - \omega t_1 - (1-\omega)t_2)$$
$$= (1-m+m\omega)t_1 + m(1-\omega)t_2$$

整理后得到新的更新函数:

$$t_{new} = \begin{cases} [(n+\omega-1)t_1 + (1-\omega)t_2]/n, & t_1 \leqslant t_2 \\ (1-m+m\omega)t_1 + m(1-\omega)t_2, & t_1 > t_2 \end{cases}$$

其中,n 和 m 的取值可按具体需要进行设定.

5　性能分析

在进行仿真实验检测信任模型的鲁棒性前,首先分析云模型可以探测到的异常行为,并以此行为属性作为信任模型评判的依据.云模型可以监测的行为规则主要有:

(1)消息冲突规则:节点传输一条消息而引发的冲突次数应保持在一个合理范围内.冲突过多,可能为恶意节点进行碰撞攻击,扰乱信道.若长期无消息冲突,则有可能为黑洞攻击,吸引正常节点向其发送数据.

(2)重传规则:节点让正常节点重发上一数据包的次数应在合理范围内,否则可能为恶意节点耗尽正常节点的能量,或恶意节点发动的黑洞攻击,吸引正常节点.

(3)数据信息规则:在位置相邻的节点之间,其通信的数据内容应该具有相似性,数值偏差会在一个合理的范围内.数值偏差较大很可能为恶意节点采用选择转发攻击,篡改数据信息.

(4)路由跳数规则:在虫洞攻击中,两个恶意节点相互合作,掩盖其实际距离远的事实,使得在正常节点看来,通过虫洞传输相比正常多跳路由具有更少跳数,更低时延.因此,在节点间路由跳数应该在一个合理范围内.

以上四条属性规则均需要一个合理范围作为限定条件,形成在峰值处最为合理,而距离峰值较远处,可能为恶意攻击.这样的特征符合云图表征的属性,因此可以将上述属性规则作为信任云判断节点可信度的依据.

5.1　实验环境及实验参数设置

本论文采用 MATLAB 仿真平台,用 M 语言进行编程实现.在实验中的网络模型为:

(1)在 100 × 100 的正方形区域内随机部署 200 个传感器节点,汇聚节点位于区域的左上角.传感器节点和汇聚节点都是静态的,即部署后不再发生位置的移动.

(2)所有节点都是同构的,具有相同的物理结构单元和能量,且具备数据融合功能.

实验采用 Intel Berkeley 实验室的 54 个 Mica2Dot 传感器节点在 2004 年 2 月 28 日至 4 月 5 日所采集到的真实数据.这些数据每 30 秒采集一次,其中包括湿度、温度、光照和电压值[16],我们将这些数据中的温度值单独筛选出来.

实验数据是每 30 秒采集一次,则在本文的实验中,每 10 分钟进行一次可信度的计算,即每次计算包含 20 个数据作为云模型的研究论域.在对全局数据进行统计分析后,首先得到全局温度的信任基准云.在此基础上,节点再根据自身收集的数据构建自身的信任基准云.在正常情况下,20 个温度数据构成的信任云与信任基准云的相似度均大于 0.6.因此,本文将可信度的阈值设定为 0.6.此外,模型中直接信任与间接信任的权值 ω_1, ω_2 分别为定义为 0.8 和 0.2,更新函数的时间衰减因子 ω 为 0.3.

5.2　On-off 攻击抵御

最典型的针对信誉系统的攻击是 On-off 攻击[17],恶意节点首先表现出很好的通信行为赚取一定的信任值,然后再表现出不好的行为,发送错误数据,随意丢弃其它节点的包.其中,错误数据为正常数据加减随机产生的、满足正态分布的、不小于正常数据 10% 的误差值.但当恶意节点的信任值下降到一定数值的时候,又表现出很好的通信行为为下一次的攻击累积信任.在整个期间,恶意节点都会使其信任值保持在一个足够的水平.因此,在建立云模型的基础上,我们进一步利用慢升快降机制来抵御 On-off 攻击.

在慢升快降机制中,n 和 m 分别为可信度上升与下降的幅度.由于慢升快降是一个相对的过程,所以,在保持下降幅度不变的情况下,只通过降低上升的幅度,也可实现慢升快降的过程.因此,在此处将 m 设定为 1,研究 n 的取值.我们选择数据中波动较大的一段数据作为研究的论域,观察 n 的不同取值对可信度更新的影响(如图 3 所示).当 $n = 4$ 时,原本正常的一组数据由于上升幅度过慢,导致可信度值变得不可信,出现了错误的判断,因此 n 值在大于等于 4 的情况下对可信度失真的影响较大,易导致误判.当 $n = 3$ 时,在时间段 3 至 5,即使连续上升 3 个时间段,所计算出的可信度值仅上升了 0.05 左右,上升的幅度过小不利于提高节点的“积极性”.因此,在本次实验环境下,取 n 值

为 2,即上升幅度变为原来的 1/2.

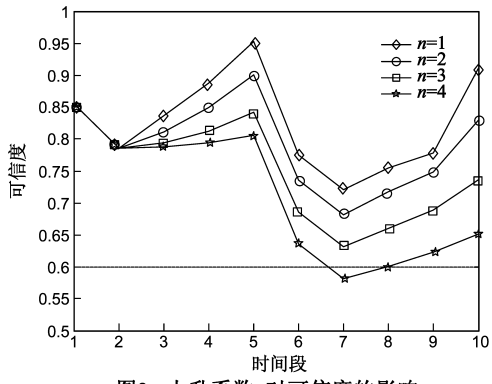

图3 上升系数n对可信度的影响

图 4 描述了 CTM 模型对于正常数据和 on-off 攻击数据的可信度.正常数据通过 CTM 计算到的可信度虽有一定的波动,但波动范围不大,比较稳定,且大于阈值.恶意节点发送的数据波动较大,存在破坏行为,在第六次可信度的计算中被 CTM 判断出为恶意节点,此后恶意节点试图掩饰其行为,通过提高可信度重新被网络接纳,但达到阈值时,节点早已被网络隔离.因此本文设计的信任模型是有效的、合理的,并且算法是稳定的.

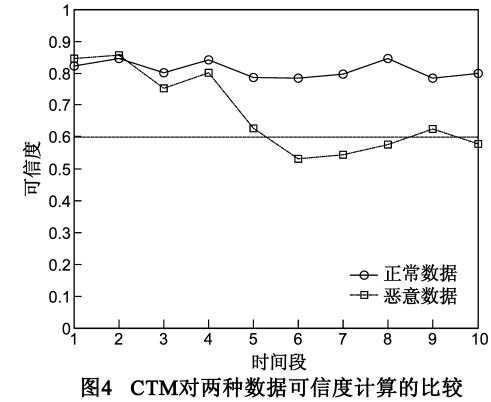

图4 CTM对两种数据可信度计算的比较

5.3 恶嘴攻击抵御

信任模型中一类常见的攻击为恶嘴攻击[18].即,在获取间接可信度的过程中,其邻居节点为恶意节点,该节点恶意诋毁其他节点,传递的可信度很低,意图让节点相信所要计算可信度的正常节点为恶意节点.

图 5 描述了恶嘴攻击时 CTM 计算所的可信度.由于在可信度整合过程中,节点计算的直接可信度占据较大比重,故面对恶嘴攻击时,可信度虽有降低,但降低幅度很小,对正常节点的诋毁效果不大.因此恶嘴攻击被抑制,显示出 CTM 的健壮性.

图 6 描述了在节点受到恶嘴攻击时慢升快降机制对可信度的影响.当 $n=1$ 时,没有采用慢升快降机制,在第九次更新之后,节点的可信度低于阈值,被判断出为恶意节点;在第十次更新后,恶意节点通过掩饰行为,成功的将可信度值超过阈值,恶意节点重新被网络接纳.当 $n=2$ 时,CTM 模型采用了慢升快降机制,节点的恶意行为对节点的信誉的影响更大.因此,在第六次更新后,可信度的值就已经接近阈值;在第八次更新之后,节点已经被识别为恶意节点;即使,恶意节点当试图通过正常行为来掩饰,也不能够在第十次更新后将可信度增加到阈值标准.因此,具有慢升快降机制的 CTM 模型能快速、有效地识别并且遏制恶意节点,尽早将其隔离出网络,降低对网络的破坏.

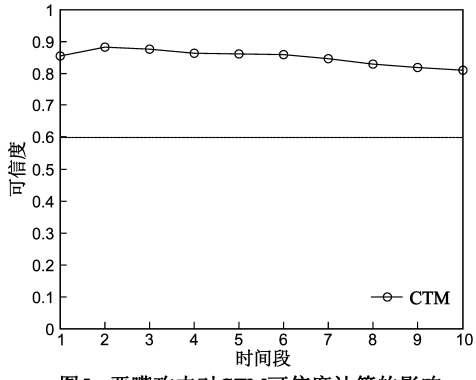

图5 恶嘴攻击对CTM可信度计算的影响

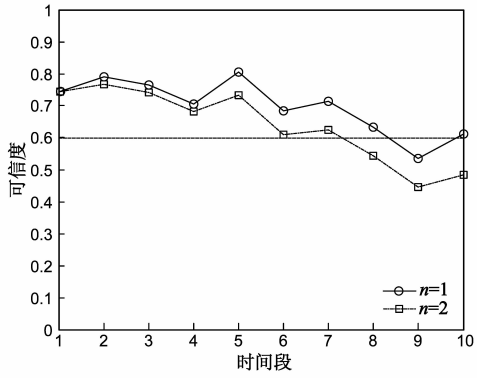

图6 更新函数对可信度计算的影响

5.4 噪音抵御

传感器网络应用环境复杂,尤其是在高噪音的环境中,节点的错误行为会明显高于正常环境.因此,一个良好的信任模型应该具有一定的容错性,能够将环境导致的错误和恶意行为区分开,使得可信度的计算更加准确.在基于云的信任模型中,sink 节点根据收集的统计数据构建全局基准云,节点在全局基准云的基础上结合自身的环境构建自身的基准云.因此,基准云模型具有一定的动态性,能够反映环境的高噪音特性.

图 7 描述了高噪音环境下 CTM 对正常数据和恶意行为的判定.尽管,高噪音导致节点经常出错,节点的可信度的计算虽然存在一定波动,但仍然和构建的基准云具有很好的相似性,可信度整体变化幅度不大.相对而言,恶意节点的可信度存在一个向下的总体趋势.尽管恶意节点在进行恶意行为后试图通过少量正常行

为掩饰身份,但是它和基准云的相似度相差较大,尤其是在慢升快降的更新机制下,最终可信度达到阈值以下,恶意节点的身份被较快地识别并隔离出网络.

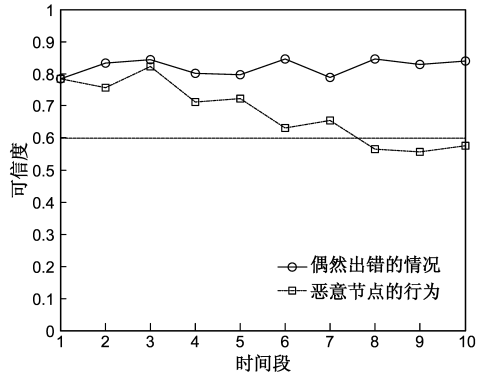

图7　两种情况下可信度比较

5.5　算法计算复杂性

由于加减法的计算复杂度远低于乘除法运算和三角函数运算的计算复杂度,所以,在这里,我们不考虑加减法的计算费用.在信誉系统中,每一次交互后,节点都要对信誉系统的信任值进行更新,并判断节点是否是恶意节点.当一个节点平均具有 5 个邻居节点,GTMS 簇的平均大小为 20 时,我们统计了各种算法一次更新平均所需的乘法次数(如表 1 所示).

表 1　算法计算复杂度比较

信誉模型	乘除法次数
RFSN	11
基于概率的信任模型	48
基于熵的模型	$8+2\times\log$
CTM	$12+\sqrt{s^2-E_n^2}$

在表 1 中,CTM 算法中,$s^2=\frac{1}{n}\sum_{i=1}^{n}(x-\bar{X})^2$ 表示样本方差,$En=\sqrt{\frac{\pi}{2}}\times d$ 表示的是信任云的熵.如果假设开发利用移位寄存器实现,则 CTM 的计算法费用 $12+\sqrt{s^2-E_n^2}=12+n=32$.在基于熵的模型中,计算费用为 $8+2\times\log$.在采用展开式的方式来计算 log 值的假设下,可以认为 log 运算的计算费用不少于 10 次乘法运算.虽然,CTM 的计算费用高于 RFSN 的计算费用,但是,它的计算费用近似于基于熵的模型的计算费用,低于基于概率的模型的计算费用.因此,CTS 具有较为合理的计算费用.

6　结论

本文在基于区间的云相似度比较算法的基础上,将云理论思想引入到无线传感器网络中,建立基于云理论的信任模型——CTM.并在可信度的更新过程中设计具有慢升快降性质的更新函数.实验和分析结果表明 CTM 不但较好地识别恶意节点,而且具有较低的计算费用.

参考文献

[1] Naif Alsharabi, Li Ren Fa, Fan Zing. Wireless sensor networks of battlefields hotspot challenges and solutions [J]. IEEE Transaction on Mobile Computering, 2007, 6(1): 554 – 562.

[2] Blaze M, Feigenbaum J. Decentralized trust management[A]. Dale J. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy[C]. IEEE, NJ, United States, 1996. 164 – 173.

[3] Saurabh Ganeriwal, Mani B. Srivastava. Reputation-based framework for high integrity sensor network [A]. Sanjeev Setia. Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Network[C]. NY: ACM, 2004. 66 – 77.

[4] 王建新,张亚男,王伟平,卢锡城.移动自组网中基于声誉机制的安全路由协议设计与分析[J].电子学报,2005,33(4):596 – 601.
Wang Jianxin, Zhang Yanan, Wang Weipin, Lu Xicheng. A security routing protocol based on reputation systems in MANET [J]. Acta Electronica Sinica, 2005, 33(4): 596 – 601. (in Chinese)

[5] Sapon T, Pinalkumar D, Rohan B. Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks [A]. Mohamed Eltoweissy. Proceedings of the IEEE Workshop on Energy-Efficient Wireless Communications and Networks [C]. Arizona: IEEE, 2004. 463 – 469.

[6] Rebahi Y, Mujica-V V E, Sisalem D A. Republican-based trust mechanism for Ad hoc network[A]. R Ammar Reda Ammar Proceedings of the 10th IEEE Symposium on Computers and Communications [C]. San Francisco: IEEE, 2005. 37 – 42.

[7] 冯健昭,肖德琴,杨波.基于β分布的无线传感器网络信誉系统[J].计算机应用,2007,27(1):111 – 113.
Feng Jianzhao, Xiao Deqin, Yang Bo. Reputation system for wireless sensor networks based on β distribution [J]. Journal of Computer Applications. 2007, 27(1): 111 – 113. (in Chinese)

[8] 肖德琴,冯健昭,周权等.基于高斯分布的传感器网络信誉模型[J].通信学报,2008,29(3):47 – 53.
Xiao Deqin, Feng Jianzhao, Zhou Quan. Gauss reputation framework for sensor networks [J]. Journal on Communications, 2008, 29(3): 47 – 53. (in Chinese)

[9] Dai Hongjun, Jia Zhiping, Dong Xiaona. An entropy-based trust modeling and evaluation for wireless sensor networks [A]. Xingshe Zhou. The 2008 International Conference on Embedded Software and Systems[C]. San Francisco: IEEE, 2008. 134 – 146.

[10] 李德毅,孟海军,史雪梅.隶属云和隶属云发生器[J].计

算机研究与发展,1995,32(6):16 – 21.
Li Deyi, Meng Haijun, Shi Xuemei. Membership clouds and membership cloud generator[J]. Journal of Computer Research and Development. 1995,32(6):16 – 21. (in Chinese)
[11] Li D Y, Cheng D W, Shi X M. Uncertainty reasoning based on cloud models in controllers[J]. Computers and Mathematics with Applications, 1998, 35(3):99 – 123.
[12] Li D Y, Han J W, Shi XM. Knowledge representation and discovery based on linguistic atoms[J]. Knowledge-based System, 1998, 10(37):431 – 440.
[13] 蔡绍滨,方伟.基于区间的云相似度比较算法[J].小型微型计算机,2011,32(12):2456 – 2460.
Cai Shaobin, Fang Wei. Research of interval-based cloud similarity comparison algorithm[J]. Journal of Chinese Computer Systems, 2011, 32(12):2456 – 2460. (in Chinese)
[14] 吕辉军,李德毅,王晔.逆向云在定性评价中的应用[J].计算机学报,2003,26(8):1010 – 1019.
Lv Huijun, Li Deyi, Wang Ye. The application of Backward Cloud in Qualitative Evaluation[J]. Chinese Journal of Computers, 2011, 32(12):2456 – 2460. (in Chinese)
[15] Bin Ma. Cross-layer trust model and algorithm of node selection in wireless sensor networks[A]. Desheng Wen. The 2009 International Conference on Communication Software and Networks[C]. Washington, DC, USA, 2009. 45 – 60.
[16] Song S, Wang K. Trusted P2P transactions with fuzzy reputation aggregation[J]. IEEE Internet Computing, 2005, 9(6):24 – 34.
[17] Yan Sun, Zhu Han, Liu, K J R. Defense of trust management vulnerabilities in distributed networks[J]. IEEE Communications Magazine, 2008, 2(46):112 – 119.
[18] Grandison T, Sloman M. A survey of trust in internet applications[J]. IEEE Communications Surveys, 2000, 14(8):114 – 128.

作者简介

蔡绍滨 男,1973 年生于哈尔滨,哈尔滨工程大学计算机学院教授.中国计算机学会会员,主要研究方向为无线自组网和无线传感器网络.E-mail:caishaobin@ hrbeu.edu.cn

韩启龙 男,1974 年生于黑龙江肇东,博士,哈尔滨工程大学计算机学院副教授.中国计算机学会会员,主要研究方向为时空数据处理、图挖掘、传感器网络、敏感数据保护等.