基于信任的反馈云模型 WSN 节点信任评价机制

杨永飞[1] 刘光杰[1] 戴跃伟[1,2]
(南京理工大学自动化学院 南京 210094)[1] (江苏科技大学 镇江 212003)[2]

摘 要 在无线传感器网络(Wireless Sensor Network,WSN)中,节点信任评价作为传统的基于加密的安全体系的补充手段,可用于识别恶意节点并处理来自网络内部的攻击。针对用于数据采集的分簇 WSN,从节点所采集数据的时间和空间相关性出发,构建基准云模型进行基准云校验,计算节点的自身信任和邻近节点信任,提出了一种基于信任反馈的云模型节点信任双重评价机制。仿真实验结果表明,该方案不仅能够有效检测单节点恶意攻击,也适用于同簇内多节点合谋攻击。

关键词 无线传感器网络,信任评价,信任反馈云模型,自身信任,邻近节点信任
中图法分类号 TP393 文献标识码 A

Trust Evaluation Mechanism for Nodes Based on Adaptive Cloud Model in Wireless Sensor Network

YANG Yong-fei[1] LIU Guang-jie[1] DAI Yue-wei[1,2]
(School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China)[1]
(Jiangsu University of Science and Technology, Zhenjiang 212003, China)[2]

Abstract As the supplementary measure of the traditional encryption-based security system for wireless sensor network, trust evaluation of nodes can be employed to recognize the malicious nodes and conduct the attacks from inside of the network. With the temporal correlation and spatial correlation of the data gathered by nodes in clustered WSN for data acquisition, standard cloud benchmark was implemented with the construction of standard cloud model, the self trust and adjacent trust were computed respectively, and a two-tiered trust evaluation mechanism for nodes was proposed based on trust-feedback cloud model. Simulation results show that the proposed scheme can detect both single-node attack and inner-cluster multi-node collusive attack effectively.

Keywords Wireless sensor networks, Trust evaluation, Trust-feedback cloud model, Self trust, Adjacent trust

1 引言

无线传感网络(Wireless Sensor Network,WSN)一般由传感器节点、汇聚节点(簇头节点)和基站组成,在大多数应用场景中,传感器节点保持静止状态,并且通常部署在无人监控的开放式环境中,极易受到包括信息窃听、篡改数据和伪造记录等方式的攻击,同时,攻击者通过物理操纵等方式也可攻破传统安全机制的防护,捕获传感器节点以获取存储在节点上的信息来达到威胁网络运行的目的[1]。只依靠传统的加密方式无法保证 WSN 的安全,节点信任管理作为对传统加密安全体系的补充,通过对节点行为进行可靠性评估,依据信任值来实现对恶意节点的识别,从而有效抵御来自网络内部的攻击。

WSN 中节点信任管理的意义在于提供一种适应于该类网络特点以及动态特性的安全决策框架,本质上是采用一种客观理性的方式来准确描述复杂的信任关系[2]。近年来,关于 WSN 信任管理问题的研究,吸引了国内外众多学者的目光。当前比较典型的 WSN 信任模型主要包括基于声誉的信任模型[3-5]、基于概率的信任模型[6-8]、基于熵理论的信任模型[9]以及近来快速发展的基于云理论的信任模型[10-13]。前 3 类信任模型主要由节点对相邻节点的行为进行评估,依据不同的策略评估节点的可信程度,以一个定性的概念在一定程度上反映 WSN 节点可信程度的动态特性,但是不能很好地反映 WSN 中的节点可信度问题是根据外部环境产生变化的。隶属云[14]是基于模糊数学和概率统计的定性定量互换理论,反映事物概念的模糊性和随机性,既可以将语言描述的定性问题转化为定量数据范围或分布规律,也可以将定量数值转化为适当的定性语言描述。马彬等利用云理论定义 WSN 中的风险信号以及节点的动态上下文的不确定性,建立了基于风险评估方法的 WSN 云信任模型[10]。蔡绍滨等将云模型用作计算一次信任值的工具,构建了基于云理论的 WSN 信任模型,并将其运用到了恶意节点识别中[11]。徐晓斌等使用轻量云模型对直接信任、间接信任、推荐行为信任进行全面的不确定性表示,实现了异常情况下容忍度和敏感性之间的较好折衷[12]。文献[13]提出了一种基于单节点数据的群体信任评估的云模型,实现了实时的 WSN 异常数

本文受国家自然科学基金项目:网络环境中的多播隐写理论与方法研究(61472188),国家自然科学基金项目:基于模型的网络隐写检测研究(61170250)资助。

杨永飞(1991—),女,硕士,主要研究方向为分布式网络安全,E-mail:18260089811@163.com;刘光杰(1980—),男,博士,副研究员,主要研究方向为多媒体安全、网络安全;戴跃伟(1962—),男,博士,教授,博士生导师,主要研究方向为复杂网络系统、网络安全。

据过滤。

这些基于云理论的信任模型虽然一定程度上解决了入侵识别的敏感度和入侵容忍之间的矛盾，但是并未对云信任模型在外部环境变化中的自适应调整问题进行进一步研究，导致外部环境变化时节点的信任计算易出现偏差，且较少考虑邻近节点合谋情形下的多恶意节点识别问题。因此，本文在现有隶属云理论的基础上，针对数据采集类分簇 WSN 中节点采集数据的时间相关性和空间相关性，首先通过对 WSN 网络各分簇节点进行基准云校验，基准云模型根据反馈的历史综合信任值自适应调整，该校验实时性较强但准确度较低，进一步地，利用节点自身历史数据和当前数据的相关性来定义自身信任值，用目标节点采集的数据和其所处分簇中邻近节点的数据相关性来定义邻近节点信任，并对自身信任和邻近节点信任进行融合得到最终的综合信任评价结果，该双重信任评价体系不仅可以有效检测多变环境下的单节点恶意攻击，也可以在一定程度上抵抗多节点合谋攻击。

2 隶属云模型

隶属云模型是由李德毅院士提出的一种定性定量转换模型[14,15]，主要反映概念的模糊性和随机性，可以实现语言描述的定性概念和具体数值之间的不确定性转换，已经广泛应用于智能控制及模糊评测领域。

设 Ψ 为用精确数值表示的定量论域，Θ 是与 Ψ 相联系的定性概念，如果定量值 $x\in\Psi$ 为定性概念 Θ 上的一次随机实现，x 对 Θ 所表达的定性概念的隶属度（确定度）$T_\Theta(x)\in[0,1]$ 是具有稳定倾向的随机数，该隶属度在论域 Ψ 上的分布称为隶属云，简称云。云是从论域 Ψ 到数值区间 $[0,1]$ 的映射，$(x,T_\Theta(x))$ 称为云滴。云由云滴构成，用期望 Ex、熵 En 和超熵 He 3 个数值来表示其数字特征，该数字特征可以反映定性概念上的定量特征。

假定论域 Ψ 上有 n 个云滴，对应的定量值为 $x_1,x_2,\cdots,x_n$，则其构建的云模型 $C(Ex,En,He)$ 的数字特征为

$$Ex=\frac{1}{n}\sum_{i=1}^{n}x_i \tag{1}$$

$$En=\frac{1}{n}\cdot\sqrt{\frac{\pi}{2}}\cdot\sum_{i=1}^{n}|x_i-Ex| \tag{2}$$

$$He=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i-Ex)^2-En^2} \tag{3}$$

其中，期望 Ex 是云滴在论域空间 Ψ 分布的期望值，即概念量化最典型的样本，也是最能表示定性概念的点，在云图中体现为云的峰值所处的位置。熵 En 度量期望 Ex 的不确定性，是定性概念的度量，表示论域空间 Ψ 中可以被定性概念接受的取值范围，即模糊度，通常来说，越大的熵对应越宏观的概念，在云图中体现为云的宽度。超熵 He 度量熵 En 的不确定性，主要表征云滴的离散程度和随机性，越大的超熵对应越大的云滴离散程度，超熵在云图中体现为云图的厚度。

记两组数据构建的隶属云分别为 $C_1(Ex_1,En_1,He_1)$ 和 $C_2(Ex_2,En_2,He_2)$，云相似度 $S(C_1,C_2)$ 可用于评估两个云 C_1 和 C_2 之间的相似程度，在文献[13]中，将两个云作为向量 $\vec{V}_1=(Ex_1,En_1,He_1)$，$\vec{V}_2=(Ex_2,En_2,He_2)$ 进行近似度比较，使用两个云向量夹角余弦值表示。

$$S(C_1,C_2)=\frac{Ex_1\cdot Ex_2+En_1\cdot En_2+He_1\cdot He_2}{\sqrt{Ex_1^2+En_1^2+He_1^2}\cdot\sqrt{Ex_2^2+En_2^2+He_2^2}} \tag{4}$$

其中，$S(C_1,C_2)\in[-1,1]$，仅当 $\vec{V}_1=\lambda\vec{V}_2$ 时，有 $S(C_1,C_2)=1$；$\vec{V}_1=-\lambda\vec{V}_2$ 时，有 $S(C_1,C_2)=-1$，$\lambda>0$。

3 基于自适应云模型的 WSN 信任评价

3.1 数据驱动的分簇 WSN 信任评价系统的体系结构

本文以用于数据采集的分簇 WSN 为研究对象，提出一种基于采集数据驱动的信任反馈云信任模型，利用隶属云来描述 WSN 中传感器节点的通信以及数据采集的状态，各分簇的簇头节点依据分簇内的局部环境特点来构建基准云，从而对分簇的节点进行基准云校验，在基准云校验之外，通过计算节点的自身信任和邻近节点信任得到综合信任值，以尽量降低正常环境变化下由于异常数据导致的错误警报，同时能够有效识别恶意节点，并抵御多个邻近恶意节点发起的合谋攻击。

已有的大量的研究工作和论文已说明分簇 WSN 较非分簇 WSN 具有更好的性能[16,17]。所谓簇，就是具有某种关联的网络节点集合，用于数据采集的分簇 WSN 中的节点分为簇头节点和成员节点。簇头节点属于上层网络中的节点，与基站直接进行通信，每个簇由一个簇头节点和多个成员节点组成，在每个簇内，依据一定的算法选取簇头节点，具体的分簇方案在本文中不进行深入讨论。本文所提的基于信任反馈的云信任模型是在分簇 WSN 中节点采集数据的基础上进行构建的，所提的信任评价系统的体系结构如图 1 所示。

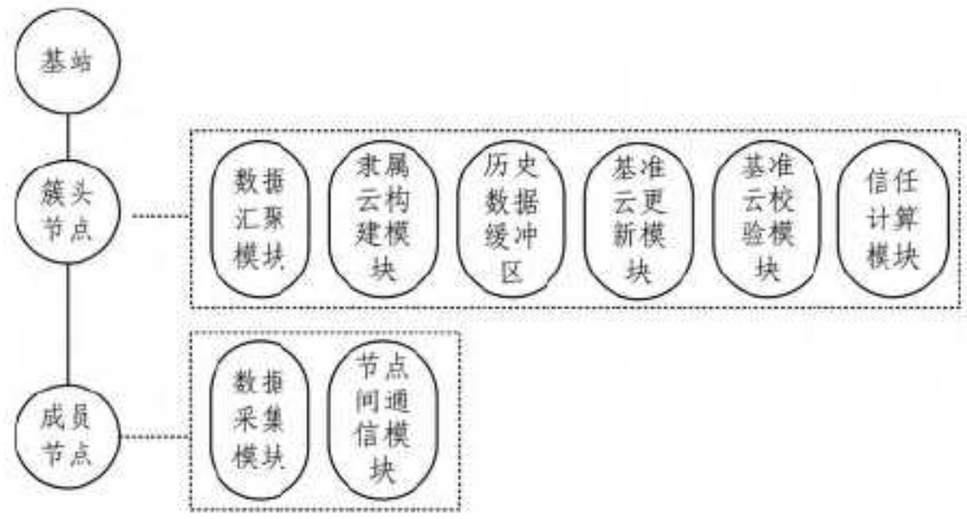

图 1 基于自适应云模型的 WSN 信任评价系统的体系结构

簇头节点包括数据汇聚模块、隶属云构建模块、历史数据缓冲区、基准云更新模块、基准云校验模块以及信任计算模块。数据汇聚模块负责将簇内成员节点采集的数据和计算得到的信任值汇集起来。隶属云构建模块将数据汇聚模块获取的数据信息处理后构建对应的隶属云。历史数据缓冲区存放节点的历史采样数据构建的云模型特征。基准云更新模块根据数据汇聚模块汇集得到的近期数据对存储在簇头节点的基准云数据进行更新以满足环境变化下节点信任管理需求。基准云校验模块负责将簇内各成员节点采集数据所构建的实时云模型与基准云进行比较。信任计算模块负责完成节点综合信任值的计算。

成员节点包括数据采集模块以及节点间通信模块。数据采集模块利用节点传感器获取节点所在位置的外部环境信息，并将其传递至簇头节点的数据汇聚模块。节点间通信模块负责接收簇头节点的信任评价结果等上层网络指令。

3.2 基于信任反馈云模型的 WSN 信任评价

对于数据采集型分簇 WSN，记各成员节点的数据采集模块的采样周期为 T，N 个采样周期为一个时间片。记节点 i 为网络中簇 A 的簇头节点，其对应的成员节点集合为 $\Phi=\{i_1,i_2,\cdots,i_m\}$，对其中任一成员节点 i_k，我们将 $i_r\in\Phi, r\neq k$ 视为其邻近节点。记节点 i_k 在时间片 t 内所采集的数据为 $X_t(k)=\{x_k(1),x_k(2),\cdots,x_k(N)\}$，则依据式(1)—式(3)构建当前采集数据对应的隶属云特征为 $C_t(Ex_t,En_t,He_t)$，历史数据缓存区中存放当前采集数据的前 p 个时间片数据所对应的隶属云特征向量 $C_{t-p+1}(Ex_{t-p+1},En_{t-p+1},He_{t-p+1})$，$\cdots,C_t(Ex_t,En_t,He_t)$，各成员节点以 1 个时间片为周期与簇头节点进行通信。为了同时兼顾节点自身信任的稳定性以及数据特性不稳定变化的 WSN 应用环境下的鲁棒性，成员节点 i_k 在时间片 t 内的自身信任值 ST_t 可由式(5)计算得到。

$$ST_t=\alpha_1\cdot ST_{t-1}+\alpha_2\cdot\left(\beta_1\cdot\frac{\min(Ex_t,\overline{Ex}_t)}{\max(Ex_t,\overline{Ex}_t)}+\beta_2\cdot\frac{\min(En_t,\overline{En}_t)}{\max(En_t,\overline{En}_t)}+\beta_3\cdot\frac{\min(He_t,\overline{He}_t)}{\max(He_t,\overline{He}_t)}\right) \tag{5}$$

其中，α_1 为历史自身信任权重系数，α_2 为当前自身信任权重系数，$\sum_{i=1}^{2}\alpha_i=1$，β_1、β_2、β_3 分别为期望、熵、超熵自身信任权重系数，$\sum_{i=1}^{3}\beta_i=1$。$\overline{Ex}_t$、$\overline{En}_t$、$\overline{He}_t$ 分别为 $C_{t-p+1},\cdots,C_{t-1}$ 这 $p-1$ 个历史隶属云对应的平均期望、平均熵以及平均超熵。

在节点自身信任的基础上，节点综合信任的评价还需要结合邻近节点的数据特性来进行比较得出。本文将同簇中的成员节点均视为彼此的邻近节点，考虑到同簇节点间数据的关联性(如地理位置相近的传感器节点监测到的温度、湿度等)，我们以节点隶属云相似度来衡量邻近节点信任，由于事实上隶属云的 3 个特征对于相似度衡量结果的影响权重并不相等，期望、熵、超熵对云相似度的影响是逐步递减的，因此，式(4)所提的夹角余弦云相似度度量方案在某些情形下并不能准确衡量两个节点数据的相似程度，以式(6)来计算时间片 t 内节点 i_r 相对于 i_k 的相似度 $S(C_r,C_k)$。

$$S(C_r,C_k)=\beta_1\cdot\frac{\min(Ex_r,Ex_k)}{\max(Ex_r,Ex_k)}+\beta_2\cdot\frac{\min(En_r,En_k)}{\max(En_r,En_k)}+\beta_3\cdot\frac{\min(He_r,He_k)}{\max(He_r,He_k)} \tag{6}$$

β_1、β_2、β_3 分别为期望、熵、超熵自身信任权重系数，$\sum_{i=1}^{3}\beta_i=1$。则时间片 t 内节点 i_k 的邻近节点信任值 AT_t 为

$$AT_t=\frac{\sum_{r\in\Phi,r\neq k}CT_{t-1}(r)\cdot S(C_r,C_k)}{\sum_{r\in\Phi,r\neq k}CT_{t-1}(r)} \tag{7}$$

其中，$CT_{t-1}(r)$ 为时间片 $t-1$ 内节点 i_r 的综合信任值。

当面临同簇内多个恶意节点发起的合谋攻击时，多个邻近的恶意节点可能通过相互刷新邻近节点信任值来提高综合信任评价值，为了有效抵抗这种簇内合谋攻击，同时减小节点的计算负荷，在轻量云模型[12]的基础上，提出一种基准云校验和更新机制，根据节点信任值反馈动态调整每个时间片内的簇基准云。时间片 t 内簇基准轻量云 $C_t^*(Ex_t^*,En_t^*)$ 对应的期望特征和熵特征为

$$\begin{cases}Ex_t^*=\dfrac{\sum_{i=1}^{p}\sum_{r\in\Phi}CT_{t-i}(r)\cdot Ex_{t-i+1}(r)}{\sum_{i=1}^{p}\sum_{r\in\Phi}CT_{t-i}(r)}\\[2ex] En_t^*=\dfrac{\sum_{i=1}^{p}\sum_{r\in\Phi}CT_{t-i}(r)\cdot En_{t-i+1}(r)}{\sum_{i=1}^{p}\sum_{r\in\Phi}CT_{t-i}(r)}\end{cases} \tag{8}$$

其中，$Ex_t(r)$、$En_t(r)$ 分别为时间片 t 内成员节点 i_r 所构建隶属云的期望和熵，$CT_t(r)$ 为其对应的综合信任值，若 i_r 已被确定为恶意节点，则 $CT_t(r)=0$。我们利用轻量云相似度算子[12]计算成员节点 i_r 时间片 t 内采集的数据构建的隶属云与基准云之间的相似度 $S_t(r)$。

$$S_t(r)=\left(1-\frac{|Ex_t(r)-Ex_t^*|}{|Ex_t(r)+Ex_t^*|}\right)\left(1-\frac{|En_t(r)-En_t^*|}{|En_t(r)+En_t^*|}\right) \tag{9}$$

$S_t(r)\in[0,1]$，若 $S_t(r)<\gamma$，则节点 i_r 视为异常节点，其中 γ 为设定的异常门限值。

综上所述，本文所提的基于信任反馈云模型的 WSN 节点信任评价机制的流程如图 2 所示。

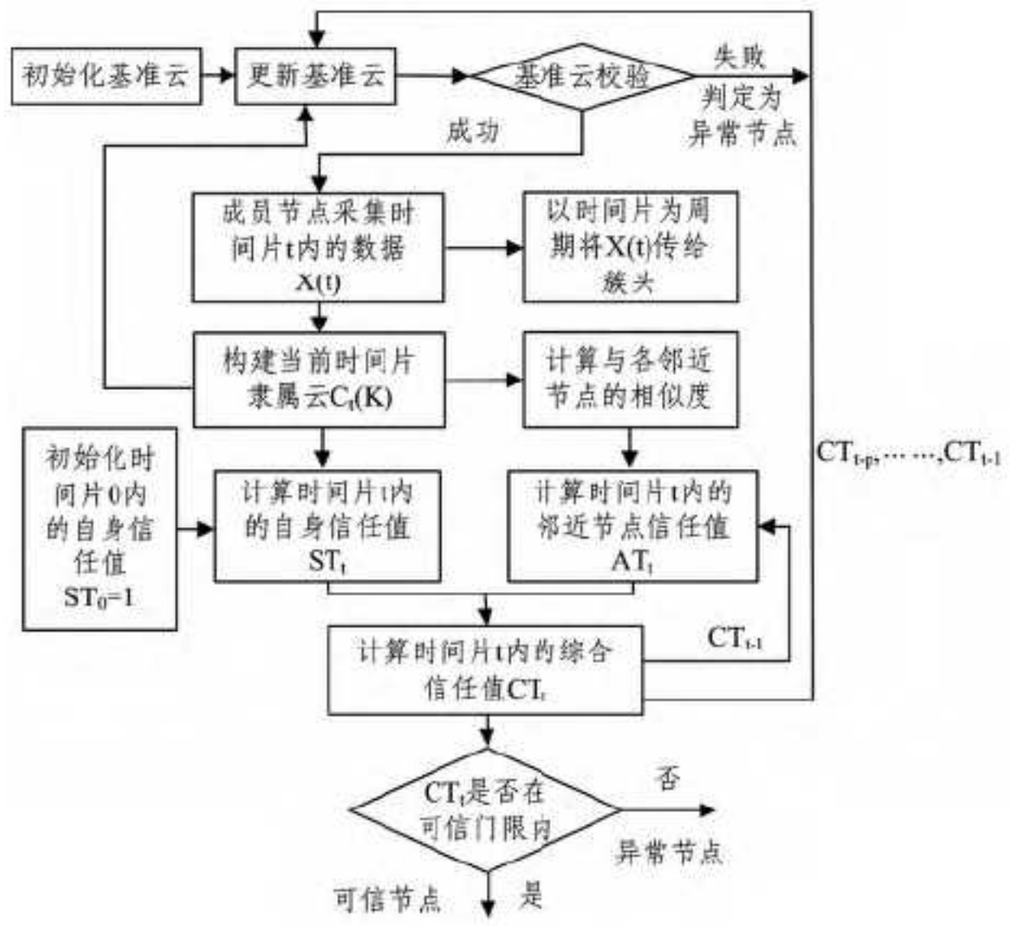

图 2 基于信任反馈云模型的 WSN 信任评价流程

Step 1 初始化簇基准云 $C_0^*(Ex_0^*,En_0^*)$，$Ex_0^*=\frac{1}{m}\sum_{r\in\Phi}Ex_0(r)$，$En_0^*=\frac{1}{m}\sum_{r\in\Phi}En_0(r)$，$Ex_0(r)$ 和 $En_0(r)$ 分别为成员节点 i_r 初始时间片内采集数据所构建的隶属云的期望和熵，各节点的初始综合信任值均设为 1，基准云以时间片为周期根据反馈的各节点的历史综合信任值按式(8)进行更新。

Step 2 利用式(9)所示的轻量云相似度算子计算任一成员节点 i_r 时间片 t 内采集的数据构建的隶属云与基准云之间的相似度 $S_t(r)$，若 $S_t(r)$ 低于门限值 γ，则节点 i_r 被视为异常节点，簇头节点限制该节点的通信行为并停止采集数据；反之，节点正常工作并继续采集数据。

Step 3 记节点 i_r 在时间片 t 内所采集的数据为 $X_t=\{x(1),x(2),\cdots,x(N)\}$，将该数据传递给簇头，由式(1)—式(3)构建当前隶属云 $C_t(Ex_t,En_t,He_t)$，并依据式(5)计算节点自身信任值 ST_t，其中，初始时间片内的节点自身信任值初始化为 $ST_0=1$。

Step 4 根据式(6)计算该节点与各邻近节点的相似度

并结合反馈的上一时间片内的综合信任值来计算邻近节点信任值 AT_t。

Step 5 该节点的综合信任值由自身信任值和邻近节点信任值综合得到，$CT_t=\omega \cdot ST_t+(1-\omega) \cdot AT_t$，若综合信任值 CT_t 高于可信门限值 η，则该节点为可信节点；反之，判定为异常节点。

4 隶属云模型

本文以 Matlab 为仿真平台，以部署在 Intel Berkeley Research Lab[18] 中的 54 个 Mica2Dot 传感器节点在 2004 年 2 月 28 日至 4 月 5 日间采集的湿度、温度、光照度和电压值等信息为基础进行仿真实验。传感器节点基于 TinyOS 平台中的 TinyDB 网内查询处理系统进行周期为 31 秒的数据采集。这些传感器在实验环境中的布局如图 3 所示。

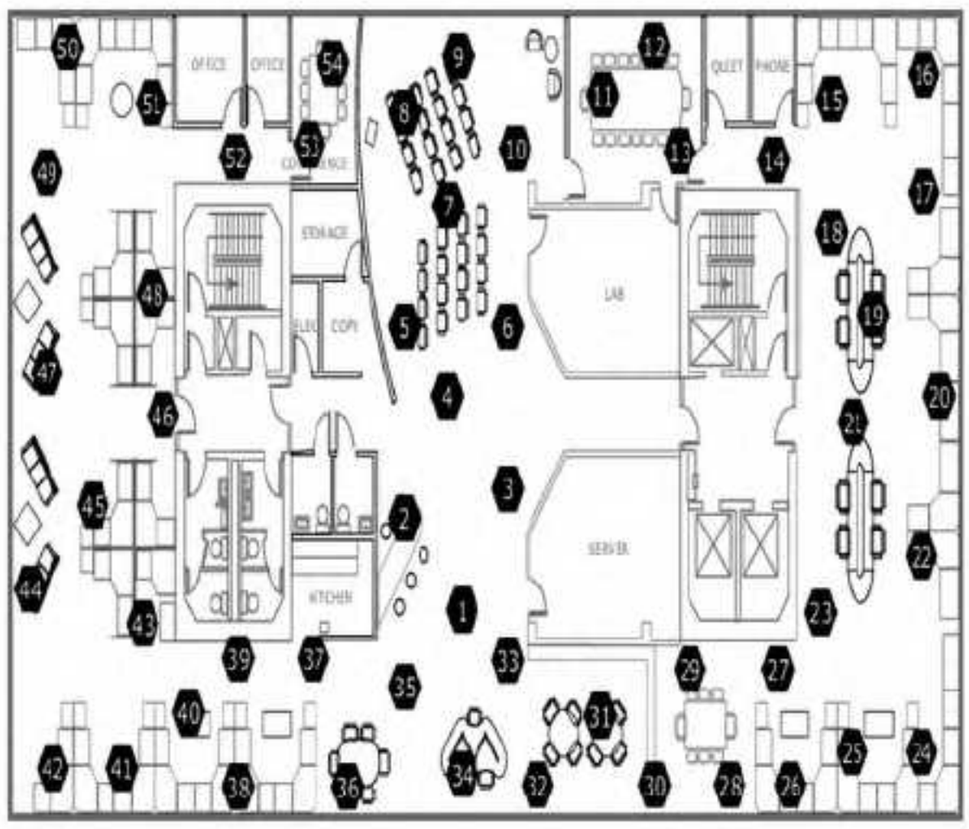

图 3 实验环境中传感器的布局

在本文实验中，我们按空间位置将 54 个传感器节点进行分簇，共分为 6 簇，每簇包括 9 个节点，Cluster 1：节点 1－9；Cluster 2：节点 10－18；Cluster 3：节点 19－27；Cluster 4：节点 28－36；Cluster 5：节点 37－45；Cluster 6：节点 46－54。簇头节点视为上层网络节点，每个分簇内的任意两个节点都视为彼此的邻近节点。

这里，设置一个时间片包含 20 个采样周期，即 $N=20$。从 230 万组采集的数据中抽取连续的 300 组数据中的电压值作为研究对象（由于该数据集的数值有较大缺失，电压项缺失较少）。每个节点采集的连续 20 个电压值构建其对应的云模型。基准云校验门限值 γ 设定为 0.6，可信门限值 η 设定为 0.8。式(5)中的历史自身信任权重系数 $\alpha_1=0.4$，当前自身信任权重系数 $\alpha_2=0.6$，期望、熵、超熵自身信任权重系数分别为 $\beta_1=0.6,\beta_2=0.3,\beta_3=0.1$，式(8)中的缓冲区参数 p 为 3，自身历史信任和邻近节点信任融合系数 ω 定为 0.5。我们以最典型的针对 WSN 网络节点信任值评价系统的 On-off 攻击[19] 为恶意节点的攻击类型。该类攻击中，恶意节点是通过保持一段时间的较好网络通信行为后再表现出不好的行为，发送错误数据，当节点信任值降低到一定限度后又开始恢复良好的通信行为为下次攻击累计信任，如此反复。错误数据是指和正常数值偏差超过 10% 的数据，偏差幅度比例记为攻击强度 δ。

首先，我们验证本文所提的信任评价机制对单节点异常的抵御，由于分簇 3 中各传感器节点的数据较为完备，这里，我们以分簇 3 为研究对象，在分簇 3 中随机选取 1 个传感器节点（这里选取节点 24）作为恶意节点，设定其在每 3 个时间片的正常通信后会在一个时间片内发送错误数据，错误数据对应的攻击强度为 $\delta=\{0.1,0.2,0.3\}$。则该节点正常数据和 On-Off 攻击下的数据在 15 个时间片内的基准云校验值和综合信任值如图 4 所示。

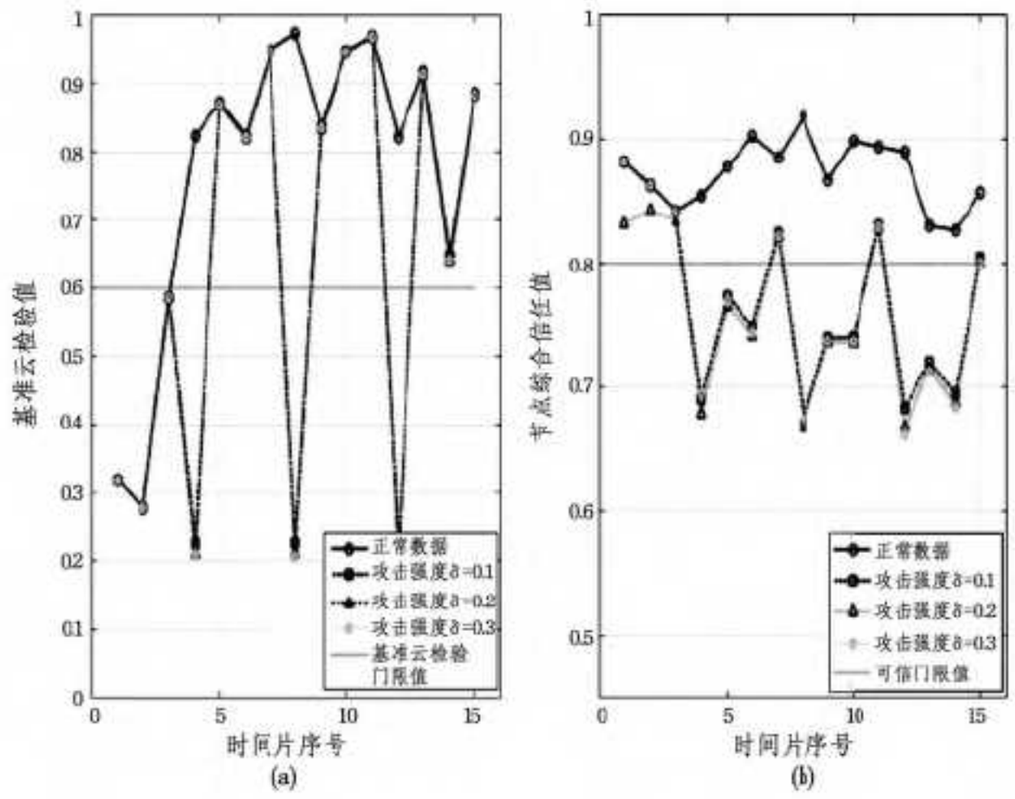

图 4 单个节点正常数据和异常数据的基准云校验值和综合信任值

由图 4 可知，除去信任评价系统起始运行时间（以时间片 5 开始进行性能分析），针对单个节点的异常数据，本文所提的方案中的基准云校验值和综合信任值均可以实时准确地将节点的异常行为区别开来，对攻击行为较为敏感，当攻击强度 $\delta=0.1$ 时依然能准确地检测出异常节点。随着攻击强度增加，节点综合信任值的下降幅度也随之增大。其中，基准云校验值的变动幅值较大，在节点发动 On-Off 攻击后恢复正常的时间片内，节点的基准云校验值又迅速回升超过基准云校验门限值，该校验对实时数据的敏感性较强，而节点综合信任值对恶意节点的恶意行为具有较强的记忆性，节点发动恶意攻击后 3 个时间片内其综合信任值依然较难恢复到可信门限值以上。

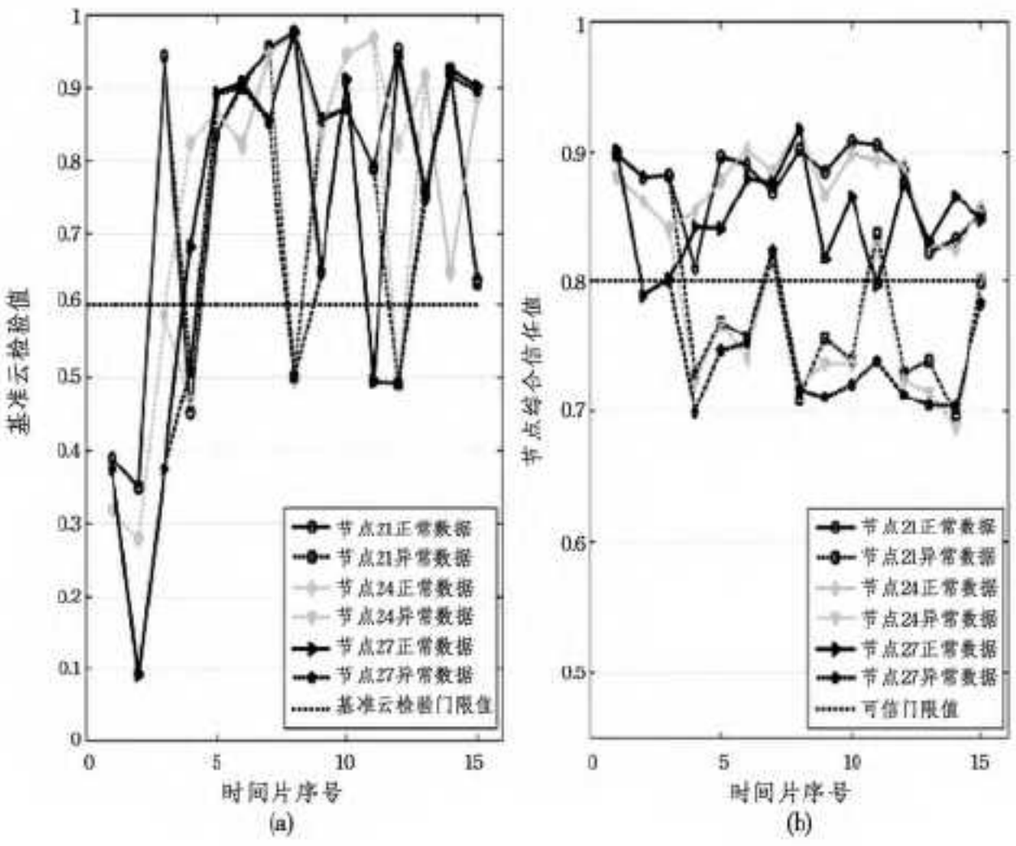

图 5 同簇多个节点正常数据和合谋异常数据的基准云校验值和综合信任值

为了考察本文所提方案对同簇内多个恶意节点同时异常刷新邻近节点信任来提高综合信任值行为的抵抗能力，选取

分簇$_3$中节点$_{21}$、节点$_{24}$和节点$_{27}$同时作为恶意节点，发动攻击强度$_{\delta=0.2}$的On-Off攻击，$_3$个节点均在每$_3$个时间片的正常通信后在一个时间片内发送错误数据。其正常数据和合谋异常数据的基准云校验值和综合信任值如图$_5$所示。

由图$_5$可知，本文所提的基准云校验对于多个节点的合谋攻击有一定的误差，以节点$_{27}$为例，该校验并不能较准确地区分正常数据和异常数据，而综合信任值依然可以准确地将同簇内的多个异常节点准确地检测出来。基准云校验作为初步信任评估手段，准确性较差，计算复杂度较低，而综合信任值计算可以进一步地对节点的通信行为进行评价，但是相应的计算复杂度较高，对簇头节点的计算能力有一定要求。二者相结合可以形成对WSN节点的双重信任评价方案，可以根据实际需求对这两重评价手段进行不同程度的侧重来兼顾评价的准确性和实时性。

结束语　本文针对分簇WSN同簇节点采集数据的空间相关性和时间相关性，基于隶属云理论提出一种基于信任反馈云模型的WSN节点信任评价方案，构建了双重信任评价体系，利用轻量云模型进行基准云校验，基准云依据反馈的历史综合信任值进行动态更新，该校验计算复杂度低但准确度较低，除基准云校验外，由节点自身信任和邻近节点信任融合成的综合信任值可以更为准确地反映节点的通信行为可信程度。二者结合构成的双重信任评价体系可以根据外界环境变化调整隶属云模型，并实时准确地检测单节点异常和多节点合谋攻击。所提的评价方案是基于采集数据驱动的，基准云校验和信任计算均在簇头节点完成，簇头节点的计算资源需求较大，对于各成员节点间的数据转发行为并未予以考虑，下一步的研究工作为对于成员节点间有转发行为的WSN网络结合信任反馈隶属云模型进行信任评价研究。

参 考 文 献

[1] 荆琦，唐礼勇，陈钟. 无线传感器网络中的信任管理[J]. 软件学报，2008，19(7)：1716-1730

[2] 邵斐. 基于模糊综合评判的主观信任模型研究[J]. 通信技术，2009，42(12)：98-100

[3] 王建新，张亚男，王伟平，等. 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

[4] Ganeriwal S，Balzano L K，Srivastava M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks(TOSN)，2008，4(3)：15

[5] 马守明，王汝传，叶宁. 基于信誉度集对分析的WSN安全数据融合[J]. 计算机研究与发展，2011(9)：1652-1658

[6] 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

[7] 刘涛，熊焰，黄文超，等. 一种基于Bayes估计的WSN节点信任度计算模型[J]. 计算机科学，2013，40(10)：61-64

[8] 刘涛，关亚文，熊焰，等. 无人值守WSN中一种具有激励机制的信任管理模型[J]. 武汉大学学报：理学版，2013(6)：578-582

[9] Hongjun D，Zhiping J，Xiaona D. An entropy-based trust modeling and evaluation for wireless sensor networks[C]// International Conference on Embedded Software and Systems(ICESS'08). IEEE，2008：27-34

[10] 马彬，谢显中. 无线传感器网络云信任模型[J]. 计算机科学，2010，37(3)：128-132

[11] 蔡绍滨，韩启龙，高振国，等. 基于云模型的无线传感器网络恶意节点识别技术的研究[J]. 电子学报，2012，40(11)：2232-2238

[12] 徐晓斌，张光卫，王尚广，等. 基于轻量云模型的WSN不确定性信任表示方法[J]. 通信学报，2014，35(2)：63-69

[13] 徐晓斌，张光卫，王尚广，等. 基于群体信任的WSN异常数据过滤方法[J]. 通信学报，2014，35(5)：108-117.

[14] 李德毅，孟海军. 隶属云和隶属云发生器[J]. 计算机研究与发展，1995，32(6)：15-20

[15] 李德毅，刘常昱. 论正态云模型的普适性[J]. 中国工程科学，2004，6(8)：28-34

[16] 冯清青，李霁野. 无线传感器网络节点分簇与非分簇性能比较[J]. 计算机应用研究，2009(11)：4244-4247

[17] 李捷，韩志杰. 一种基于预测的WSN非均衡分簇路由算法[J]. 计算机研究与发展，2010(8)：1459-1465

[18] http://db.lcs.mit.edu/labdata/labdata.html

[19] Sun Y L，Han Z，Liu K J R. Defense of trust management vulnerabilities in distributed networks[J]. Communications Magazine，IEEE，2008，46(2)：112-119

(上接第381页)

[2] Winslett M. An introduction to trust negotiation [M]// Trust Management. Springer Berlin Heidelberg，2003：275-283

[3] Harrison M A，Ruzzo W L，Ullman J D. Protection in operating systems[J]. Communications of the ACM，1976，19(8)：461-471

[4] Bell D E，LaPadula L J. Secure computer systems：Mathematical foundations[R]. Mitre Corp Bedford MA，1973

[5] Ferraiolo D，Kuhn D R，Chandramouli R. Role-based access control[M]. Artech House，2003

[6] Sandhu R S，Coyne E J，Feinstein H L，et al. Role-based access control models[J]. Computer，1996，29(2)：38-47

[7] Blaze M，Feigenbaum J，Lacy J. Decentralized trust management [C]// Proceedings.，1996 IEEE Symposium on Security and Privacy，1996. IEEE，1996：164-173

[8] Bertino E，Ferrari E，Squicciarini A C. Trust-𝒳：a peer-to-peer framework for trust establishment[J]. IEEE Transactions on Knowledge and Data Engineering，2004，16(7)：827-842

[9] Liu B，Lu H. A peer-to-peer framework for accelerating trust establishment[C]// International Conference on Multimedia Information Networking and Security，2009 (MINES'09). IEEE，2009，1：135-139

[10] Liu B，Lu H，Zhao Y，et al. A Framework：Trust Establishment for E-services[C]// International Conference on e-Education，e-Business，e-Management，and e-Learning，2010 (IC4E'10). IEEE，2010：141-145

[11] Jianli L. Multi-negotiation targets in Automated Trust Negotiation over TrustBuilder framework[C]// 2012 8th International Conference on Computing Technology and Information Management(NCM and ICNIT). 2012，1：101-105

[12] 廖振松. 虚拟组织中自动信任协商研究[D]. 武汉：华中科技大学，2008