doi:10.3969/j.issn.1000-436x.2014.02.009

基于轻量云模型的 WSN 不确定性信任表示方法

徐晓斌，张光卫，王尚广，孙其博，杨放春
（北京邮电大学 网络与交换技术国家重点实验室，北京 100876）

摘 要：参考云模型定性定量不确定性转换特性，设计了适用于 WSN 的轻量云模型，使用此模型对直接信任、间接信任、推荐行为的信任进行全面的不确定性表示。轻量云模型计算简单，每一个 WSN 节点均可独立建立轻量云模型，并对邻居节点信任情况进行全面的评估，从而发现 WSN 应用中的安全问题。实验结果表明，该方法克服了传统信任管理框架中敏感度与容忍度之间的矛盾，既保证了多种异常情况的高容忍度，又具备较敏感的攻击识别能力。

关键词：WSN 安全；信任管理；入侵容忍；入侵识别；云模型
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)02-0063-07

Representation for uncertainty trust of WSN based on lightweight-cloud

XU Xiao-bin, ZHANG Guang-wei, WANG Shang-guang, SUN Qi-bo, YANG Fang-chun
(State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: According to the characteristic of qualitative and quantitative uncertainty conversion ability of cloud model, a lightweight cloud model was designed, and the uncertainty representation of direct trust, indirect trust, and recommendation trust in WSN was proposed. The computation cost of lightweight cloud model is quite low so that a single node can build lightweight cloud model independently and evaluate the trust of other nodes to find out the safety hazards in WSN. Simulations in multiple scenarios verify the effectiveness of the proposed method. Simulation results show that this method overcomes the contradiction between the sensitivity and tolerance of traditional trust management framework, furthermore, it's not only tolerant of abnormal conditions, but also sensitive to multiple attacks.

Key words: WSN security; trust management; intrusion tolerance; intrusion recognition; cloud model

1 引言

无线传感器网络（WSN, wireless sensor network）是物联网感知层的一种典型应用。WSN 是一个动态的开放网络，通常部署于外界，易于出现突发故障或者遭遇敌手的恶意攻击，WSN 节点的安全保护在 WSN 应用中尤为重要[1,2]。由于 WSN 节点硬件通常较为廉价，计算能力较弱，难于实现较复杂的加密算法，仅通过传统的加密方式不足以保护 WSN 的安全[3]。作为对 WSN 传统加密安全策略的有效补充，信任管理对节点行为进行分析，使用信任值描述节点行为的可靠性，为 WSN 的路由选择、数据融合等提供支持，从而保证在出现攻击时，WSN 能够保持可靠的运作。基于信任的 WSN 安全保护通常有 2 个主要目标：入侵的识别与入侵的容忍。入侵的识别要求信任的变化对于入侵行为有较高的敏感度，以便及时发现入侵行为；入侵的容忍要求在出现入侵行为时，尽可能不影

收稿日期：2013-09-06；**修回日期**：2013-11-29
基金项目：教育部新世纪优秀人才支持计划基金资助项目(NCET100263)；教育部博士点基金资助项目(20110005130001)；国家高技术研究发展计划(“863”计划)基金资助项目(2011AA01A102)；国家自然科学基金资助项目(61272521)
Foundation Items: The New Century Talent Supporting Project of Education Ministry (NCET100263); PhD Programs Foundation of Ministry of Education(20110005130001); The National High Technology Research and Development Program of China (863 Program) (2011AA01A102); The National Natural Science Foundation of China (61272521)

响原有信任情况，以便顺利完成原定任务。二者存在矛盾关系。

1996年，B1aze等人首先提出了信任管理的概念[4]。之后，信任管理被应用于WSN、ad hoc等多种场景。在现有信任管理方法中，对信任的表示通常有2种方式：一种方式使用信任等级来表示节点是否可信[5]，另一种表示方式在业界应用较多，通过对节点的行为、数据等因素进行计算，使用[0,1]之间的数值表示信任。Ganeriwal等人提出的RFSN系统[6]是一个较为完整的基于信誉的无线传感器网络信任管理的框架，该方法使用直接信息和间接信息来计算信誉。然而由于对信誉的表示过于简单，该算法不具备恶嘴攻击的容忍能力。Klasniewski等人提出的TIBFIT模型[7]参照信任值进行数据的融合，以减小误差。然而这种模型仍然无法准确描述节点信任的不确定性，灵活性较差。Momani等人提出了无线传感器网络中的贝叶斯网络信任模型(BNWSN)[8]，通过贝叶斯网络，对节点通信信任和数据信任进行整和，从而评估节点之间的信任关系，不同信任组件可以便捷的添加或删除。肖德琴等人探讨了一种基于高斯分布的传感器网络信誉模型(GRFSN)[9]，并通过仿真实验，说明了高斯分布可更好地保持信誉稳定性。杨光等人提出了一种WSN节点行为评测模型MA&TP-BRSN，将节点评价行为与通信行为区分开来，建立了对第三方节点恶意评价行为的具体测评方法[10]，该方法能在一定程度上消除高信誉节点的恶意诽谤行，然而由于最终的信任情况仅用一个数字表示，恶意诽谤识别的敏感度较低。蔡绍滨等人在信任模型和云理论的研究基础上，构建了基于云理论的无线传感器网络信任模型——云信任模型(CTM)，并将之运用到了恶意节点识别中[11]。此模型中，云模型被用做计算一次信任值的工具，信任值仍然使用一个数字表示，该方法未能很好地利用云模型解决入侵识别的敏感度与入侵容忍之间的矛盾。Bao等人提出了一个高度可扩展的集群层次信任管理无线传感器网络协议[12]，通过多种信任属性，总体评价一个传感器节点的信任，并将之应用于地理路由及其入侵检测中。现有的WSN信任管理模型大多将多种类型的行为整合为一个信任值，使用此单一数值表征节点信任情况，使用此方法可能遇到如下情况：当节点出现噪声、遭遇入侵或恶意诋毁时，若该节点信任值降低程度较高，则入侵识别敏感度较高，而入侵容忍能力相对不足，该节点将在长时间内无法按照原定计划完成任务；若信任值减低程度较低，则入侵容忍程度较高，而入侵识别敏感度相对不足，难于及时发现恶意攻击。因此，如何设计一种信任表示方法，既保证异常行为的敏感度，又实现噪声及入侵的容忍是信任评估的核心问题。

本文在已有信任管理方法研究的基础上，在不确定性定性定量转换模型——云模型[13]基础上，提出了计算简单，适用于WSN的轻量云模型。轻量云模型主要包括轻量云的表示、轻量正向云算子、轻量逆向云算子、轻量云相似度算子。使用轻量云，表征节点之间的信任关系，既描述了节点的整体信任情况，又对信任的不确定度进行了量化评估；在信任值计算时，对节点直接交互情况和邻居节点的推荐情况进行分别评估，全面表示网络中节点间的信任情况；提出了WSN中轻量云信任(LCT，lightweight-cloud trust for sensor network)的概念，并给出了信任管理中常见的直接信任、间接信任、推荐行为信任的表示和计算方法，实现了WSN中节点信任度全面的不确定性描述。

经过仿真实验，证明了这种表示方法对于噪声和入侵既有较强的容忍能力，又有较敏感的识别能力。为WSN应用中的可信路由选择及可靠数据融合提供了基础。

2 轻量云信任

由于WSN节点硬件计算存储能力较弱，且电能受限，因此传统信息安全相关技术在WSN中不再适用，WSN应用中节点能力具备不确定性，使用云模型对WSN节点进行信任评价，能够量化评估节点信任的不确定性，既可以保证信任情况的相对稳定，又可以实现较敏感的异常行为发现。在WSN的信任管理中，如何降低算法的复杂度是一个重要问题，基于此，本文在云模型的基础上，提出了计算简单高效，且性能与云模型接近的轻量云模型，并将之运用于WSN信任表示中。

2.1 云模型

云模型是定性概念与其数值表示之间的不确定性转换模型，由我国工程院院士李德毅教授于1995年正式提出。至今云模型已成功应用到数据挖掘、智能控制、图像处理等众多领域。

定义1 云和云滴 设U是一个用数值表示的定量论域，C是U上的定性概念，若定量值$x\in U$

是定性概念 C 的一次随机实现，x 对 C 的确定度 $\mu(x)\in[0,1]$是有稳定倾向的随机数。

$\mu:U\to[0,1]\ \forall x\in U\ x\to\mu(x)$，则 x 在论域 U 上的分布称为云，记为云 $C(X)$。每一个 x 称为一个云滴[13]。

正态云模型是最重要的一种云模型，可以表征自然科学、社会科学中大量的不确定现象。以云的数字特征——期望 Ex、熵 En 和超熵 He 表示定量数据的定性特征，用以表示数据的整体水平、离散程度及不确定度，记做 $C(Ex, En, He)$，称为云的特征向量。

通过正向云算法可以把定性概念的整体特征变换为定量数值表示；通过逆向云算法可以实现从定量值到定性概念的转换，将一组定量数据转换为以数字特征$\{Ex, En, He\}$表示的定性概念。

2.2　轻量云模型

在 WSN 中，节点计算能力有限，因而在设计 WSN 中算法时，应尽量以加减法为主，尽可能减少乘除法，尽量避免较复杂的计算，如开方、求对数等。WSN 中计算的开销往往以乘除法的次数衡量。基于此，在云模型的基础上，提出适合 WSN 中信任表示及计算的轻量云模型(LCM, lightweight cloud model)，其表示方法如下。

定义 2　轻量云模型的定性　表示轻量云模型的定性表示是由 2 个数字特征构成的元组 $LC=(Ex, En)$，其中，Ex(expected value)是云滴在论域空间分布的期望；En(entropy)表示熵，是定性概念随机性的度量，反映了能够代表这个定性概念的云滴的离散程度；另一方面又是定性概念亦此亦彼性的度量，反映了在论域空间可被概念接受的云滴的取值范围。

在轻量云模型中，正向云算子实现定性概念向定量数据的转换，逆向云算子实现定量数据想定性概念的转换，云相似度算子实现了 2 个概念之间的相似度比较。3 个算子定义如下。

定义 3　轻量正向云算子　轻量正向云算子 $Ar^{\text{Forward}}(LC(Ex,En))$ 是一个把轻量云模型的定性表示变换为定量数据集合的映射 $\pi:LC\to S$，满足：

1) $X=\{x_i\mid x_i=Norm(Ex,En),i=1,2,\cdots,N\}$；

2) $S=\{(x_i,y_i)\mid x_i\in X,y_i=\mathrm{e}^{-(x_i-Ex)^2}\}$

定义 4　轻量逆向云算子　轻量逆向云算子 $Ar^{\text{Backward}}(S)$ 是一个把定量数据集合变换为轻量云模型的定性表示的映射 $\pi:S\to LC$，满足：

1) $Ex=\overline{X},X=\{x_i\mid(x_i,y_i)\in S\}$；

2) $En=\sqrt{\dfrac{\pi}{2}}\overline{|x_i-Ex|},x_i\in X$

定义 5　轻量云相似度算子　轻量云相似度算子 $Ar^{\text{likeness}}(LC_i(Ex_i,En_i),LC_j(Ex_j,En_j))$ 是一个把 2 个轻量云模型变换为二者相似度表示的映射 $\pi:(LC_i,LC_j)\to sim(i,j)$，满足：

1) $sim(i,j)\in[0,1],LC_i=LC_j$ 时，$sim(i,j)=1$；

2) $sim(i,j)=(1-\dfrac{|En_i-En_j|}{|En_i+En_i|})(1-\dfrac{|Ex_i-Ex_j|}{|Ex_i+Ex_i|})$。

使用轻量云模型表示信任，即可以反映信任的整体水平，还能表示信任的不确定性，当信任度改变时，整体水平的变化较平缓，而不确定度的变化较剧烈。使用轻量逆向云算子，可以实现定量的信任值向定性的信任情况的映射，使用轻量云相似度算子，可以实现 2 个定性信任情况的相似度比较。

3　基于轻量云模型的 WSN 信任表示方法

信任指标是对信任值计算的基础与目标。本文综合了当前信任管理框架中的主要信任元素，提出了较为全面的信任指标，并定义了各指标的轻量云表示，在此基础上，提出了信任云算法。

3.1　信任指标及其轻量云信任

在信任管理体系中，评估信任情况的指标通常有直接信任、间接信任、推荐行为的信任等。现给出 3 个指标的定义如下。

定义 6　直接信任　WSN 中，节点根据直接交互行为得到的另一节点信任情况称为直接信任。直接信任可以通过对通信情况、数据可靠程度的分析得到。节点 i 对节点 j 的直接信任用 T_{ij} 表示。

定义 7　间接信任　节点通过其他节点的推荐行为得到的另一节点的信任情况称为间接信任。节点 i 对节点 j 的间接信任用 ST_{ij} 表示。

定义 8　推荐行为的信任　节点对推荐行为评估得到的信任情况称为推荐行为的信任。节点 i 对节点 j 推荐行为的信任用 RT_{ij} 表示。

传统的 WSN 信任管理模型通常将多次计算的不同信任值整合为一个信任值，这种方法往往无法兼顾入侵识别的敏感度与入侵的容忍。使用轻量云，使用二元组表示各信任指标：$T_{ij}(Ex,En)$、$ST_{ij}(Ex,En)$、$RT_{ij}(Ex,En)$，以轻量云的期望作为整

体信任情况，熵作为信任的不确定性。信任值改变时，期望会较为稳定，而熵对于变化较为敏感，可以兼顾入侵的容忍与入侵识别的敏感度，用户可根据应用的场景与需要，综合分析 2 个参数的变化，制定管理策略。这种信任表示方法称为轻量云信任(LCT, lightweight-cloud trust for sensor network)。

3.2 轻量云信任算法

直接信任、间接信任、推荐行为的信任均可通过轻量云模型中的算子进行计算，算法如下。

算法 1 WSN 直接信任算法

输入：节点 i 对节点 j 直接信任值 $\{t_1,t_2,\cdots,t_n\}$，$n\in N^*$

输出：直接信任 T_{ij}

step 1：令 $S=\{t_1,t_2,\cdots,t_n\},n\in N^*$；

step 2：$LC=Ar^{\text{Backward}}(S)$；

step 3：$T_{ij}=LC$。

直接信任算法使用逆向云算子，只需 2 次除法 1 次乘法，计算较为简单，适用于 WSN 节点。

算法 2 WSN 间接信任算法

输入：节点集 $\{k_1,k_2,\cdots,k_n\},n\in N^*$ 向节点 i 推荐的节点 j 信任 $\{T_{k_1j},T_{k_2j},\cdots,T_{k_nj},\},n\in N^*$

输出：间接信任 ST_{ij}

step 1：令 $S=\{T_{k_1j},T_{k_2j},\cdots,T_{k_nj},\},n\in N^*$；

step 2：$Ex=\{ex_i\mid(ex_i,en_i)\in S\},i=1,2,\cdots,n$；

step 3：$En=\{en_i\mid(ex_i,en_i)\in S\},i=1,2,\cdots,n$；

step 4：$LC=(\overline{Ex},\overline{En})$；

step 5：$ST_{ij}=LC$。

间接信任算法只需 2 次除法，计算较为简单，适用于 WSN 节点。

算法 3 WSN 推荐行为信任算法

输入：推荐信任集 $\{T_{jk_1},T_{jk_2},\cdots,T_{jk_n}\},n\in N^*$，直接信任集 $\{T_{ik_1},T_{ik_2},\cdots,T_{ik_n}\},n\in N^*$。

输出：推荐行为的信任 RT_{ij}

step 1：$sim_t=Ar^{\text{likeness}}(T_{jk_t},T_{ik_t}),t=1,2,\cdots,n$；

step 2：$S=\{sim_t\},t=1,2,\cdots,n$；

step 3：$LC=Ar^{\text{Backward}}(S)$；

step 4：$RT_{ij}=LC$。

推荐行为信任算法使用云相似度算子及逆向云算子，只需 4 次除法 2 次乘法，计算较为简单，适用于 WSN 节点。

使用 LCT，直接信任、间接信任、推荐行为的信任计算与更新条件与具体安全策略有关。一般情况下，直接信任的计算与更新在与目标节点交互后开始；当节点第一次与目标节点交互，未存储其直接信任时，需要进行信任的推荐，计算间接信任；推荐成功后，与目标节点进行交互，并进行推荐行为信任的评估。

4 仿真实验

基于 LCT 的信任表示方法，既可以实现对入侵识别的敏感度，还可以实现对多种入侵的容忍。通过对 WSN 中场景进行模拟，对多种入侵情况下节点的 3 个信任指标进行计算，并与文献[11]中提出的 CTM 进行了对比分析，验证 LCT 的有效性。

4.1 实验设计

实验使用的无线节点由 SoC zigbee 芯片 CC2530、加速度传感器、PCB 天线、电源电路以及 JTAG 调试接口组成。对实验场景进行定制设计：WSN 中共有 150 个节点，协议使用 802.15.4，节点间平均距离 10 m，节点工作的占空比为 5%。选取实验场景中一个节点 i 与室内新节点 j 以及室外旧节点 k 通信情况进行分析，每小时统计一次数据发送成功率。对 20 次数据发送成功率使用正态分布进行统计，如表 1 所示。

表 1　　节点通信成功率

方向	统计频率	统计次数	平均值	标准差
$i\to j$	1 h	30	0.96	0.01
$i\to k$	1 h	30	0.90	0.03

基于以上实验结果中的数据，设计仿真实验，对信任指标进行分析。仿真环境建立的 PC 机配置为：Intel(R) i5-2450M CPU @ 2.50 GHz，RAM=2 GB，Windows 7 操作系统。所采用的仿真环境为 Matlab2011Rb。以 2 个节点间直接信任数据为基础，模拟推荐数据及攻击数据，在以上环境中进行多种场景下信任指标的仿真，并对结果进行分析。

4.2 多攻击场景入侵容忍及识别

4.2.1 On-Off 攻击容忍及识别

On-Off 攻击首先通过正常的行为积累信任度，之后进行恶意攻击。这种攻击方式利用了信任的评价，是较典型的针对信誉系统的攻击[11]。假设攻击节点 j 与 i 进行交互，前 50 个小时进行正常数据发送，积累信任，之后按照正态分布 N(0.5, 0.16)进行选择性转发，此时信任大大降低。在这组仿真实验中，直接信

任在最近 20 次信任值的基础上进行计算，间接信任在 5 个邻居节点直接信任的基础上进行计算，仿真得到直接信任、间接信任曲线，如图 1 所示。

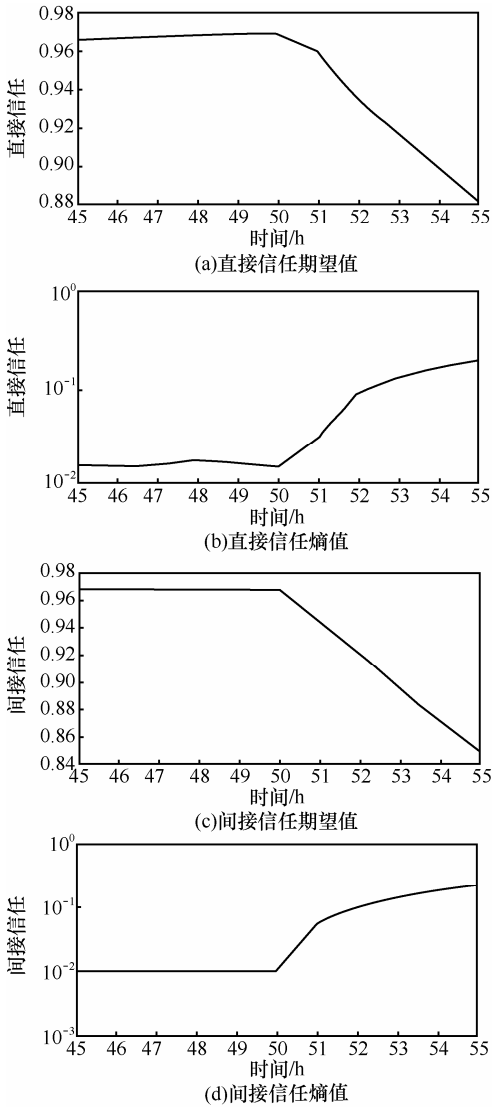

图 1　j 遭遇 On-Off 攻击，T_{ij} 及 ST_{ij} 变化曲线

从图 1 中可以看出，使用 LCT，WSN 遭遇 On-Off 攻击时，信任的期望降低，说明信任整体水平下降；信任的熵增高，说明信任的不确定度变大。间接信任相比直接信任变化更为明显。

为了进一步验证 LCT 在入侵容忍与入侵识别敏感度方面的作用，在相同的场景下，使用 CTM 进行信任评估。采取文献[11]中的参数设置，节点 i、j 共同邻居数为 5 个，直接信任与间接信任的权值 $w1$，$w2$ 分别为定义为 0.8 和 0.2，衰减因子 w 为 0.3，上升幅度 m 为 1，下降幅度 n 为 2，仿真得到信任变化曲线如图 2 所示。

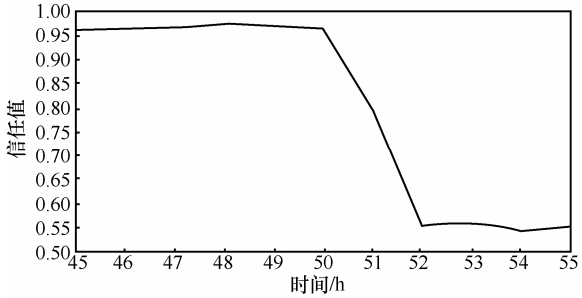

图 2　j 遭遇 On-Off 攻击，CTM 信任值变化曲线

从直观上看，使用 LCT，当 On-Off 攻击出现时，轻量云信任直接信任、间接信任的期望降低均较平缓，能够保证入侵的容忍；而熵数值的增加较剧烈，能够保证入侵行为的敏感识别；而使用 CTM 计算信任值，入侵识别敏感度与入侵容忍能力的平衡由下降幅度 n 决定[11]，无法兼顾二者。使用变化幅度 dv 量化评估信任指标变化的剧烈程度，dv 计算公式为 $dv=(V_{\text{new}}-V_{\text{old}})/V_{\text{old}}$，当 dv 大于 0 时，指标上升，小于 0 时，指标下降，dv 绝对值越大，信任指标变化越剧烈，对入侵的敏感度越高，绝对值越低，信任指标变化越平缓，入侵容忍能力较高。在第 51 个小时，攻击刚刚出现时，LCT 与 CTM 信任指标的变化幅度对比如表 2 所示。

表 2　On-Off 攻击出现时，LCT 与 CTM 信任指标变化幅度对比

LCT 与 CTM	信任指标	数值	变化幅度
LCT	直接信任	期望	−0.009 1
		熵	1.005 3
	间接信任	期望	−0.024 2
		熵	4.479 3
CTM	信任	信任值	−0.173 9

根据表 2，当 On-Off 攻击出现时，LCT 直接信任、间接信任期望降低程度分别为 CTM 降低程度的 1/20、1/7 左右，对入侵的容忍能力较高；而 LCT 直接信任、间接信任熵的增加程度分别为 CTM 降低程度的 6 倍、26 倍左右，识别入侵的敏感度较高。在 LCT 中，直接信任相比间接信任入侵容忍能力较高，而入侵识别的敏感度较低。在第 51 小时，发现节点 j 信任的变化时，若在应用中需要对信任的变化具备一定容忍能力，则可基于信任指标的期望制定应对策略，若需要及时发现入侵，则可基于信任指标的熵制定应对策略。

根据上述实验对比及分析，可知使用 LCT，在 WSN 中出现入侵时，用户易于根据应用的需要，

综合应用 LCT 的信任参数，制定更多的应对策略。

4.2.2 恶嘴攻击容忍及识别

如果 WSN 节点被敌手捕获，内部程序被修改，修改后的节点并不进行直接的恶意攻击，而是在推荐过程中，篡改信任数据，对目标节点进行恶嘴攻击，诋毁其信任。在此情况下，进行信任管理框架下的仿真实验。

假设节点在运行 50 个小时后，遭遇恶嘴攻击，在节点 i 要求对节点 j 进行推荐时，5 个邻居中 k 对 j 发起恶嘴攻击，按照正态分布 N(0.5,0.16)伪造节点 j 信任值，并将伪造的信任值发送给 i。仿真得到间接信任、推荐行为的信任的曲线，如图 3 所示。

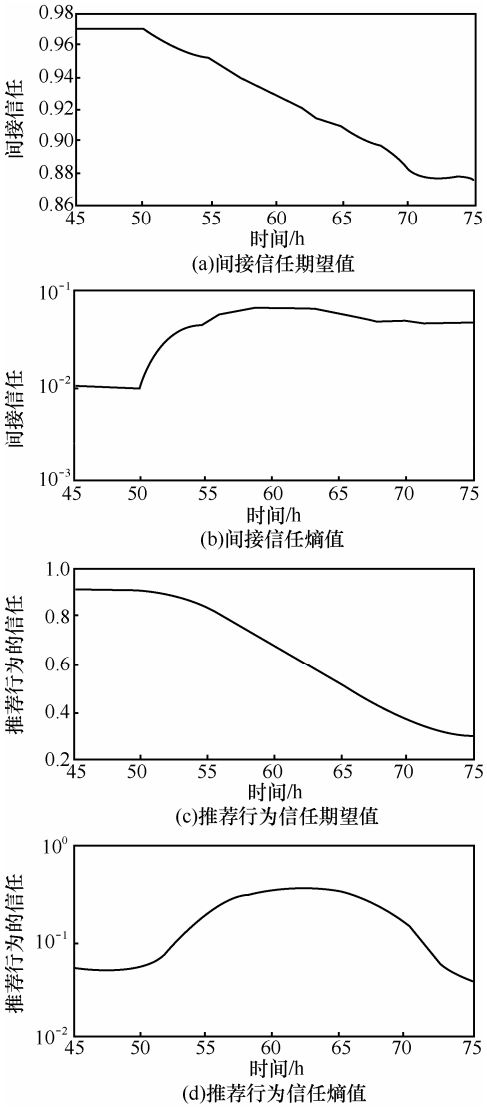

图 3 j 遭遇 k 恶嘴攻击，ST_{ij} 及 RT_{ij} 变化曲线

从图 3 中可以看出，当出现恶嘴攻击时，间接信任的期望降低，然而减低速度较平缓，最终信任值仍与实际信任值较接近，具备对恶嘴攻击的容忍能力；而此时间接信任的熵骤增，用户易于判断，WSN 中可能存在攻击行为；同时，节点 k 推荐行为的信任期望骤降，熵骤增，且期望最终降低为 0.4 以下，用户可判断出节点 j 遭遇节点 k 恶嘴攻击。节点信任指标的变化既保证了对恶嘴入侵的容忍，又敏感地识别了攻击行为。在相同场景下使用 LCT 进行仿真实验，参数设置与上组实验相同。仿真结果如图 4 所示。

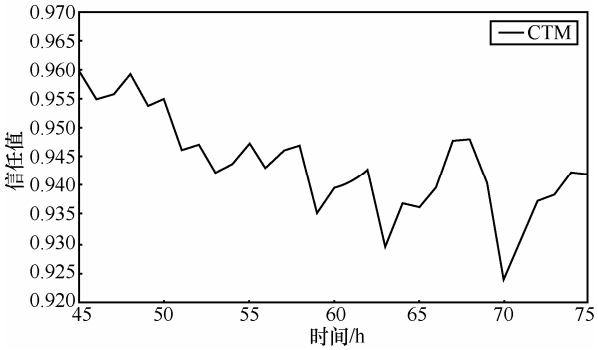

图 4 j 遭遇 k 恶嘴攻击，CTM 信任值变化曲线

根据图 4 可以看出，当出现恶嘴攻击时，CTM 信任值变化较小，最终信任值仍然高于 0.92，对于恶嘴攻击的容忍度较高，然而由于信任值变化的不明显，用户无法发现恶意节点 k，在这种场景下，CTM 对入侵的容忍能力较高，然而入侵识别的敏感度较弱，无法兼顾二者。

4.3 开销分析

由于 WSN 中，节点电能有限，在制定安全策略与算法时，还需要考虑算法的开销，并分析对节点寿命的影响。由于 WSN 中加减法时间复杂度远小于乘除法、开平方复杂度，因此计算开销仅仅比较乘除法及开平方次数。当一个节点平均具有 5 个邻居节点，簇的平均大小为 20，并且每个节点根据最近 10 次信任计算信任云时，统计 LCT 与 CTM 更新平均所需的乘除法以及次数，如表 3 所示。

表 3 LCT 与 CTM 计算开销对比

LCT 与 CTM	信任指标	乘除次数	开方次数
LCT	直接信任	3	0
	间接信任	2	0
	推荐行为信任	6	0
CTM	信任值	14	1

在仿真实验的应用场景中，每个节点第一次交互需要计算间接信任，之后需要建立直接信任云，

并计算推荐行为的信任，第一次交互需要 11 次乘除法计算，之后每次交互只需更新直接信任即可，每次只需 3 次乘除法计算，远小于 CTM 的开销。当用户制定复杂的信任管理策略，发起更多信任计算要求时，计算开销会增大，然而由于 WSN 节点执行每条指令所消耗的电量为发送 1 bit 数据所消耗电量的 1/1 000[14]，一般情况下，使用 LCT 对节点寿命的影响可以忽略不计。

5　结束语

本文根据对 WSN 应用特点及场景的分析，提出了信任管理中入侵容忍能力与入侵识别的敏感度是 2 个重要且存在矛盾的目标，为了克服 2 个目标之间的矛盾，实现既具备容忍能力，又具有入侵识别敏感度的信任管理，设计了基于轻量云模型的信任表示方法。并根据典型的 WSN 应用场景，对此信任表示方法进行了仿真实验，实验结果证明，在 WSN 中出现 On-Off 攻击、恶嘴攻击时，使用该方法，既能保证入侵的容忍，又能实现入侵行为的敏感识别。LCT 算法简单，对 WSN 寿命的影响可以忽略，具有较高的可用性。

下一步的研究工作为：搭建大规模的物理实验网络，在其基础上，使用基于轻量云模型的信任表示方法构建 WSN 的安全与信任网络，并研究基于信任的增强路由协议、数据融合算法等。

参考文献：

[1] PERRIG A, SZEWCZYK R, WEN V, *et al*. SPINS: security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534.

[2] WATRO R, KONG D, CUTI S F, *et al*. TinyPK: securing sensor networks with public key technology[A]. Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks[C]. New York, USA, 2004.59-64.

[3] 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.
JING Q, TANG L Y, CHEN Z. Trust management in wireless sensor networks[J]. Journal of Software, 2008, 19(7):1716-1730.

[4] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[A]. IEEE Conference on Security and Privacy[C]. Oakland, California, USA, 1996.164-173.

[5] GANERIWAL S, BALZANO L K, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks, 2008, 4(3): 15.

[6] 黄海生, 王汝传. 基于隶属云理论的主观信任评估模型研究[J]. 通信学报, 2008, 29(4):13-19.
HUANG H S, WANG R C. Subjective trust evaluation model based on membership cloud theory[J]. Journal on Communications, 2008, 29(4): 13-19.

[7] KRANSNIEWSKI M D, VARADHARAJAN P, RABELER B, *et al*. TIBFIT:trust index based fault tolerance for data faults in sensor network[A]. International Conference on Dependable Systems and Networks[C]. Washington DC, USA, 2005.672-681.

[8] MOMANI M, CHALLA S, ALHMOUZ R. BNWSN: Bayesian network trust model for wireless sensor networks[A]. Mosharaka International Conference on Communications, Computers and Applications[C]. Amman, Jordan, 2008.110-115.

[9] 肖德琴, 冯健昭, 周权等. 基于高斯分布的传感器网络的信誉模型[J]. 通信学报, 2008,29(3):47-53.
XIAO D Q, FENG J Z, ZHOU Q, *et al*. Gauss reputation framework for sensor networks[J]. Journal on Communications, 2008, 29(3): 47-53.

[10] 杨光, 印桂生, 杨武等. 无线传感器网络基于节点行为的信誉评测模型[J]. 通信学报, 2009, 30(12): 18-26.
YANG G, YIN G S, YANG W, *et al*. Reputation model based on behaviors of sensor nodes in WSN[J]. Journal on Communications, 2009, 30(12): 18-26.

[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.
CAI S B, HAN Q L, GAO Z G , *et al*. Research on cloud trust model for malicious node detection in wireless sensor network[J]. Acta Electronica Sinica, 2011, 40(11):2232-2238.

[12] BAO F, CHEN R, CHANG M J, *et al*. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection[J]. IEEE Transactions on Network and Service Management, 2012, 9(2): 169-183.

[13] 李德毅, 杜鹢. 不确定性人工智能[M]. 北京: 国防工业出版社, 2005.
LI D Y, DU Y. Artificial Intelligence with Uncertainty[M]. Beijing: National Defence Industry Press, 2005.

[14] CHENG S, LI J, REN Q, *et al*. Bernoulli sampling based (ε, δ)-approximate aggregation in large-scale sensor networks[A]. Proc of the 29th IEEE INFOCOM[C]. San Diego, CA, USA, 2010.1181-1189.

作者简介：

徐晓斌（1986-），男，河南鹤壁人，北京邮电大学博士生，主要研究方向为物联网安全、无线传感器网络。

张光卫（1970-），男，山东德州人，博士，北京邮电大学讲师，主要研究方向为物联网安全、人工智能、数据挖掘。

王尚广（1982-），男，河南周口人，博士，北京邮电大学讲师，主要研究方向为车联网技术、物联网。

孙其博（1975-），男，河南郑州人，博士，北京邮电大学副教授，主要研究方向为服务计算、物联网和网络安全。

杨放春（1957-），男，北京人，博士，北京邮电大学教授，主要研究方向为智能网络、服务计算和交换技术。