一种基于云模型的 WSNs 节点信誉安全方案

肖云鹏,姚豪豪,刘宴兵
(重庆邮电大学网络与信息安全技术重庆市工程实验室,重庆 400065)

摘 要: 针对已有基于轻量云模型的节点信誉安全方案中存在的决策困难问题以及推荐节点的恶意行为识别问题,提出了优化的轻量云模型 MLCM(Modified Light-weighted Cloud Model),并在此基础上设计实现一种新型的节点信誉安全方案.首先,在传统无线传感网信任管理信任值的处理方式的基础上,对节点的直接信任值和间接信任值进行综合处理后再利用云模型简化逆向云算子进行计算,以解决信任误判问题;其次,用云隶属度函数计算推荐信任值,在涉及推荐节点信任值计算时可以提高恶意节点识别的准确度.实验表明,该方案在克服传统的入侵容忍和敏感度之间矛盾问题的同时,还解决了攻击节点对单一节点发动攻击时造成的决策困难问题和恶意节点准确识别问题.

关键词: 信任值; 无线传感网安全; 信誉安全; 云模型
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2016)01-0168-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.01.025

A WSNs Node Reputation Security Scheme Based on Cloud Model

XIAO Yun-peng, YAO Hao-hao, LIU Yan-bing
(*Chongqing Engineering laboratory of Internet and Information Security, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: Consider the problems of decision-making and recognizing malicious nodes in traditional node reputation security scheme based on light-weighted cloud model, this paper proposes a Modified Light-weighted Cloud Model (MLCM) firstly, and a novel node reputation security scheme is given by then. In order to resolve trust misjudgment, direct and indirect trust values are treated comprehensively before its calculation with simplified backward cloud operator, on the basis of the traditional approach of wireless sensor network trust management on trust value. In addition, cloud membership function is leveraged to obtain recommendation trust value to improve accuracy of recognizing malicious nodes. The experiment shows that the scheme can not only work out the problem of contradiction between the intrusion tolerance and sensitivity but also figure out matter of decision-making and recognizing malicious nodes.

Key words: trust value; wireless sensor network security; reputation security; cloud mode

1 引言

随着无线传感器网络的广泛应用,其安全性显得越来越重要.无线传感器网络工作在一个开放、合作和高度任意的环境中,具有节点间链接脆弱、拓扑结构动态变化、身份认证缺乏、没有集中监控或管理点等特性.网络本身存在许多安全漏洞,引发了多种类型的攻击,直接影响了无线传感器网络的可用性.所以在传感器网络部署应用之前,必须解决好节点间的信誉安全问题,但传感器节点一般都是造价低廉、计算能力较差的结构单元,在判断节点间是否该建立信任链接时,复杂的加密算法不论从计算开销上还是抵抗内部攻击上都不适合应用在这种节点上,因此,信任机制的引入有效地补充了这一不足.

早在 1996 年 Blazer 提出信任管理这个概念后,它就被很多研究者应用到 P2P 和 ad hoc 网络中,这些文献[1~4]中虽然引入了信任机制,建立信任模型,起到了很好的作用,但在这些网络中的许多应用需求和特性并不都适应于 WSNs,因此,人们开始了 WSNs 信任管理的研究[5],Z. Yao[6] 等人提出的分布式信任模型,该模型通过局部节点去评估它们的邻居节点信任值从而做出相应的信任决策,但由于该模型的主要操作是对节点行为进行建模,参数考虑过于单一. S. Ozdemir[7] 等人则提出一种 RDAT 的系统,该系统将基站作为最可信

收稿日期:2015-03-04;修回日期:2015-07-15;责任编辑:蓝红杰
基金项目:国家自然科学基金(No. 61272400);重庆市青年人才项目(No. cstc2013kjrc-qnrc40004);教育部-中国移动研究基金(No. MCM20130351);重庆市研究生研究与创新项目(No. CYS14146);重庆邮电大学文峰基金(No. WF201403);重庆市教委科学计划项目(No. KJ1500425)

实体,并将所有的信任计算和数据融合都交予基站处理,但这种处理的弊端是若遇到针对基站的 Lap-TOP 攻击时,损失将会更大. 而 S. Ganeriwal 等人提出的系统 RFSN(Reputation-based framework for sensor networks)[8] 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,该方法使用贝叶斯函数将直接信息和间接信息结合起来计算信誉值. 然而由于对信誉的表示过于简单,该算法不具备抵御恶嘴攻击的能力. M. Krasniewski 等人提出的 TIBFIT 模型[9],这其实就是一个主要用来检测事件驱动型 WSN 中的 arbitrary 节点故障的容侵模型,并且这种 WSN 的节点是成簇部署的. 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. 杨光、印桂生等人提出了一种 WSN 节点行为评测模型[10] MA&TP BRSN,建立了对第三方节点恶意评价行为的具体测评方法,将节点评价行为与通信行为区分开来,该方法虽然能在一定程度上消除高信誉节点的恶意诽谤行为,可是由于最终仅用一个数字表示信任值,导致诽谤攻击的识别敏感度偏低.

在无线传感器网中,为实现节点的信誉安全,更好地为安全路由和数据融合服务,出现了各种各样的信任管理模型和框架,但这些方法[11~19]没有考虑到信任关系的不确定性和模糊性等特征,这样将会造成信任评估的不准确,这时,云模型的优势就体现出来了,将信任机制和云模型融合起来,实现信任的准确性评估[20,21],虽然蔡绍滨等人将云理论和信任计算有效的结合起来,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[21](CTM),并将之运用到了恶意节点识别中. 但在此模型中,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. 徐晓斌等人就此种情况提出 LCM(轻量云模型)[20],此模型利用逆向运算子对直接信任和间接信任分别计算,并对各自的云特征值进行研究分析,从而克服敏感度和入侵容忍的矛盾问题,但徐等人的算法忽略了恶意节点只针对某一节点进行攻击的情况,结果将会直接导致决策困难.

2　云模型及问题相关定义

2.1　云模型

在传统的模糊数学和概率统计的基础上,李德毅院士提出表述定性定量互换的云模型[22]. 该模型可以用定量的数值表示出某个定性概念的含义,或者用定性的语言描述出定量的数值. Ω 是一个定量的论域,T 一个定性值. 隶属度 $CT(x)$,($CT(x)\in[0,1]$)是一个具有稳定倾向的随机数. 它描述 Ω 中的元素 x 和 T 之间的定性关系. 隶属度在论域上的分布称为隶属云,简称云. 因此,云是从论域 Ω 到区间[0,1]的一个映射,即 $x\in\Omega, x\to CT(x)$ 序对 $(x,CT(x))$ 称为云滴. 云的整体形态是由云的数字特征决定的. 云的数字特征由期望 Ex,熵 En,超熵 He 三个数值来表示,他们反映了定性概念上的定量特征.

由于现实生活中的大多数不确定事件都具备正态分布特性,所以,理论实施时常用到正态云模型的正向云算子和逆向运算子.

定义 1　正向云算子 $For(\mathrm{Ex},\mathrm{En},\mathrm{He})$. 是实现从定性到定量的一种映射,输入云数字特征值 $C(\mathrm{Ex},\mathrm{En},\mathrm{He})$,产生云滴,反应定性概念的一种具体表示.

定义 2　逆向云算子 $Rev(X)$. 输入一组反映具体事件的精确数值,转化为定性的云数字特征值,现有的逆向云算子一种是有确定度的,一种是不需要确定度的.

但实际应用中,定性事件的隶属度并不易获得,所以将云模型应用到 WSN 中时,需要对其进行简化.

2.2　简化云算子相关定义

继承了徐等人的轻量优点,常规云模型一般要有三个参数 $C(\mathrm{Ex},\mathrm{En},\mathrm{He})$,但出于对无线传感器网节点简单,计算能力有限的角度考虑,在无线传感器网中,该方法只采用其中的两个,即 $LC(\mathrm{Ex},\mathrm{En})$ 来表示简化云特征.

定义 3　简化云模型的定性表示 $LC(\mathrm{Ex},\mathrm{En})$. 其中,Ex(expected value)是信任云滴在论域空间分布的期望;En(entropy)表示熵,是对当前信任期望的随机度量,反映了信任云的云滴的离散程度;另一方面又是信任云的模糊性度量,反映了在论域空间可被论域期望接受的云滴的取值范围.

定义 4　简化正向云算子 $LFor(\mathrm{Ex},\mathrm{En})$. 就是将二元定性的云特征值转化为定量的云滴分布,其转化算式如下:

$$X=\{x_i \mid x_i=NORM(\mathrm{Ex},\mathrm{En})\},\quad i=1,2,3,\cdots,N \tag{1}$$

$$Drop=\{(x_i,y_i)\mid x_i\in X, y_i=e^{-\frac{(x_i-\mathrm{Ex})^2}{2E_n^2}}\},\quad i=1,2,3,\cdots,N \tag{2}$$

定义 5　简化逆向运算子 $LRev(X)$. 在实际应用中,能直接得到的往往只有表示某个概念的一组数据值,而代表这个概念的确定度 y 的值并没有给出或者难以获得. 因此,有必要对传统逆向云算法进行改进[23]. 仅仅利用云滴 x_i 的定量数值来还原出云的两个参数,

不需要确定度 y 的值,其转化算式如下:

$$\mathrm{Ex}=\bar{X},X=\{x_i\mid i=1,2,3,\cdots,N\} \tag{3}$$

$$\mathrm{En}=\sqrt{\frac{\pi}{2}}\frac{1}{N}\sum_{i=1}^{N}\mid x_i-\mathrm{Ex}\mid,x_i\in X \tag{4}$$

3 基于 MLCM 模型的节点信誉安全方案

3.1 方案整体框架

目前研究表明,在无线传感器网中遇到的攻击有很多,本文模型就如何识别恶意节点和正确地做出信任决策这两种问题对当前轻量云模型做出对应的算法改进. 本文提出的模型框架如图 1 所示.

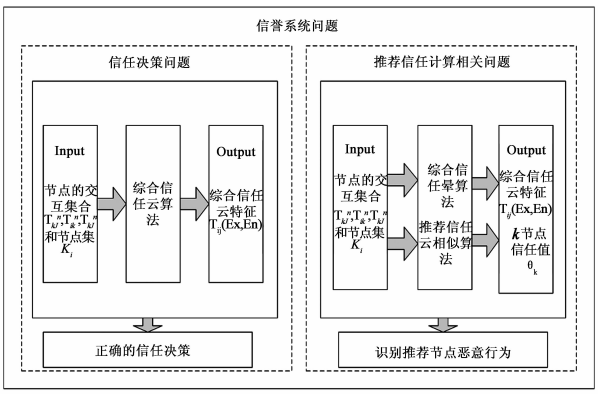

图1 MLCM模型框架

针对信任决策问题的解决来说,首先,从系统中获取节点间的信任集合,然后利用改进后算法即综合信任云算法得出信任云特征值,通过云特征值的变化来实现恶意节点识别并完成信任决策;而对于推荐节点恶意行为的识别来说,节点的抗攻击能力可以通过综合信任云算法实现,而恶意节点的识别则通过推荐信任云算法计算推荐节点的信任值来实现.

3.2 MLCM 模型信任计算相关定义

上节已提到,MLCM 信任计算要用到简化云算子,引入云模型,通过简化逆向运算子进行处理,以下是引入云模型后的信任定义:

定义 6 综合信任 T_{ij}^n. 直接信任(节点间直接交互获得的信任情况)和间接信任(节点通过其他节点获得被观测节点的信任情况)按照一定的权值加和的到的信任状况.

$$T_{ij}^n=\omega t_{ij}^n+(1-\omega)\hat{t}_{ij}^n,n=1,2,3,\cdots,N \tag{5}$$

定义 7 推荐信任 θ_k. 观测节点和中间节点的交互情况与中间节点和被观测节点的交互情况的云相似度,以此定义为推荐节点的信任

$$\ln(y_n)=\frac{-(t_{ik}^n-\mathrm{Ex})^2}{2\mathrm{En}^2} \tag{6}$$

$$\theta_k=\frac{1}{N}\sum_{n=1}^{N}y_n \tag{7}$$

这里,在计算综合信任值时,用到的间接信任值不仅仅是中间节点和被观测节点的交互情况,还要考虑中间节点和观测节点的交互情况,这样做可以提高综合信任值的准确度.

3.3 方案

基于上述 MLCM 模型,本文进而设计实现了一种 WSNs 节点信誉安全方案. 具体包括两个方面:首先是针对决策困难问题提出的信任决策问题解决模型;另一方面是针对恶意推荐节点识别的推荐信任计算模型. 两个解决模型方案共同保证了节点在受到攻击时的入侵容忍和攻击节点的识别,从而保证了无线传感网的系统安全.

3.3.1 信任决策问题解决模型

本文的信任决策问题解决模型首先需要用到直接信任值 t_{ij}^n 和间接信任值 $\hat{t}_{ij}^n$ 进行加权求和计算综合信任值 T_{ij}^n,权值 $0<\omega<1$ 的设定将在算法设计与实验中进行讲解,最后用简化后的逆向运算子将 T_{ij}^n 作为输入计算得出信任期望 Ex 和信任熵值 En,计算公式如下:

$$T_{ij}^n=\omega t_{ij}^n+(1-\omega)\hat{t}_{ij}^n,n=1,2,3,\cdots,N \tag{8}$$

$$T_{ij}(\mathrm{Ex},\mathrm{En})=LRev(T_{ij}^n) \tag{9}$$

直接信任值即节点 i 和 j 的直接交互状况,也就是 $t_{ij}^n=[t_{ij}^1,t_{ij}^2,t_{ij}^3,\cdots.t_{ij}^N]$,而间接信任值 $\hat{t}_{ij}^n$ 的计算要同时考虑 i 和 k,k 和 j 之间的信任状况,即如下所示:

$$\begin{aligned}\hat{t}_{ij}^n=&\frac{1}{m}*[t_{ik_1}^n,t_{ik_2}^n,t_{ik_3}^n,\cdots,t_{ik_m}^n]\\&*[t_{kj}^n,t_{kj}^n,t_{kj}^n,\cdots,t_{kj}^n]^{\mathrm{T}},\\&n=1,2,3,\cdots,N\end{aligned} \tag{10}$$

上式中的 m 为 i 和 j 的中间节点个数,所以最终得出具体的综合信任值和对应的云特征值为:

$$T_{ij}^n=[T_{ij}^1,T_{ij}^2,T_{ij}^3,\cdots,T_{ij}^N]=X \tag{11}$$

$$\mathrm{Ex}=\bar{X},X=\{x_i\mid i=1,2,3,\cdots,N\} \tag{12}$$

$$\mathrm{En}=\sqrt{\frac{\pi}{2}}\frac{1}{N}\sum_{i=1}^{N}\mid x_i-\mathrm{Ex}\mid,x_i\in X \tag{13}$$

该模型中,期望 Ex 用来反映节点的信任值的抗攻击能力,熵值 En 则用来表示节点的识别攻击的敏感度,在解决入侵容忍和敏感度矛盾问题的同时,又解决了节点单一攻击时造成的信任决策困难问题.

3.3.2 推荐信任计算模型

本文提出推荐信任计算模型分为两部分,在表示节点的抗攻击能力时,采用 3.3.1 节的计算模型,在表示节点识别攻击敏感度时,采用云相似度来进行计算,计算公式如下:

第一部分的计算同公式(9),只是在模拟攻击时:

对推荐节点 k 进行模拟

$$T_{ij}(\mathrm{Ex},\mathrm{En}) = LRev(T_{ij}^n) \tag{14}$$

第二部分的计算只需要 i 和 k,k 和 j 的交互集合即可. 首先计算 kj 信任集合的信任云特征:

$$T_{kj}^n(\mathrm{Ex},\mathrm{En}) = LRev(T_{kj}^n) \tag{15}$$

其次利用云确定度方程计算 ik 信任集合在 kj 中的确定度 θ_k

$$\ln(y_n) = \frac{-(t_{ik}^n - \mathrm{Ex})^2}{2\mathrm{En}^2} \tag{16}$$

$$\theta_k = \frac{1}{N}\sum_{n=1}^{N} y_n \tag{17}$$

这样,该模型亦可解决入侵容忍和敏感度之间的矛盾问题,同时,利用云相似度能更精确的反映推荐信任值.

3.4　信任算法设计

本文方法最主要的特点就是将以往对信任的处理方法和云模型结合处理,定义简化逆向云算法为 $LRev(X)$,X 为一集合,其对应的具体算法设计如下:

算法 1　综合信任云算法

input:节点 i 和 j,i 和 k,k 和 j 的交互集合 $T_{ij}^n = \{t_{ij}^1, t_{ij}^2, t_{ij}^3, \cdots. t_{ij}^N\}$,$T_{ik}^n = \{t_{ik}^1, t_{ik}^2, t_{ik}^3, \cdots. t_{ik}^N\}$,$T_{kj}^n = \{t_{kj}^1, t_{kj}^2, t_{kj}^3, \cdots. t_{kj}^N\}$ 和节点集 $\{k_1, k_2, k_3, \cdots. k_m\}$,直接信任值权重 $\omega = 0.8$;

output:综合信任云特征值 $T_{ij}(\mathrm{Ex},\mathrm{En})$;

step1:$\hat{t}_{ij}^n = \frac{1}{m}\sum_{p=1}^{m} t_{ik_p}^n * t_{k_pj}^n, n = 1,2,3,\cdots,N$;

step:$T_{ij}^n = \omega t_{ij}^n + (1-\omega)\hat{t}_{ij}^n, n = 1,2,3,\cdots,N$;

step3:$T_{ij}(\mathrm{Ex},\mathrm{En}) = LRev(T_{ij}^n)$;

从上述算法中涉及到的计算分析,对于综合信任云算法,虽然交互集各有 N 个数量值,但二者的计算是逐一计算,另外,简化后的逆向云算子,只涉及平均值的计算,所以该算法的时间复杂度为 $O(N)$.

算法 2　推荐信任云相似算法

Input:节点 i 和 k,k 和 j 的交互集合 $T_{ik}^n = \{t_{ik}^1, t_{ik}^2, t_{ik}^3, \cdots. t_{ik}^N\}$,$T_{kj}^n = \{t_{kj}^1, t_{kj}^2, t_{kj}^3, \cdots. t_{kj}^N\}$;

output:k 的信任值 θ_k;

step1:$T_{kj}^n(\mathrm{Ex},\mathrm{En}) = LRev(T_{kj}^n)$;

step2:将 T_{ik}^n 中的元素带入到 $T_{kj}^n(\mathrm{Ex},\mathrm{En})$ 的确定度方程 $\ln(y_n) = \frac{-(t_{ik}^n - \mathrm{Ex})^2}{2\mathrm{En}^2}$;

step3:$\theta_k = \frac{1}{N}\sum_{n=1}^{N} y_n$;

同样,对于推荐信任云算法,计算其中一个交互集 T_{kj}^n 的信任特征,利用到简化后的逆向云算子,只有在计算相似度时,需先计算 T_{ik}^n 在 T_{kj}^n 中的隶属度,计算复杂度为 $O(N)$,相似度则通过求隶属度均值得到,所以最终的计算复杂度也为 $O(N)$.

信任值的计算不论采取何种方法,都应该全面考虑,这样得到的信任值的可信度才足够精确,不过,在获取直接信任值时,第一次直接交互可能还未开始,这时的综合信任值就会用间接信任代替,当然,如果节点与节点间没有中间节点或者没有推荐信任的话,综合信任就只能用直接信任来表示,但是,在本文中,为了计算简单和方便介绍,对这些特殊情况不作详细介绍.

4　仿真实验与分析

4.1　实验环境

(1)本实验根据文献[20,21]等情况,首先是采用 Opnet14.5 仿真软件,在 100 * 100 的虚拟场景中布置 200 个节点,模拟运行可获得节点间的交互通信情况,本实验中的局部拓扑情况如图 2 所示.

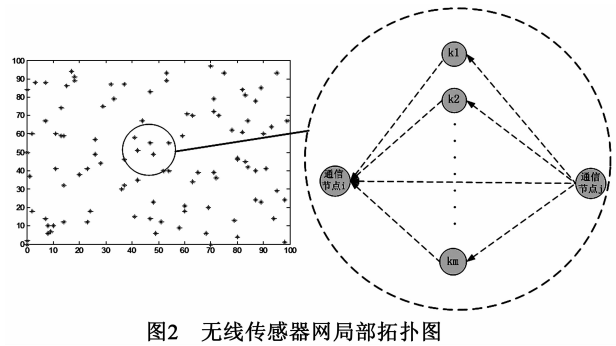

图2　无线传感器网局部拓扑图

(2)其次,在采集节点交互通信情况时,每隔 1 小时采集一次数据,一般在计算信任时,采用最近 30 次的通信成功率进行计算,对数据的处理是采用算法开发工具 Matlab7.0,采用 Windows7 操作系统,在网络正常工作时,数据使用采集到的数据,当模拟攻击时,采用期望为 0.5,方差为 0.16 的正态随机数来模拟攻击数据.

4.2　抗 On-off 攻击实验及分析

前面提到的权值 ω,取不同的值时会对结果造成一定的影响,因为信任机制源自人类社会学,直接信任的权重要远大于间接信任,所以,在开始正式的实验前,针对 j 节点对 i 和 k 同时发动攻击和进行单一攻击两种模式就 ω 究竟设定多大最合适进行实验性的选择,因此,ω 取值从 0.6 开始,分别取 0.8、0.9,其对应的两种模式的实验结果如图 3、图 4 所示.

从图 3 中观察,似乎 ω 越大越好,但从图 4 中可以看到,在超过一定时间后,ω 越大期望下降越快,入侵容

忍能力也越低,所以,综合考虑,令 $\omega=0.8$.

On-off 攻击是比较典型的针对信誉系统的攻击. 其攻击原理为恶意节点首先表现出很好的通信行为来赢得一定的信任值,然后发送错误数据、随意丢弃其它节点的包.

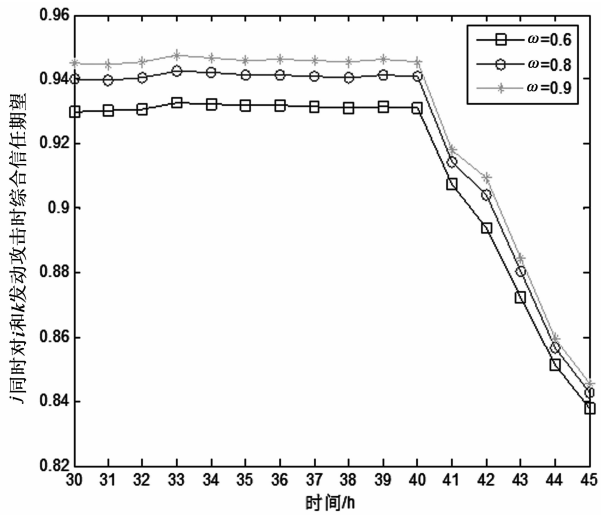

图3 j 节点同时向k和i发动攻击时不同 ω 对应的期望变化

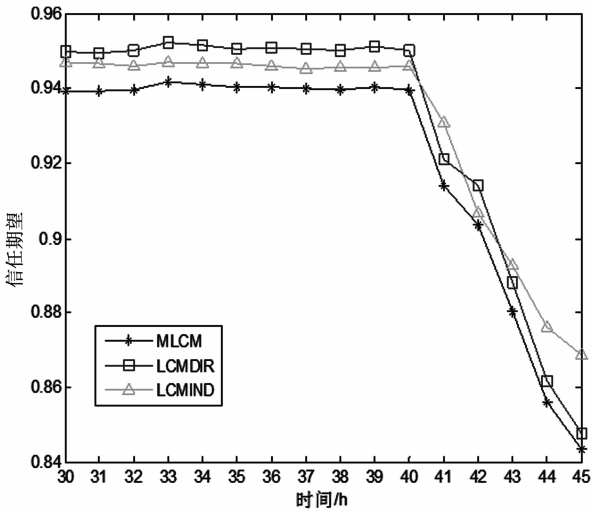

图5 j节点同时向k和i发动On-off攻击时的信任期望值

从图 5 可以很直观的看到,本文算法可以和徐晓斌等人的 LCT 算法一样,在节点受到 On-off 攻击时,信任的期望虽有降低但变化并不大,说明本算法能够表现出良好的入侵容忍能力,从图 6 可以看到,在节点受到攻击时,信任值的熵值发生明显变化,说明系统能够很敏感的意识到攻击的发生,从而及时采取措施,做出适当的信任决策.

上述情况是发生在被观测节点 j 同时向它的邻居节点 k 和 i 都发动攻击的情况下,假如 j 只向 i 或 k 其中一个节点发动了攻击,会产生怎样的决策问题呢,针对这个问题,本文与文献[20]作了以下实验对比:

同样,从图 7、8 可以看出,当 j 节点只向 k 发动攻击时,LCT 算法中的直接信的任期望和熵值都是基本不变的,但间接信任的期望略有降低且熵值会有相对的明显变化,从图 9、10 上可以看到间接信任的期望值和熵值是几乎不变的,但直接信任的期望会有下降且熵值有明显变化,由于熵值是反映期望值波动的一个指标,它的变化与否直接反映了期望的正常与否,所以,从前两幅图的直接信任的图中可以得出节点未遭到攻击的结论,而从间接信任的图中可以得出节点受到攻击的结论,而从后两幅图则得出与之相反的结论,不论上述哪种情况,其直接导致信任管理者决策困难,不过,本论文算法针对这一问题很好地利用了综合信任的优势和云模型的定性定量转换机制,不管 j 节点单

其中,错误数据为上节提到的模拟数据,在第 40 小时后开始发动攻击,为了比较本文方法的优势,实验将与徐等人[20]的实验作对比,仿真对比结果如图 5、图 6 所示.

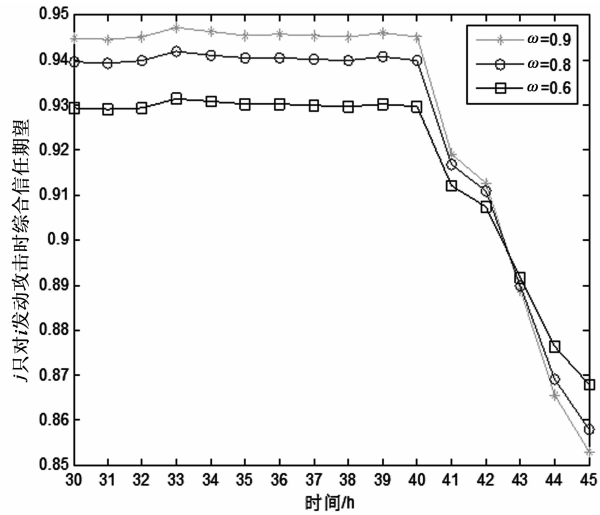

图4 j 节点只对i发动攻击时不同 ω 对应的期望变化

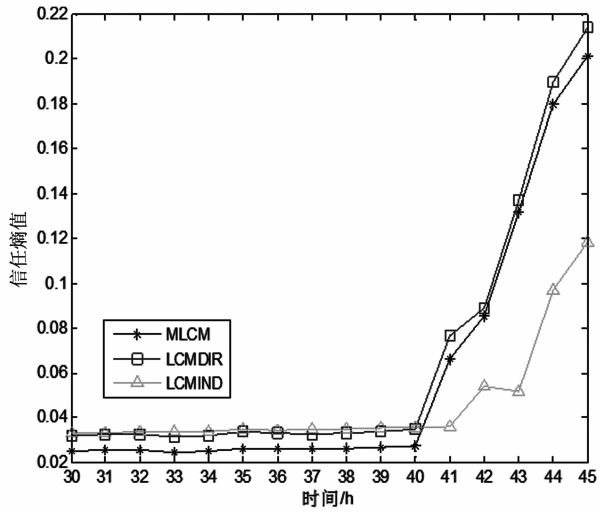

图6 j节点同时向k和i发动On-off攻击时的信任熵值

一的向 k 还是 i 发动攻击,综合信任云算法 MLCM 都能保障系统既有良好的入侵容忍能力,也有很好的攻击识别敏感度,而且绝对不会产生决策困难问题.

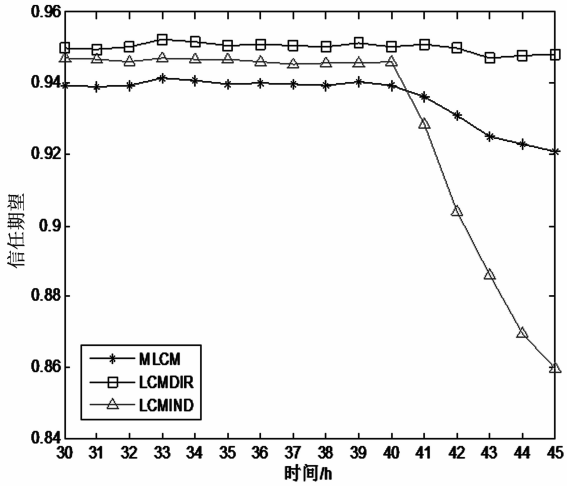

图7　j节点只对k发动on-off攻击时的信任期望值

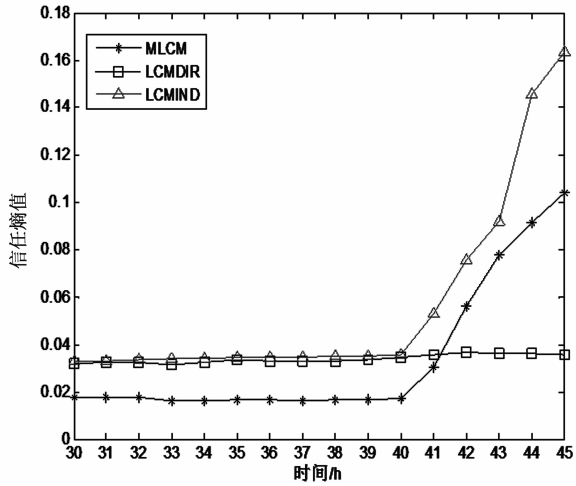

图8　j节点只对k发动on-off攻击时的信任熵值

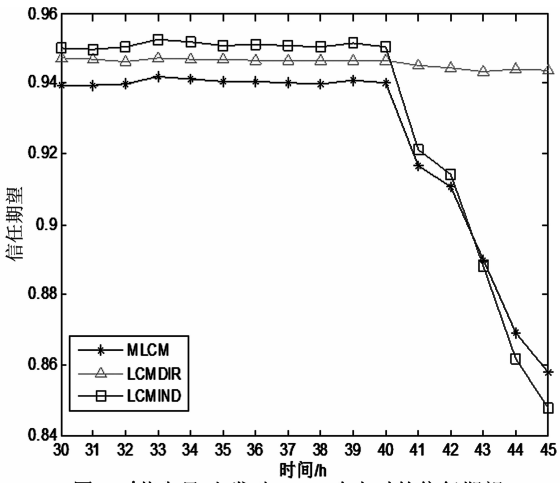

图9　j节点只对i发动on-off攻击时的信任期望

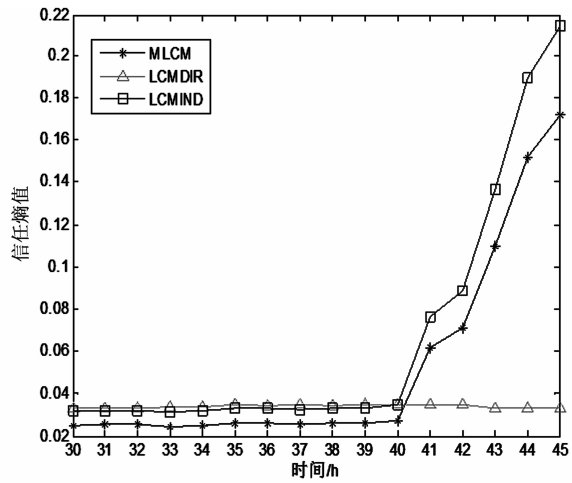

图10　j节点只对i发动on-off攻击时的信任熵值

4.3　抗 bad-mouthing 攻击实验及分析

无线传感器网的节点的程序会被攻击者进行恶意修改,常常被用来发动 bad-mouthing 攻击,这种攻击一般是通过提高恶意节点的信任值或降低正常节点的信任值来实现,也就是说,这种节点不会直接篡改数据包的数据,而是在转发数据时伪造转发的信任信息,达到对被攻击节点的信任进行捏造的事实,由于本文模型解决方案用的是综合信任值处理,不管是提高恶意节点信任还是降低正常节点的信任,得到的综合信任基本是一样的,利用云模型进行处理后得到的特征值的变化也是是一样的,所以在本文中,只对降低正常节点的信任值的情况进行实验.

从图 11 可以观察到在开始发动攻击以及之后的数小时内,信任期望虽有降低,但变化较小,说明本算法很好地防止了恶意节点发动的 bad-mouthing 攻击,保证了节点应该有的良好信誉度,从图 12 中可以看到,k 的信任值有明显下降,所以能够很容易观测到 k 节点是否做出恶意行为,本文在讨论 k 节点的信任值的计算时,选择了比较符合云模型特征的相似度算法进行计算,精确度更高,得出的结论也更贴合实际的节点运行状况.

5　结论

本文就当前无线传感器网中有关信任管理遇到的安全问题进行研究分析,针对信任管理中信任值的处理方式对信任判定的影响,在 LCM 的基础上进行算法改进提出了基于 MLCM 的节点信誉安全方案. 对攻击中的 On-off 攻击场景和 Bad-mouthing 攻击场景进行了仿真实验和分析对比表明,对信任值进行综合处理并结合云模型能够很好地解决 On-off 攻击中的单一攻击造成的决策困难问题,利用云相似度来计算推荐节点

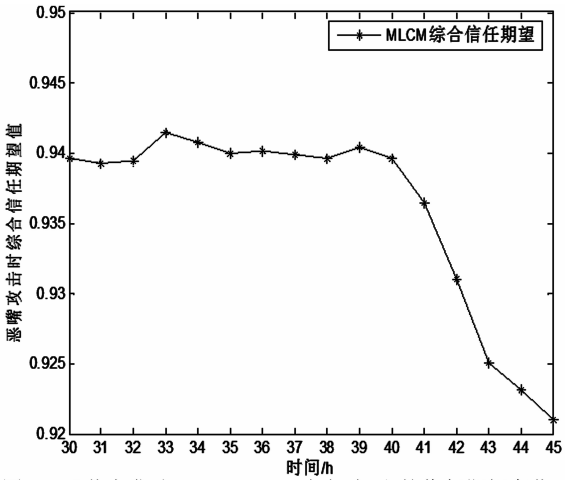

图11 k节点发动bad-mouthing攻击时i对j的信任期望变化

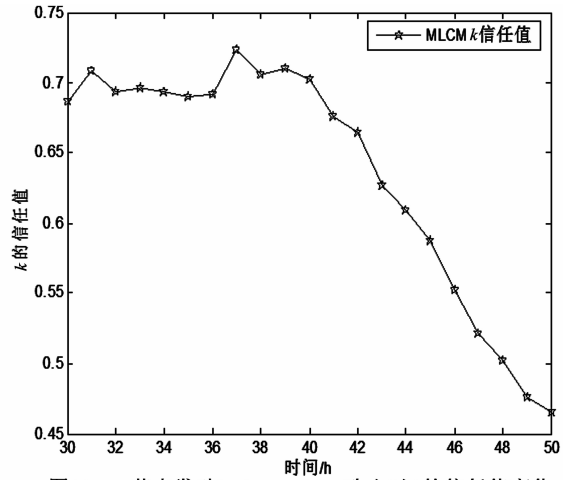

图12 k节点发动bad-mouthing攻击时k的信任值变化

的信任值也有效地提高了 Bad-mouthing 攻击中恶意节点的识别精度,增强了 WSNs 的安全性和鲁棒性. 能耗是关乎无线传感器网寿命的重要指标,下一步的研究工作是根据节点历史能量值进行能量预测,以便准确选择合适的节点作为下跳节点.

参考文献

[1] Chen R, Guo J, Bao F, et al. Trust management in mobile ad hoc networks for bias minimization and application performance maximization[J]. Ad Hoc Networks, 2014, 19: 59 – 74.

[2] 吴旭. 基于增强稳定组模型的移动 P2P 网络信任评估方法[J]. 计算机学报, 2014, 37(10): 2118 – 2127.
Wu X. Enhanced stable group model-based trust evaluation scheme for mobile P2P networks[J]. Chinese Journal of Computers, 2014, 37(10): 2118 – 2127. (in Chinese)

[3] 李致远, 王汝传. 一种移动 P2P 网络环境下的动态安全信任模型[J]. 电子学报, 2012, 40(1): 1 – 7.
Li Z Y, Wang R C. A dynamic secure trust model for mobile P2P networks[J]. Acta Electronica Sinica, 2012, 40(1): 1 – 7. (in Chinese)

[4] 陆峰, 郑康锋. 构建风险敏感的对等网安全信任模型[J]. 北京邮电大学学报 2010, 33(1): 33 – 37.
Lu F, Zheng K F, et al. Construct a risk-aware peer-to-peer security trust model[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(1): 33 – 37. (in Chinese)

[5] 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. (in Chinese)

[6] Z Yao, D Kim, et al. A security framework with trust management for sensor networks[A]. Workshop of the First International Conference on Security and Privacy for Emerging Areas in Communication Networks[C]. San Francisco: IEEE, 2005. 190 – 198.

[7] Ozdemir S. Functional reputation based reliable data aggregation and transmission for wireless sensor networks[J]. Computer & Communications 2008, 31 (17): 3941 – 3953.

[8] S Ganeriwal, L Balzano, K Srivastava, B Mani. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks 2004, 4(3): 1 – 37.

[9] Krasniewski M, Varadharajan P, Rabeler B, et al. TIBFIT: Trust index based fault tolerance for arbitrary data faults in sensor networks[A]. Dependable Systems and Networks, 2005. DSN 2005. Proceedings International Conference on IEEE[C]. San Francisco: IEEE, 2005. 672 – 681.

[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. (in Chinese)

[11] Altisen K, Devismes S, Jamet R, et al. SR3: secure resilient reputation-based routing[A]. Distributed Computing in Sensor Systems (DCOSS)[C]. San Francisco: IEEE, 2013. 258 – 265.

[12] Bai Y, Wu N, Sun B. Secureroute selection based on trust value for distributed networks[A]. Wireless Communications, Networking and Mobile Computing[C]. San Francisco: IEEE, 2008. 1 – 4.

[13] Ping D, Jianfeng G, Xiaoping X, et al. Attack-resistant trust management model based on beta function for distributed routing in internet of things[J]. China Communications, 2012, 9(4): 89 – 98.

[14] Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago. Trust management systems for wireless sensor networks: Best practices[J]. Computer Communications, 2010, 33: 1086 – 1093.

[15] Karthik N, Dhulipala V R S. Trust calculation in wireless sensor networks[A]. Electronics Computer Technology (ICECT)[C]. San Francisco: IEEE, 2011. 4: 376 – 380.

[16] Lu Y, Lin K, Li K. Trust evaluation model against insider attack in wireless sensor networks[A]. Cloud and Green Computing (CGC)[C]. San Francisco: IEEE, 2012. 319 – 326.

[17] Boukerche A, Li X. An agent-based trust and reputation management scheme for wireless sensor networks[A]. Global Telecommunications Conference[C]. San Francisco: IEEE, 2005. 3 – 5.

[18] Kim T K, Seo H S. A trust model using fuzzy logic in wireless sensor network[J]. World academy of science, engineering and technology, 2008, 42: 63 – 66.

[19] Ukil A. Trust and reputation based collaborating computing in wireless sensor networks[A]. Computational Intelligence, Modeling and Simulation (CIMSiM)[C]. San Francisco: IEEE, 2010. 464 – 469.

[20] 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.
Xu X B, Zhang G W, Wang S G et al. Representation for uncertainty trust of WSN based on lightweight-cloud[J]. Journal on Communications. 2014, 35(2): 63 – 69. (in Chinese)

[21] 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 mode1 for malicious node detection in wireless sensor network[J]. Acta Elec-tronica Sinica, 2012. 40(11): 2232 – 2238. (in Chinese)

[22] 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. (in Chinese)

[23] 刘常昱,冯芒,戴晓军,李德毅. 基于云 X 信息的逆向云新算法[J]. 系统仿真学报,2004,16(11):2417 – 2420.
Liu C Y, Feng M, Dai X J, Li D Y. A new algorithm of backward cloud[J]. Journal of System Simulation, 2004, 16(11): 2417 – 2420. (in Chinese)

作者简介

肖云鹏　男,1979 年生,重庆邮电大学副教授,硕士生导师,主要研究方向为大数据,移动互联网,信息安全.
E-mail: xiaoyp@ cqupt. edu. cn

姚豪豪　男,1989 年生,重庆邮电大学硕士研究生,主要研究方向为无线传感网安全.

刘宴兵　男,1971 年生,重庆邮电大学教授,博士生导师,主要研究方向为网络分析和网络安全.