基于关联度分析的WSN节点信任模型研究

张乐君，邓 鑫，国 林，张健沛，杨 静，李泓波

(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

【摘要】该文基于社会网络关联度分析的无线传感网络节点信任模型进行研究。给出了无线传感器网络的模型并将其与社会网络模型进行了相似性分析；建立了基于社会网络关联度的WSN节点信任模型，提出了基于关联度的传感器节点信誉度的计算方法；并设计了基于滑动窗口的传感器节点信任值计算及更新算法(SNTUA)。通过仿真实验，证明了该算法的有效性和准确性，其性能优越于其他两种算法。

关 键 词 关联度分析； 社会网络； 信任模型； 无线传感器网络
中图分类号 TP393 文献标志码 A doi:10.3969/j.issn.1001-0548.2015.01.018

Research on Trust Model Based on Social Network Correlation Degree Analysis in Wireless Sensor Networks

ZHANG Le-jun, DENG Xin, GUO Lin, ZHANG Jian-pei, YANG Jing, and LI Hong-bo

(College of Computer Science and Technology, Harbin Engineering University Harbin 150001)

Abstract Based on the similarity comparison of WSN model and social network model, this paper proposes a trust model based on social network correlation degree in wireless sensor networks (WSN). The computing method of WSN node credit with network correlation degree is built. The sensor node trust update algorithm (SNTUA) is designed based on sliding windows. Simulation experiments prove that SNTUA is better than other two algorithms and the correctness and effectiveness of SNTUA is testified.

Key words relational degree analysis; social network; trust model; wireless sensor network

无线传感器网络(简称WSN)是由大量传感器节点以自组织方式构成的无线网络，已广泛应用于军事和民事等领域[1]。WSN的开放性以及资源受限等特点使得对其进行攻击的形式更加复杂和多样化。它所面临的威胁不仅仅是外部攻击者所发起的攻击, 内部节点也极有可能被俘获从而发起内部攻击。此外，节点出于节省自身能源的目的也会产生一系列特定的自私行为。因此，如何评价合法的WSN节点、识别并剔除行为不端的节点是无线传感器网络亟待解决的重要安全问题之一。

近年来，网络的可信[2]研究已成为一个研究热点。网络可信技术是在原有网络安全技术的基础上增加行为可信的安全新思想，强化对网络状态的动态处理，为实施智能自适应的网络安全和服务质量控制提供策略基础。传感器节点的信任模型通常应用于路由选择、数据认证等方面，因此信任模型将直接影响WSN网络的工作效率。

本文借鉴社会网络中关联度分析的思想，将其应用于无线传感器网络的信任模型中，提出一种基于社会网络关联度分析的无线传感器网络信任模型。

1 WSN信任模型研究现状

WSN信任模型的相关研究起源于对人类社会学的研究，之后被逐渐引入到电子商务、无线局域网等其他领域中。近年来又引起无线传感器网络领域研究学者的关注，并已经研究和设计了一些无线传感器网络节点的信任评价模型。

文献[3]提出的Confident协议是一种WSN节点信誉评测机制。通过对邻居节点监测的同时，计算信誉值，并将计算结果与预设置阈值比较，判断节点的可信度。文献[4]提出了Core协议，该协议在计算节点自身观测得到的直接信誉值的同时，还将其他节点推荐的间接信誉值考虑进来协同计算节点的

收稿日期：2013 – 02 – 10； 修回日期：2014 – 11 – 13
基金项目：国家自然科学基金(61073043, 61073041, 61100008)；黑龙江省自然科学基金(F200901, F201023)；高等学校博士学科点专项科研基金(20112304110011)；中央高校基本科研业务费专项资金(HEUCF061002)
作者简介：张乐君(1979 –)，男，博士，副教授，主要从事网络安全、传感器网络、系统生存性等方面的研究.

信誉值。文献[5]考虑到资源受限情况，设计了信誉评测模型BRSN。BRSN利用贝叶斯公式对信誉分布于Beta分布进行拟合，并通过对计算Beta分布的期望值的方法得到节点的信任值。文献[6]根据节点直接和间接的经验建立信誉值的置信区间，同时，考虑了转发数据的通信因素和感知数据的数据因素。不足之处在于各传感器节点需要较大的缓存器，并需要安装位置感知系统。

国内的研究学者也进行了相关研究，如文献[7]提出了用于安全数据融合的信任模型，该模型综合考虑了数据一致性和能量因素，能较全面地评价节点的信任值，不足之处在于该模型并没有考虑通信因素。文献[8]提出了一种无线传感器网络节点信誉的故障检测算法，为每个传感器节点建立信誉函数，定期更新和维护信誉值，并据此判断节点故障和敏感事件。

尽管无线传感器网络的信任模型取得了一定的进展，但仍存有不少需要改进和完善之处，如对传感器节点信誉的恶意推荐和诋毁等，基于社会网络分析的无线传感器网络的节点信任模型的研究并不多见。为此，本文分析了社会网络和无线传感器网络的一些相似性行为关系，并在WSN中引入社会网络的关联度概念，通过“社会网络关联度”修正和综合利用节点以及其邻近节点的信誉度评价值，并通过仿真实验验证了本文所提方法的有效性，提高了对恶意诽谤行为的检测率，降低其对传感器网络的影响，并为传感器节点的成功通信提供了保障。

2　WSN模型及其与社会网络模型的相似性分析

2.1　WSN模型

无线传感器网络系统通常包括传感器节点(sensor node)、汇聚节点(sink node)和管理节点。传感器节点被部署在监测区域内部或附近。传感器节点的监测数据沿着其他传感器节点的路径逐跳进行传输，在传输过程中监测数据可能被多个节点处理和分析，并最终路由到汇聚节点。用户通过管理节点实现对传感器网络的配置和管理，发布监测任务以及收集监测数据。典型的WSN结构如图1所示。

传感节点定义为 $s=\{s_1,s_2,\cdots,s_n\}$，汇聚节点定义为 $g=\{g_1,g_2,\cdots,g_m\}$，为了减少部署成本，m 远远小于 n。管理节点和汇聚节点一般为有源的，因此不受能量的限制。传感节点具有同样的初始能量，具有同样的存储、计算和通信的能力。受传感器节点通信范围的影响，传感节点通常与其最新的汇聚节点进行通信。如果其中的传感器节点无法直接与最近的汇聚节点通信，那么它就会选择一条路由，通过其他节点的转发将数据最终传输到汇聚节点，如下图2所示。

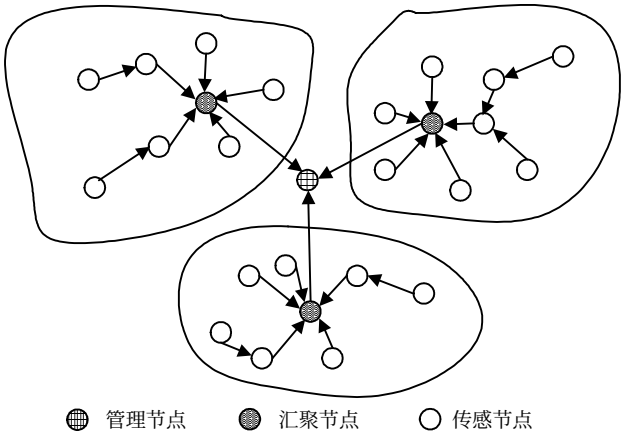

图1　无线传感器网络体系结构示意图

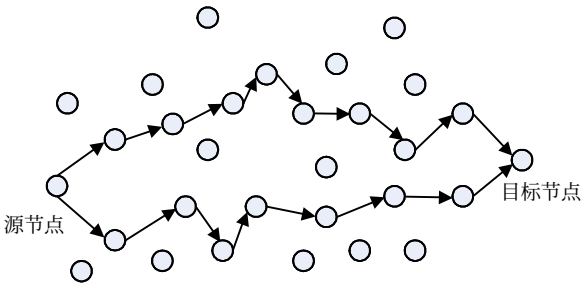

图2　节点通过多跳与汇聚节点通信示意图

2.2　WSN与社会网络的相似性分析

在社会网络中，信任关系是人际关系中的核心内容，在传感器网络中，节点之间的信任关系也是影响传感器网络性能的关键因素。下面说明社会网络和WSN之间的相似性。

2.2.1　WSN和社会网络对比关系

表1　社会网络和WSN对比关系

内容	社会网络	无线传感器网络
实体	个人	节点
实体属性	个人属性，包括：性别、年龄等	传感器节点类型、电池类型、分簇号、传送数据类型等
实体覆盖范围	个人的生活区域	节点通信范围
信誉	其他人的尊重	其他节点的估计
信任	其他人对其的信任程度	信任等级

社会网络分析主要研究社会网络，理解社会的结构，社会节点的行为和节点之间的关系。社会网络和传感器网络有很多相似之处：1) 网络中节点具有自主性；2) 节点间进行信息交互；3) 通过搜索和分析交互信息，建立信任关系；4)采用推荐的方式

传播信任关系；5) 单节点失效并不影响网络的整体性能等。社会网络和WSN元素之间的对应关系如表1所示。

2.2.2 社会网络中的节点关联度

人类社会网络是由人的个体组成，社会网络通常可以用图来表示。图中个人是节点，人与人之间的关系用连接表示，在人类社会网络中，人们通常更加愿意将自己的隐私信息告诉与他关系紧密的人，而对不熟悉的人则通常会隐藏这些信息。节点的关系是人类社会网络的一个显著特点，两个关系紧密的人互相之间会分享更多的信息。

人类中两个个体存在直接关系(父亲和孩子，如图3中节点*A*和*B*)，那么他们的分离度为1，如果两个个体之间需要 n 个中间人才能建立起连接的话，那么其分离度为 $n+1$。这种关系在人类网络中是动态变化的，由于个人在社会网络中不断的沟通，因此其可能获得了更多的使其关系更加紧密的信息，如：居住在同一个社区，对同一个话题感兴趣等等(如图中节点*A*和*C*)。通常来说，两个个体之间信息交换的越频繁，那么节点的关联度就越大，其推荐信任度的可信度也越大。如：在图中个体*B*可将其同学*C*推荐给个体*A*，个体*A*对推荐的相信程度取决于其与节点*B*的关联度，关联度越高那么越可信。

综上，社会节点的关联度具有如下几个原则：

1) 节点的关联度和两个个体之间的分离度成反比；2) 两个个体之间获得彼此的信息越多，他们的关联度就越大；3) 两个个体之间的关联度会随时间逐渐变化；4) 如果两个个体之间交流变少，他们的关联度就会减少；5) 信任关系通过节点关联度传递，关联度越近的个体所推荐的信任度越可信。

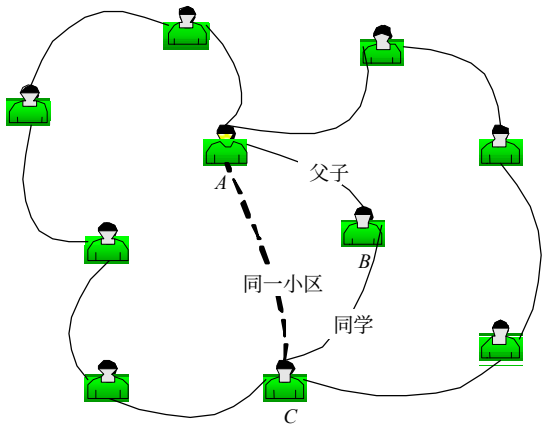

图3 社会网络中关联度及信任传递示意图

2.2.3 WSN网络中的节点关联度

WSN网络中传感器节点也具有相似的节点关联度，在人类社会中，每个实体具有多重属性，如：年龄、性别、民族等；WSN中每一个传感器节点也包括多重属性，如：传感器类型、电池类型、传送数据类型等。在WSN中也存在着和人类网络中类似的关联度，其遵循如下原则：

1) 节点的关联度与两个传感器节点中数据交换经过的跳数成反比；2) 每一个传感器节点保留一张表，表中其他节点的属性信息与它们之间数据通信经过的跳数成反比，即越远的节点其知道的信息就越少；3) 表中存储的信息越多，那么它们数据交换的概率就越大，如果它们通信次数增加，那么它们知道对方的信息就越多，它们的关联度就越大；4) 节点的信任度可通过推荐方式传播。

3 基于社会网络关联度分析的WSN节点信任模型

3.1 信任模型相关定义

网络中恶意节点通常会对网络发动各种攻击。而正常节点由于能量策略、优先级设置等原因，偶尔会发生丢包、不转发包等类似恶意通信行为。本文将这些统称为不良通信行为。

定义 1 不良通信行为：在WSN中，节点违反所在网络的协议规范进行的通信行为称为不良通信行为。

所谓信任模型[9]，是指通过传感器节点本身及与其他节点交互的历史来建立量化的评价体系，以信任值度量节点的可信程度。本质上是节点的实际物理属性和其行为的一个综合能力的反映。

定义 2 节点信誉为一个传感器节点对另一个传感器节点的评价，被视为一种概率分布。

信誉分为直接信誉和间接信誉两种，直接信誉来自于节点 s_i 对 s_j 的直接评价，间接信誉是 i 得到的所有第三方节点 k 对 j 的间接综合评价信息。如直接信誉和间接信誉分别用 $R_{\mathrm{D}}(s_i,s_j)$ 和 $R_{\mathrm{ID}}(s_i,s_j)$ 表示，节点的信誉由两者加权求和计算而得，为：

$$R(s_i,s_j)=\alpha R_{\mathrm{D}}(s_i,s_j)+(1-\alpha)R_{\mathrm{ID}}(s_i,s_j) \quad (1)$$

式中，α 为信任因子，α 越高说明它对自己的判断越相信。

定义 3 信任 $T(s_i,s_j)$ 是传感器节点 s_i 对传感器节点 s_j 将要发生行为的期望值，即计算两个节点之间信誉概率分布的统计期望。$T(s_i,s_j)$ 表示节点 s_i 对节点 s_j 的信任，表示为：

$$T(s_i,s_j)=E(R(s_i,s_j)) \quad (2)$$

传感器节点的关联度表示两个节点之间的相似性，当两个传感器节点进行数据通信时经过的路由

节点(跳数)越多，它们通信的概率越小，同时期获取对方节点的信息就越少，关联度就越小。

定义 4　节点关联度表示节点关联关系的紧密程度，两个节点的相似属性越多其关联度越大。其计算公式为：

$$\delta(s_i,s_j)=\frac{|A(s_i,s_i)\bigcap A(s_i,s_j)|}{\mathrm{Max}(|A(s_i,s_i)|,|A(s_i,s_j)|)} \tag{3}$$

式中，$A(s_i,s_j)$ 表示节点 s_i 中保存的节点 s_j 的属性集合。

3.2　基于关联度的传感器节点信誉参数计算模型

信任模型包括的两个重要参数是直接信誉参数和间接信誉参数。

直接信誉 $R_{\mathrm{D}}(s_i,s_j)$ 是指节点 s_i 在一段时间内直接观察节点 s_j 所得的信誉参数，表示节点 s_i 对节点 s_j 在通信过程行为的评价，其计算公式为：

$$R_{\mathrm{D}}(s_i,s_j)=\frac{\beta}{\beta+\chi}\times\delta(s_i,s_j)=\frac{\beta}{\beta+\chi}\times\frac{|A(s_i,s_i)\bigcap A(s_i,s_j)|}{\mathrm{Max}(|A(s_i,s_i)|,|A(s_i,s_j)|)} \tag{4}$$

式中，β 代表正常通信的次数；χ 代表不良通信行为的次数；$\delta(s_i,s_j)$ δ_{ij} 代表节点 s_i 和 s_j 的关联度。

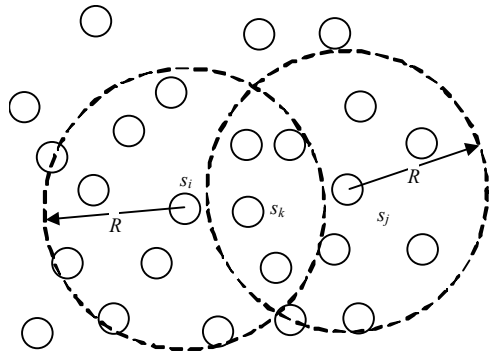

图4　间接信誉度计算中节点邻域示意图

图4为间接信誉度计算中节点邻域示意图，节点 s_i 在计算完节点 s_j 的直接信誉参数 $R_{\mathrm{D}}(s_i,s_j)$ 后，会将这个参数广播给其所有邻居节点的集合 $N(s_i)$。如果节点 s_k 在节点 s_i 的邻居集合 $N(s_i)$ 中，且 s_j 处于集合 $N(s_k)$。节点 s_i 将会收到节点 s_k 发送的节点 s_j 的信誉参数 $R_{\mathrm{D}}(s_k,s_j)$，节点 s_i 通过计算和汇总这些参数得到间接信誉参数 $R_{\mathrm{ID}}(s_i,s_j)$，如果两个节点之间的关联度越高，那么它传递过来的信誉评价就越可信，有：

$$R_{\mathrm{ID}}(s_i,s_j)=\frac{\sum_{s_k\in N(s_i)\bigcap N(s_j)}\delta(s_k,s_j)R_{\mathrm{D}}(s_k,s_j)}{|\{s_k\,|\,s_k\in N(s_i)\bigcap N(s_j)\}|} \tag{5}$$

信誉整合过程中，将式(1)、式(4)和式(5)进行合并，得到综合信任评价为：

$$R(s_i,s_j)=\frac{\alpha\beta}{\beta+\chi}\times\frac{|A(s_i,s_i)\bigcap A(s_i,s_j)|}{\mathrm{Max}(|A(s_i,s_i)|,|A(s_i,s_j)|)}+\frac{(1-\alpha)\times\sum_{s_k\in N(s_i)\bigcap N(s_j)}\delta(s_k,s_j)R_{\mathrm{D}}(s_k,s_j)}{|\{s_k\,|\,s_k\in N(s_i)\bigcap N(s_j)\}|} \tag{6}$$

3.3　传感器节点信任值计算及更新算法

为了节约并充分利用传感器节点的存储资源，本文采用滑动窗口模型实现对传感器节点信任值的计算和更新，如图5所示。在每个传感器节点 s_i 上均保留一个滑动窗口，其中记录当前节点所获得的其他传感器节点的属性信息。每进行一次正常通信，节点 s_i 将从目标节点中获得一个属性数据，滑动窗口的空间大小 p 由传感器网络规模、节点分布密度和传感器节点的属性数量相关，窗口中保存最近 p 次通信所获得的其他节点信息。

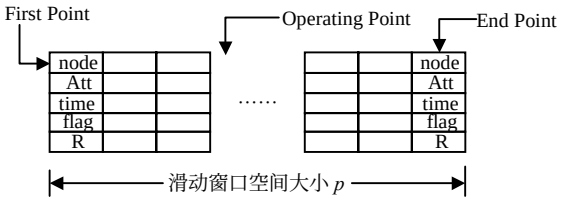

图5　WSN节点信任度计算滑动窗口模型

每次通信传感器节点都将在滑动窗口中添加一条存储记录，node中存储当前通信的目标节点，flag记录通信状态(通信是正常还是不良)，通信的时间time，以及通信过程所获得的目标节点的属性数据，并将其存储在Att中，以便后续的信任值得的计算，R 表示在time时，节点 s_i 对 s_j 的信任评价。传感器节点信任值计算和更新算法(sensor node trust update algorithm，SNTUA)正是基于这个滑动窗口的，SNTUA算法描述如下：

输入：WSN节点信任度计算滑动窗口(windows(s_i))

输出：节点 s_i 对 s_j 的信任评价

1) Initialize all the variable;
2) Receive the $\delta(s_t,s_j)$ and $R_{\mathrm{D}}(s_t,s_j)$ of s_j from s_i neighbor
3) Calculate $R_{\mathrm{ID}}(s_i,s_j)$ using formula (5);
4) For (i = 0 ; i<p; i++)　{
5)　　if (windows[i].node = = s_j) {
6)　　　　n++;
7)　　　　R = R + windows[i].R

8) if (flage = = ‘ture’) β ++；

9) else χ ++;

10) if (windows[i].Attr = = s_j .Attr) SimAttr++；

11) }//end if

12) }//end for

13) Calculate $\delta(s_i, s_j)$ using formula (3) and $R_{\mathrm{D}}(s_i, s_j)$ using formula (4);

14) Calculate $R(s_i, s_j)$ using formula (1);

15) $R = R + R(s_i, s_j)$;

16) $T(s_i, s_j) = R/(n+1)$;

17) Return($T(s_i, s_j)$);

SNTUA算法中通过遍历滑动窗口获得节点 s_i 近期通信的所有信息，并通过步骤5)～步骤10)将这些信息搜索和统计出来, 通过步骤13)～步骤16)步计算出所需要的信任值 $T(s_i, s_j)$。分析SNTUA算法可知，本算法仅需要遍历滑动窗口一次，因此其时间复杂度为 $O(p)$。

4 仿真实验与分析

本文实验使用C语言实现算法, 在实验环境中设置200个传感器节点，随机分布在 $10R \times 10R$ 的正方形区域内，每个节点具有10个属性，为了简化实验过程，每个节点的这些属性是相同的。节点信誉交换的时间周期为100 ms，通信时间间隔为20 ms，初始信任值设定为0.5，每个节点的滑动窗口大小p设置为30。

实验中设定了4类节点：1) 正常节点，其始终按照正常通信行为进行工作，占总数的70%；2) 恶意节点：其始终具有不良通信行为，占10%；3) 伪善节点[10]，网络行为前期分表现良好，后期表现恶劣，占10%；4) 恶意推荐节点，其网络行为表现良好，后期不参与正常数据通信，广播诋毁其他节点信息，占10%。

实验内容有：

1) 各种类型传感器节点的信任值计算。

图6显示了4种传感器节点在1 s之内(每个节点50次数据通信)后信任值的变化情况。

如图6所示, 正常节点的通信行为表现一直处于良好状态，其节点的信任值随着通信次数的增加逐渐提高；相反，恶意节点的信任值随着通信周期的的增加快速减少；伪善节点在通信前期表现良好，后期信任值急剧下降，因此可以快速识别出恶意节点；恶意推荐节点从300 ms时开始不参与通信，其信任值跟着降低，其原因是该节点的属性信息在其他节点中滑动窗口中迅速减少所致。这些情况符合对节点信任度建立缓慢、毁坏迅速的要求。

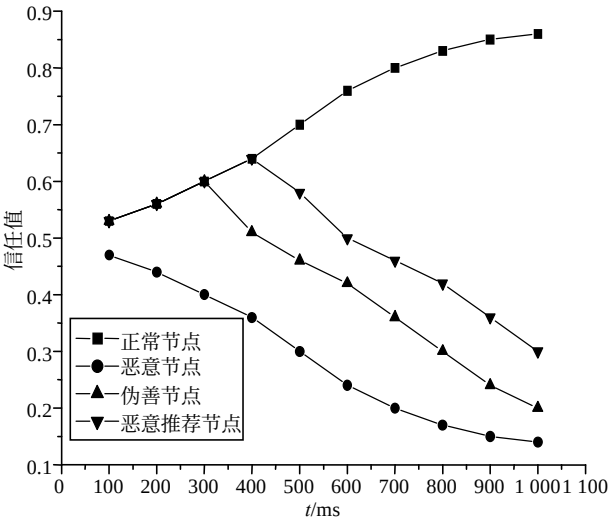

图6 多种类型传感器节点的信任值计算结果图

2) 恶意推荐节点对善意节点的影响。

图7中体现了恶意推荐节点对正常节点信任值的影响，并与BRSN[5]和TP-BRSN[8]算法进行了比较。

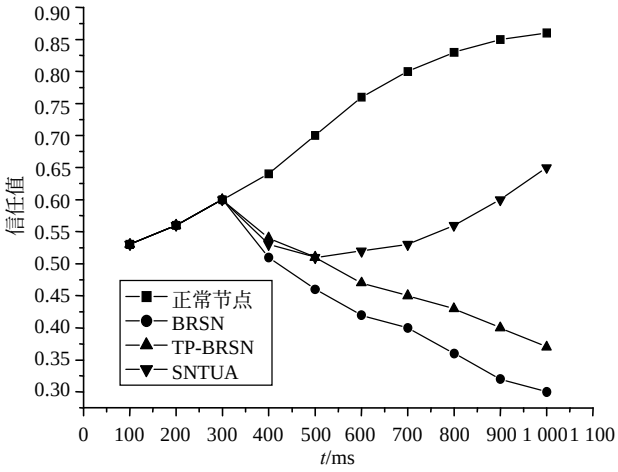

图7 恶意推荐节点对善意节点的影响结果图

图7显示了BRSN对第三方节点的恶意诋毁行为没有抵抗能力，正常节点的信任值急剧下降；TP-BRSN算法具有一定的抵抗能力，一定程度上减少了诋毁的影响程度；本文提出的算法在诋毁刚发生时，对正常节点的信任值也发生了下降，但在经过4～6次通信后，信任程度又开始逐渐上升，这是因为恶意推荐节点的关联度极具降低导致的结果。

3) SNTUA 算法与已有模型的性能比较。

仿真实验结果如图8所示。信任模型的抗攻击能

力主要由系统中所有节点的通信成功率体现的。随着信任模型的更新，3个模型通信的成功率都上升，并逐步放缓，表明性能在后期趋于稳定。SNTUA的通信成功率一直高于其他两个信任模型，证明了该模型的正确性和有效性。

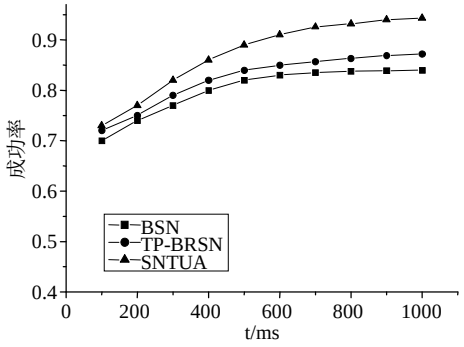

图8　各算法通信成功率性能对比图

综上所述，SNTUA算法使得善意节点的信任值平缓上升(相对缓慢)，而恶意节点的信任值下降剧烈，这样的性能可以保证信任模型在抵抗攻击更加可靠、迅速。通过对比试验证明了SNTUA比其他两个模型有更好的通信成功率。因此，SNTUA算法将社会网络关联度引入信任模型的有效性和正确性。

5　结　论

本文将社会网络分析中的关联度引入到WSN节点信任模型中，通过“社会网络关联度”修正和综合利用节点及其邻近节点的信誉度评价，提出了传感器节点信任值计算和更新算法(SNTUA)。通过仿真实验与其他两种算法在性能上进行了对比分析，证明SNTUA算法提高了恶意诽谤行为的检测率，降低其对传感器网络的影响，并为传感器节点的成功通信提供了保障。未来将在本文的基础上，进一步借鉴社会网络分析的方法和思想，重点研究将社会个体行为分析应用于WSN信任模型中，识别恶意攻击和推荐的行为特征，提高识别准确率。

参　考　文　献

[1] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y，et al. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4): 393-422.

[2] 林闯，彭雪海. 可信网络研究[J]. 计算机学报，2005, 28(5): 113-122.
LIN Chuang, PENG Xue-hai. Research on trustworthy networks[J]. Chinese Journal of Computers. 2005, 28(5): 113-122.

[3] BUCHEGGER S, BOUDEC J L. The selfish node: Increasing routing security in mobile Ad Hoc networks[R]. New York, USA: IBM, 2001

[4] MICHIARDI P, MOLVA R. Core: a collaborative reputation mechanism to enforce node coopetation in mobile ad hoc networks[C]//Proceedings of Sixth IFIP Conference on Secuirty Communications and Multimedia (CMS2002). Portoroz, Slvenia: Kluwer Academic Publisher, 2002: 107-121.

[5] GANERIWAL S, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks[C]// Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’04). New York. USA: ACM, 2004: 66-77.

[6] PROBST M J, KASERA S K. Statistical trust establishment in wireless sensor networks[C]//Proceedings of 13th International Conference on Parallel and Distributed Systems. Hsinchu: IEEE Computer Society, 2007: 1-8.

[7] HUR J, LEE Y, YOON H, et al. Trust evaluation model for wireless sensor networks[C]//Proc of the ICACT 2005. Piscataway: IEEE Computer Society, 2005: 491-496.

[8] 熊翱，赵晓东，高志鹏，等. 节点信誉相关的无线传感器网络故障检测[J]. 北京邮电大学学报, 2012, 35(1): 41-45.
XIONG Ao, ZHAO Xiao-dong, GAO Zhi-peng, et al. Wireless sensor networks fault detection via node credit value[J]. Journal of Beijing University of Posts and Telecommunications. 2012, 35(1): 41-45.

[9] 肖德琴，冯健昭，杨波，等. 基于无线传感器网络的信誉形式化模型[J]. 计算机科学, 2007, 34(6): 84-87,100.
XIAO De-qin, FENG Jian-zhao, YANG Bo, et al. Reputation formal model for wireless sensor network[J]. Computer Science. 2007, 34(6): 84-87,100.

[10] XIONG Li, LIU Ling. A reputation based trust model for peer to peer e-commerce communities[C]//Proceedings of IEEE International Conference on Ecommerce (CEC 2003). Newport Beach: IEEE, 2003: 275-284.

编　辑　税　红