nTRUST—A New Trust Scheme Based on Certainty Theory in Wireless Sensor Networks*

PAN Julong[1*], *GAO Jianqiao*[1], *XU Zhanyi*[1], *LI Wenjin*[1], *LI Ziyin*[2]

(1. *College of Information Engineering, China Jiliang University, Hangzhou* 310018, *China*;
2. *College of Optical Engineering, China Jiliang University, Hangzhou* 310018, *China*)

Abstract: As a safety protection scheme, trust scheme has significant effects and it has been widely used in the wireless sensor networks security. In this paper, we propose a new trust model named as nTRUST which based on Certainty Theory in uncertainty reasoning. An integrated trust value is computed to decide a node that is reliable or malicious. Some related experiments are testified with effectiveness and feasibility of nTRUST. In addition, under the work of this new trust scheme, we further consider the residual energy of the nodes. The simulation results also show that the modified nTRUST with residual energy can balance the node's energy consumption and prolong the whole network lifetime.

Key words: wireless sensor networks; security; trust scheme; Certainty Theory

EEACC: 6150P **doi**: 10.3969/j.issn.1004-1699.2012.02.020

一种基于确定性理论的无线传感器网络信任机制 nTRUST*

潘巨龙[1*], 高建桥[1], 徐展翼[1], 李文锦[1], 李子印[2]

(1. 中国计量学院信息工程学院, 杭州 310018; 2. 中国计量学院光学工程学院, 杭州 310018)

摘 要: 信任机制作为一种安全保护机制, 目前在无线传感器网络安全中有着显著效果并得到广泛应用。基于不确定性推理中的确定性理论, 提出了一种新的无线传感器网络信任模型—— nTRUST, 该模型采用综合信任值作为评价节点信任依据, 相关实验证实了 nTRUST 的有效性和可行性。同时, 在 nTRUST 信任机制作用下, 进一步考虑节点剩余能量, 通过实验取得较好效果, 改进后的模型可以达到均衡网络内节点能量消耗和延长整个网络生存周期目的。

关键词: 无线传感器网络; 安全; 信任机制; 确定性理论

中图分类号: TP393.08 **文献标识码**: A **文章编号**: 1004-1699(2012)02-0240-06

无线传感器网络 WSNs(Wireless Sensor Networks)是集分布式、自组织、嵌入式等技术于一体的一种新型无线网络, 它由低能量、低能耗、较少计算能力和存储能力的微型节点组成, 广泛应用于军用和民用领域, 如敌方军情侦探、森林火灾检测和医疗卫生监护等领域。它的工作原理主要是通过节点间的相互协作来收集目标对象信息, 并将信息通过路由发送给用户。随着 WSNs 的广泛应用, 以及 WSNs 常被部署在无人照看或危险地带, WSNs 安全和服务质量等问题日益受到人们关注。但由于 WSNs 节点资源受限等特点, 使得传统解决网络安全问题的常规方法, 如防火墙和公钥密钥加密等机制, 因其需要较多的计算资源而不再适用无线传感器网络。

近年来, 研究者提出基于信誉和信任的安全机制来解决 WSNs 中相关安全问题, 保证节点间能够安全地进行信息交换[1-3]。信任机制通过对节点过去行为的统计(即原有信誉情况)推断节点将来动作行为, 它是一种不确定推理机制。Ganeriwal 等人首先提出了基于贝叶斯理论和 β 分布的信任模型 RFSN[4], 利用先验概率与后验概率的关系对信任的不确定性进行分析, 同时结合先验概率 β 分布, 进而建立了 WSNs 安全相关的信任机制基本模型。但该模型存在高信誉值节点可能带来的恶意诽谤等缺点(即它贬低原有可信节点以提升恶意节点自身的信誉值)。成坚等人提出基于 D-S 证据理论的 WSNs 信任模型[5], 利用 D-S 证据理论处理信任的不确定性。但 D-S 证据理论计算复杂度呈现指数级的增长[6], 不利于在资源受限的无线传感器网络中应用。RGR(Trust

项目来源: 国家自然科学基金项目(61007012)
收稿日期: 2011-09-04 **修改日期**: 2011-11-17

Management for Resilient Geographic Routing)[7]协议利用节点直接信任值,它不考虑邻居节点对它的影响,该协议适应范围相对较窄。

确定性理论是 Shortliffe 等人提出的一种不确定性推理模型[8]。确定性理论具有简单、直观以及计算复杂度呈线性等优点[6],许多专家系统都是基于这一方法建立起来的。侯孟书等人已经成功地将确定性理论运用到 P2P 网络中,有效地隔离欺骗节点,提高电子交易成功率[9-10]。

本文基于不确定性推理中的确定性理论提出了一个新的无线传感器网络信任模型 nTRUST。该模型采用可信度作为节点的直接信任值,通过向邻居节点索取推荐信任值,最后合成综合信任值并作出节点是否可信的判断。同时,本文还在信任机制作用下,引入节点剩余能量的考虑,并通过实验验证达到均衡节点的能量消耗和延长网络生存周期的目的。

1　基于确定性理论的信任模型 nTRUST

确定性理论采用可信度作为不确定性测度。基于可信度表示的不确定性推理的基本方法也被称为 C-F 模型(Certainty Factors)[11]。

在 C-F 模型中,知识是用产生式规则表示的,一般形式表示为:

IF E THEN H(CF(H,E))

其中:E 是知识的前提条件,H 是结论,CF(H,E)是该条知识的可信度,可称为可信度因子或规则强度。CF(H,E)的取值范围在[-1,1]之间。

结论　H 的可信度 CF(H)由下式计算:

$$CF(H)=CF(H,E)\times\max\{0,CF(E)\} \quad (1)$$

CF(E)表示证据 E 的可信度,其取值范围在[0,1]之间。

在局部信任管理方式中,无线传感器网络内节点相互之间进行信任值的量化计算,具有主动发起角色的节点称为发起节点,具有被动角色的节点称为目标节点,发起节点和目标节点互为邻居关系。

在 WSNs 中采用最多的评价依据是节点的综合信任值,它由直接信任值与间接信任值合成。本文提出的新信任模型 nTRUST 也采用这种方式。首先,发起节点初始化目标节点的直接信任值,并根据目标节点的不同行为进行更新;其次,发起节点收集其它节点关于当前目标节点的推荐信任值,然后对推荐信任值进行过滤,再根据确定性理论的结论以及不确定性合成算法,将过滤后的推荐信任合成间接信任值,最后与直接信任值进行加权运算而形成节点的综合信任值。

1.1　节点直接信任值

节点直接信任值用 DT(Direct Trust)表示。$DT_{i,j}$表示节点 i 对节点 j 进行信任值量化而形成的关于节点 j 的直接信任值。

借鉴文献[9],我们定义式(2)

$$CF(H,E_{i,j})=\frac{\alpha_{i,j}-\beta_{i,j}}{\alpha_{i,j}+\beta_{i,j}} \quad (2)$$

其中 $E_{i,j}$是发起节点 i 对目标节点 j 的直接观察,故被认为是可信的,假设 $CF(E_{i,j})=1$。在节点 i 与节点 j 交互通信期间,合作次数为 $\alpha_{i,j}$,不合作次数为 $\beta_{i,j}$,结论 H 为节点 j 是 WSNs 中的一个正常节点。因而,我们可以推断:当 $\alpha_{i,j}=0$ 时,表示结论 H 完全不可信;而当 $\beta_{i,j}=0$ 时,表示结论 H 完全可信。再结合式(1),可推得式(3)

$$DT_{i,j}=CF_{i,j}(H)=\frac{\alpha_{i,j}-\beta_{i,j}}{\alpha_{i,j}+\beta_{i,j}} \quad (3)$$

1.1.1　节点信任值初始化

当 $t=t_0$ 时,WSNs 的信任机制开始工作,发起节点 i 首先初始化目标节点 j 的直接信任值。我们假设当 $t_0=0$ 时,节点 i 还没有开始与节点 j 交互,证据 $E_{i,j}$为空,即 $\alpha_{i,j}=0,\beta_{i,j}=0$. 此时,设 $DT_{i,j}=0$。

1.1.2　节点信任值更新

为了实时地响应目标节点 j 的行为变化和保持直接信任值 $DT_{i,j}$的新鲜性,发起节点 i 需要不断地更新目标节点 j 的直接信任值 $DT_{i,j}$,这体现了信任的上下文相关性。本文采用周期性更新方式,假设更新周期为 τ(τ 为某一固定值)。设当 $t=t_n$ 时,经过一个周期 τ 后,节点 i 又与节点 j 发生交互,产生了 $\delta_{i,j}+\theta_{i,j}$的新事件,$\delta_{i,j}$为合作次数,$\theta_{i,j}$为不合作次数。

考虑到恶意节点可能通过伪装和欺骗手段快速提升自己的信任值,并保持节点一直处于“正常”状态,在信任更新过程中,节点 i 将动态地选择更新权重 w_{rt}的大小,如式(4)所示。

$$w_{rt}=\begin{cases}0 & 当\left|\frac{\alpha_{i,j}^n}{\alpha_{i,j}^n+\beta_{i,j}^n}-\frac{\delta_{i,j}}{\delta_{i,j}+\theta_{i,j}}\right|\le\lambda\\ \frac{\alpha_{i,j}^n}{\alpha_{i,j}^n+\beta_{i,j}^n}-\frac{\delta_{i,j}}{\delta_{i,j}+\theta_{i,j}} & 当\left|\frac{\alpha_{i,j}^n}{\alpha_{i,j}^n+\beta_{i,j}^n}-\frac{\delta_{i,j}}{\delta_{i,j}+\theta_{i,j}}\right|>\lambda\end{cases} \quad (4)$$

其中 $\lambda\subset[0,0.5]$。

在 $t_{n+1}=t_n+\tau$ 时刻,节点 i 根据式(4)更新 $\alpha_{i,j}$和 $\beta_{i,j}$,得到式(5):

$$\begin{cases}\alpha_{i,j}^{n+1}=\alpha_{i,j}^n+(1+w_{rt})\times\delta_{i,j}\\ \beta_{i,j}^{n+1}=\beta_{i,j}^n+(1+w_{rt})\times\theta_{i,j}\end{cases} \quad (5)$$

当$\frac{\alpha_{i,j}^n}{\alpha_{i,j}^n+\beta_{i,j}^n}>\frac{\delta_{i,j}}{\delta_{i,j}+\theta_{i,j}}$　时,$w_{rt}>0$,即近期信任比重

较大,可维持节点处于原有正常状态,一旦发生恶意行为,节点将会受到相应惩罚;而当$\frac{\delta_{i,j}}{\delta_{i,j}+\theta_{i,j}} > \frac{\alpha_{i,j}^{n}}{\alpha_{i,j}^{n}+\beta_{i,j}^{n}}$时,$w_{rt}<0$,这样可以防止恶意节点通过伪装和欺骗手段快速提升自身的信任值。

节点 i 利用更新后所得的 $\alpha_{i,j}^{n+1}$ 和 $\beta_{i,j}^{n+1}$,再结合式(3),当 $t=t_{n+1}$ 时,节点 i 对节点 j 的直接信任值为 $\mathrm{DT}_{i,j}^{n+1}=\frac{\alpha_{i,j}^{n+1}-\beta_{i,j}^{n+1}}{\alpha_{i,j}^{n+1}+\beta_{i,j}^{n+1}}$。

1.2 节点间接信任获取

间接信任主要是发起节点向目标节点的邻居节点索取的。在无线传感器网络的信任机制下,同时采用直接、间接信任值可获得目标节点更加详细状况,保持目标节点在网络中的状态一致性。但是向邻居节点索取信任信息,会消耗发起节点大量的能量,不利于网络的生存时间,并且还会引来节点的诽谤攻击。为了解决采纳间接信任所带来的上述问题,我们分别采用推荐信任过滤机制和考虑节点剩余能量来解决。间接信任值用 IT(Indirect Trust)表示。

节点间接信任值的推荐过程示意图见图 1 所示。设 $\mathrm{IT}_{k,j}$ 和 $\mathrm{IT}_{l,j}$ 分别为节点 k 和 l 对节点 j 的间接信任值,$\mathrm{IT}_{k,s}$ 为节点 k 对节点 s 的间接信任值。首先节点 i 向它的邻居节点发送包含目标节点 j 和 s 的 id 号的信任请求包,邻居节点在收到发起节点 i 的请求包后,查询节点 j 和 s 是否在自己的邻居列表中,根据查询结果,产生一个应答包,将自己对被评估节点 j 和 s 的直接信任值送回节点 i。节点 i 在收到邻居节点发送的推荐信任值后,将分别对 j 和 s 进行推荐信任合成,具体过程见 §1.4。

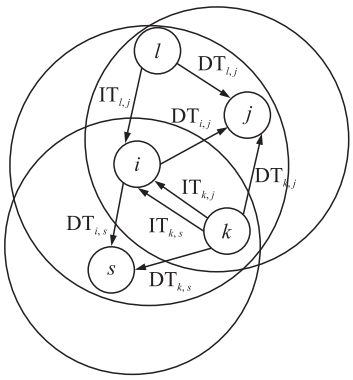

图 1 节点间接信任值推荐过程示意图

1.3 推荐信任值过滤

如上所述,采用间接信任会引来节点的诽谤攻击。原因在于无线传感器网络的节点是部署在开放的、分布式环境中,故网络中可能存在恶意推荐者,它们为了达到破坏网络目的,可能提供一些不公正的推荐信息。例如,在选择下一跳路由节点时,恶意推荐者通过提供虚假的推荐信任值,干扰节点做出正确选择。因此在信任模型中,寻找可以有效避免或者减少恶意推荐影响的方法是一个至关重要的问题[12]。

本文仅关注单独恶意推荐者的恶意推荐行为,即不考虑恶意推荐者之间的合谋。单独不公正推荐行为包括以下 3 类:正常节点由于误察而发送不真实推荐;恶意节点发送不真实推荐;表现“良好”的节点(被称为恶意间谍)发送不真实推荐[13]。本文主要关注后两种情况。

在现有的无线传感器网络信任模型中,如 RFSN[4],GTMS[14] 等,主要考虑恶意节点发送不真实推荐的情况。它们通过设定信任阈值 Threshold(在 RFSN 中,设定 Threshold = 0.9),仅接受信任值超过阈值的节点发送的推荐,即要求 $\mathrm{DT}_{i,k} \geqslant$ Threshold。但不能防止恶意间谍节点发送的不真实推荐。

为解决上述问题,我们在设定信任阈值的基础上,将已通过阈值检测而被接受的推荐信任进行数据分簇,选取较大簇的数据作为最终接受的推荐信任,即进行聚类[15]。由于真实的推荐信息之间有一定的相关性,而不真实与真实信息之间存在差异性,同时不真实的推荐个数一般较少,故能产生较大簇。本文采用经典的 C-Means 聚类算法[16],进行节点信任的最后处理,具体处理流程见图 2 所示。

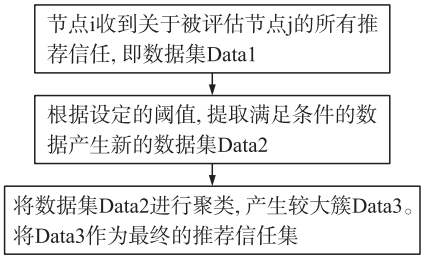

图 2 推荐信任数据集相关处理流程图

1.4 节点信任的综合

在完成推荐过滤之后,发起节点 i 将 Data3 数据集中的推荐信任值,根据结论不确定的合成算法,合成间接信任值 $\mathrm{IT}_{i,j}$,见下式所示:

$$\mathrm{IT}_{i,j}=\begin{cases}\mathrm{DT}_{k,j}+\mathrm{DT}_{l,j}-\mathrm{DT}_{k,j}\times\mathrm{DT}_{l,j} & \text{若 } \mathrm{DT}_{k,j}\geqslant 0,\mathrm{DT}_{l,j}\geqslant 0\\ \mathrm{DT}_{k,j}+\mathrm{DT}_{l,j}+\mathrm{DT}_{k,j}\times\mathrm{DT}_{l,j} & \text{若 } \mathrm{DT}_{k,j}<0,\mathrm{DT}_{l,j}<0\\ \dfrac{\mathrm{DT}_{k,j}+\mathrm{DT}_{l,j}}{1-\min\{|\mathrm{DT}_{k,j}|,|\mathrm{DT}_{l,j}|\}} & \text{若 } \mathrm{DT}_{k,j}\text{与 }\mathrm{DT}_{l,j}\text{异号}\end{cases}$$

最后,发起节点 i 将关于目标节点 j 的直接信任值和间接信任值最后合成综合信任值,见下式所示:

$$T_{i,j}=W_{dt}\times \mathrm{DT}_{i,j}+W_{it}\times \mathrm{IT}_{i,j}$$

其中($W_{dt}+W_{it}=1$),W_{dt}和 W_{it}分别表示直接信任值 $\mathrm{DT}_{i,j}$和间接信任值 $\mathrm{IT}_{i,j}$所占的权重。

2　能量有效性

本文在 nTRUST 的基础上,进一步考虑节点的剩余能量,用来弥补采用间接信任值所导致的节点能量消耗过快的缺陷,以达到均衡网络节点的能量消耗,延长网络生存周期的目的[17],并将该改进信任模型称为 nTRUST-E。首先设置节点剩余能量阈值 Ethreshold,然后节点通过比较自身的能量是否大于该阈值,选择是否继续工作。在 nTRUST-E 下,当节点的能量低于阈值时,节点不再周期性更新信任值和作为路由节点发送数据包,但是仍会响应其他节点发送的推荐信任请求。当某个节点的所有邻居节点的能量都低于阈值,重新设置阈值,将其设为 0,我们称之为阈值切换。此时,在这个节点的邻居列表中的低于能量阈值的节点将会重新参与信誉值计算和路由转发。而不在这个节点的邻居列表中的低于阈值的节点则不受影响。

但是,我们注意到考虑剩余能量后同时会带来一些新的问题:

(1)考虑剩余能量可能产生发起节点切换目标节点的情况,使得选中的目标节点能保留所设最低门限能量,但这样需付出更换路径的代价,将影响网络的吞吐率。

(2)在存在恶意节点的情况下,考虑剩余能量会迫使发起节点在一个正常节点不能满足能量要求的情况下,不得不去重新选择另一个节点,这样会增加潜在恶意节点被选中的机会,从而降低网络的转发率和吞吐率。

考虑上述因素,在选用 nTRUST-E 模型时,节点 i 根据如下规则选择正常节点作为下一跳路由,避免恶意节点参与计算:首先节点 i 会根据能量阈值筛选邻居节点,然后再根据它们信任值排序筛选出前几个,得到节点 i 认为正常的邻居集,最后,根据路由协议选择某个节点作为下一跳。特别的是,当邻居中只有一个节点的能量大于阈值时,但它的信任值已低于设定信任阈值,此时将提前进行能量阈值切换,以避免选择恶意节点作为路由。

3　实验分析

实验环境如下:100 个节点随机分布在 100 m×100 m 的场景中,随机选择 5% 的节点为恶意节点,某一场景的节点分布图见图 3 所示。假设恶意节点的转发率为 33.3%,正常节点的转发率为 90%。另选取 5 个节点作为发起节点。采用 GPSR 路由协议,对目标节点可用邻居根据信任值高低作出限制,实验中将最高信任和次高信任节点作为邻居节点。假设节点之间通信半径为 20 m。实验采用 OMNET4.1 软件实现。

假设信任机制在网络运行 200s 后开始工作。此时,恶意节点的初始合作次数小于等于初始不合作次数,而正常节点的初始合作次数大于等于初始不合作次数。假设接受推荐信任的直接信任阈值为 0.8,节点信任更新周期为 10 s。

为了在考虑剩余能量时更好地观察阈值切换,我们将初始节点能量假设为较小值,约为 2 J,剩余能量阈值为 0.4 J。空闲功率为 0 W;发送功率为 0.5 W;接收功率为 0.2 W。其中,假设发送节点有较大能量,数据包的大小为 280 bit。

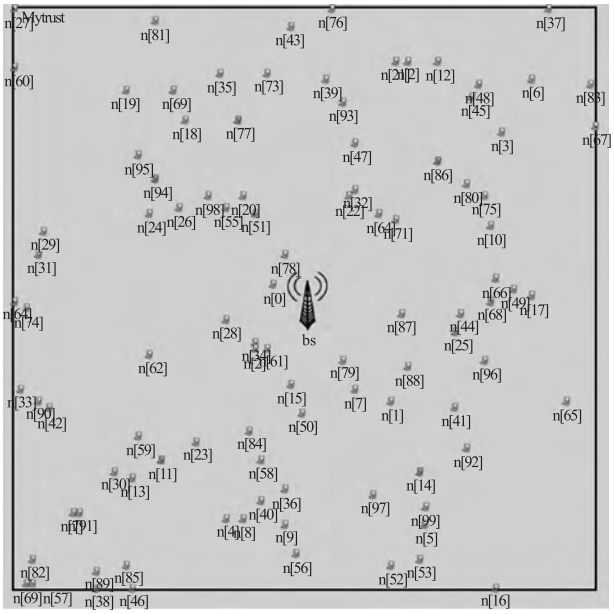

图 3　100 个节点随机分布图

3.1　可行性分析

首先,我们通过 nTRUST 与 RFSN、RGR 在网络转发率和吞吐率方面进行比较,验证 nTRUST 的可行性,参见图 4 和图 5。

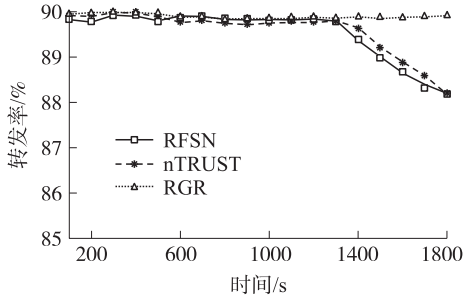

图 4　网络转发率比较图

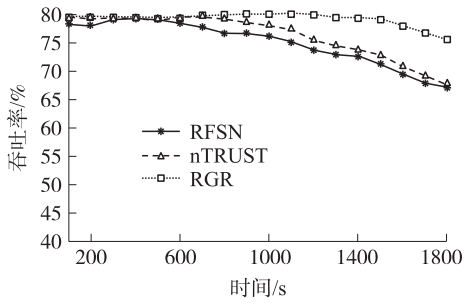

图 5 网络吞吐率比较图

从图 4 和图 5 比较可以发现,nTRUST 在网络转发率与吞吐率上与 RFSN 模型相差不大。观察到 RGR 的转发率和丢包率要好于 nTRUST,但是 RGR 协议有它的局限性,它仅考虑节点直接信任值,尤其是存在 sybil 节点时,它的适用性较差。在图 4 中可以观察到在 1 300 s 后,nTRUST 和 RFSN 的转发率都开始下降,说明节点开始选择较低转发率节点作为下一跳路由节点。这可以与之后加入剩余能量的 nTRUST-E 模型进行比较,观察是否 nTRUST-E 会比 nTRUST 更早地选择较低转发率节点作为下一跳路由节点。

3.2 节点剩余能量的影响

如前所述,考虑 WSNs 节点剩余能量后,可以均衡节点的能量消耗和延长网络生存周期。但是,考虑节点剩余能量需付出因更换路由所付出的代价。特别地,在有恶意节点的情况下,考虑剩余能量会增加选择恶意节点作为路由节点的风险,可能导致降低网络的转发率和吞吐率。见图 6、图 7、图 8 和图 9。

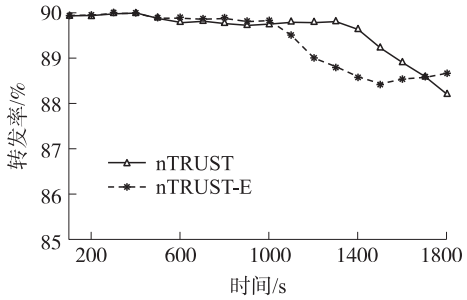

图 6 两种模型转发率比较图

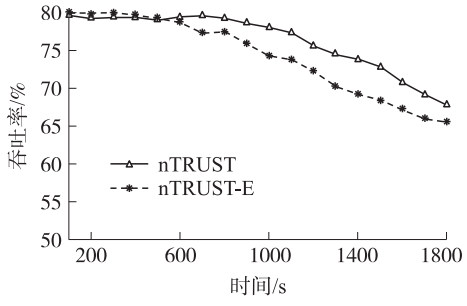

图 7 两种模型吞吐率比较图

比较图 6 和图 7 可以发现,两种模型网络转发率在 1 000 s 前是十分相似的,但在 1 000 s 开始,nTRUST-E 网络的转发率和吞吐率明显下降。这是因为考虑了剩余能量,导致更换路由表带来的结果。nTRUST-E 网络的吞吐率因为网络转发率下降和网络需更换转发路径而比 nTRUST 要略低一些。

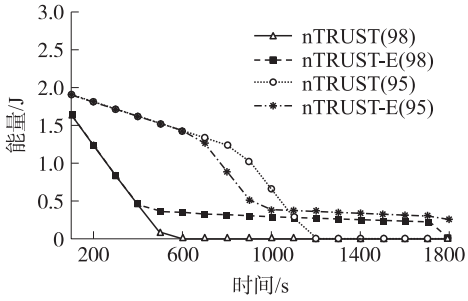

图 8 任意两节点的能量消耗比较图

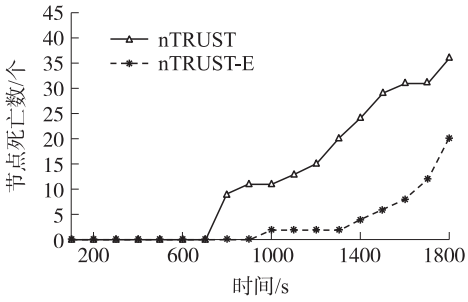

图 9 网络死亡节点数比较图

从图 8 中,显示了随机选择的 95 号和 98 号节点的能量变化情况。可以看到在 nTRUST-E 下,节点的能量消耗要比 nTRUST 缓慢,达到了均衡节点能量消耗的目的。从图 9 我们看到,在工作 1 000 s 后,nTRUST-E 节点死亡数明显比 nTRUST 节点死亡数要少,验证了考虑节点剩余能量能延长网络生存周期的目的。

3.3 推荐过滤

针对 RFSN 存在的无法应对高信任节点发送的诽谤推荐,即存在诋毁正常节点和鼓吹恶意节点行为,从而降低网络整体服务质量的情况。我们在设定信任阈值的基础上,再对推荐信任进行聚类处理,选择较大的数据集作为最终推荐信任集。

从图 10 可以看到,在存在高信任节点发起诽谤攻击的情况下,nTRUST-E 的网络转发率与网络吞

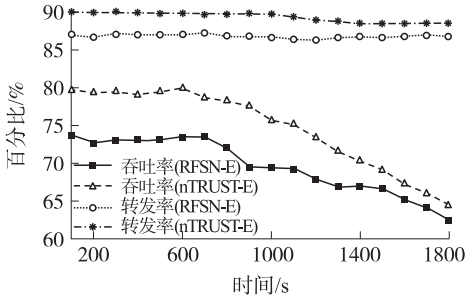

图 10 两种模型转发率和吞吐率比较图

吐率明显要好于 RFSN-E。从而可以证实在增加了对推荐信任进行聚类处理的操作后,nTRUST-E 可以在一定程度上阻止高信任节点发起的诽谤攻击,进而提高网络的服务质量。

4　结论

本文基于不确定性推理中的确定性理论提出了一钟新的无线传感器网络信任模型 nTRUST。针对高信任节点存在发送虚假推荐的可能性,我们采用聚类算法进行防止虚假推荐相关技术处理,通过实验验证了其有效性。同时,在 nTRUST 信任机制作用下,引入节点剩余能量的考虑,并通过实验验证,达到了均衡节点的能量消耗和延长网络生存周期的目的,取得了较好实验效果。

参考文献:

[1] Jaydip S. A Survey on Reputation and Trust-Based Systems for Wireless Communication Networks[J]. International Journal HIT Transaction on ECCN(Electronics,Communication,Computers and Networking),arXiv e-print,2010,1(2):92-111.

[2] Yu Y, Keqiu L, Wanlei Z, et al. Trust Mechanisms in Wireless Sensor Networks:Attack analysis and countermeasures[J]. Journal of Network and Computer Applications,2011,1-14.

[3] 黄旗明,南海燕. 基于 Dirichlet 分布的无线传感器网络的信誉计算模型研究[J]. 传感技术学报,2009,22(4):526-530.

[4] Ganeriwal S,Balzano L,Srivastava M. Reputation-Based Framework for High Integrity Sensor Networks[J]. ACM Transactions on Sensor Networks(TOSN),2008,4(3):1-37.

[5] 成坚,冯仁剑,许小丰,等. 基于 D-S 证据理论的无线传感器网络信任评估模型[J]. 传感技术学报,2009,22(12):1802-1807.

[6] 陈翔. 专家系统中不精确推理的研究与应用[D]. 合肥:安徽大学硕士论文,2006.

[7] Liu K,Abu -Ghazaleh N,Kang K. Location Verification and Trust Management for Resilient Geographic Routing[J]. Journal of Parallel and Distributed Computing,2007,67(2):215-228.

[8] Heckerman D E,Shortliffe E H. From Certainty Factors to Belief Networks[J]. Artificial Intelligence in Medicine,1992,4(1):35-52.

[9] 侯孟书,卢显良,任立勇,等. 基于确定性理论的 p-p 系统信任模型[J]. 电子科技大学学报,2005,34(6):806-808.

[10] Mengshu H,Xianliang L,Xu Z,et al. A Trust Model of p-p System Based on Confirmation Theory[J]. ACM SIGOPS Operating Systems Review,2005,39(1):56-62.

[11] 王永庆. 人工智能原理与方法[M]. 西安:西安交通大学出版社,2006.

[12] Weiwei Y, Donghai G, Sungyoung L, et al. Finding Reliable Recommenda-tions for Trust Model[J]. Web Information Systems, CWISE 2006,LNCS Vol 4255/2006,375-386.

[13] Weiwei Y, Donghai G, Sungyoung L, et al. Filtering out Unfair Recommen-dations for Trust Model in Ubiquitous Environments[J]. Information Systems Security,2006,LNCS Vol 4332/2006:357-360.

[14] Shaikh R A,Jameel H. Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks[J]. IEEE Transactions on Parallel and Distributed Systems,2008,20(1):1698-1712.

[15] 杨磊,秦志光,钟婷. 基于聚类推荐的 p-p 信任模型[J]. 计算机应用研究,2010,27(4):1469-1472.

[16] 孙即祥. 现代模式识别[M]. 长沙:国防科技大学出版社,2002.

[17] 刘志新,郑庆超,薛亮,等. 一种综合能量和节点度的传感器网络分簇算法[J]. 软件学报,2009,20(zk):250-256.

潘巨龙(1965-),男,博士,教授,主要研究方向为无线传感器网络安全、移动计算、嵌入式系统及应用等,pjl@cjlu.edu.cn。