结合模糊集合与 D-S 证据理论的 WSN 信任评估模型

周治平，赵晓晓，邵楠楠
(江南大学物联网技术应用教育部工程研究中心，江苏 无锡 214122)

摘要： 兼顾安全性需求和能耗因素，定义 3 种典型信任因子来计算节点的直接信任值，利用模糊集合理论进行模糊划分，将模糊隶属度函数作为 D-S 证据理论中的基本置信度函数；通过邻居节点的推荐获取节点的间接信任值，根据 Dempster 组合规则对基于权重修正后的直接信任值与间接信任值进行融合。将基于身份的密码机制与信任管理机制进行有效结合，提高信任信息在传递中的安全性。分析与仿真结果表明该模型有良好的动态适应性及鲁棒性，能及时、准确地识别网络中的恶意节点，有效提高网络的安全性。

关键词： 无线传感器网络；信任评估；模糊集合；D-S 证据理论；密码机制
中图分类号：TP393 文献标识码：A 文章编号：1004-731X (2018) 04-1229-08
DOI: 10.16182/j.issn1004731x.joss.201804003

Trust Evaluation Model Based on Fuzzy Set and D-S Evidence Theory in Wireless Sensor Network

Zhou Zhiping, Zhao Xiaoxiao, Shao Nannan
(Engineering Research Center of Internet of Things Technology Applications Ministry of Education, Jiangnan University, Wuxi, 214122, China)

Abstract: A trust evaluation model based on fuzzy set and D-S evidence in wireless sensor network is proposed. Considering security requirements and energy consumption, *three typical trust factors are defined to calculate node's direct trust which is for fuzzy classification by using fuzzy set theory. Fuzzy membership function is the basic belief function of the D-S evidence theory.* Indirect trust is obtained from neighbor nodes' recommendations, the direct trust and indirect trust are fused according to Dempster combination rule after being amended with weight. *The effective combination of identity-based cryptosystem and the trust management mechanism improve the security of trust information in the transmission.* The analysis and simulation results show that the proposed model has good dynamic adaptability and robustness, and can identify the malicious nodes timely and accurately, so as to improve the security of the networks availably.

Keywords: wireless sensor networks (WSNs); trust evaluation; fuzzy set; D-S evidence theory; cryptosystem

引言

随着无线传感器网络[1](Wireless Sensor Network，WSN)的广泛应用，其面临的安全威胁日益多样化[2]，安全需求也越来越迫切。基于认证和加密的安全机制[3]只能抵御来自网络外部的攻击，不能有效识别通过认证的节点发起的网络内部攻击。作为有效的补充机制，信任管理[4]系统根据节点行为特征计算节点信任值来判断节点是否可信，进一步调整网络安全措施，保证网络的安全性与可靠运行。

作为信任管理系统的核心，信任评估模型的建

收稿日期：2016-05-19 修回日期：2016-07-24；
基金项目：国家自然科学基金(61373126)，江苏省自然科学基金(BK20131107)，中央高校基本科研业务费专项资金(JUSRP51510)；
作者简介：周治平(1962-)，男，江苏无锡，博士，教授，研究方向为检测技术与自动化装置、信息安全等。

立是近年来 WSN 安全的研究热点之一[5-6]。Ganeriwal 等[7]提出了一个较完整的典型 WSN 信任管理框架 RFSN(Reputation-Based Framework for High Integrity Sensor Networks)，采用看门狗机制监测节点行为，利用贝叶斯公式和 beta 分布计算节点信任值，然而节点不允许传播恶意推荐，无法应对网络中一些不确定的情况。房卫东等[8]提出一种基于 beta 分布的信任机制，能有效的抵御 on-off 攻击，但不能快速准确的识别攻击节点。Ishmanov 等[9]考虑持久恶意行为的影响，利用 one-step M-estimator 进行推荐信任融合，能有效抵御 on-off 攻击及持久的恶意行为。Duan[10]提出一种能量感知的信任推导方案，利用风险策略模型激励节点合作，并采用博弈论的方法减少信任推导过程中的开销，但该算法复杂度较高，不适用于能量有限的 WSN。Che 等[11]提出一种轻量级的 WSN 信任管理方案，利用贝叶斯理论进行直接信任的更新与计算，并判断直接信任的置信度是否足够作为综合信任，若不能则考虑推荐信任，利用熵进行权重分配，降低了主观分配权重的局限性。Jiang 等[12]充分考虑通信信任、能量信任及数据信任等计算节点直接信任，并定义了推荐可靠性及关系熟悉度来提高推荐信任的准确性。上述方案大多采用单一信任因子获取信任值，不能完全反映节点真实的信任属性；基于概率统计来计算节点信任，不能体现节点信任评估的主观性及不确定性。模糊逻辑和 D-S 证据理论是信任不确定性表达和处理的一种有效方法。基于 D-S 证据理论，成坚等[13]提出一种有效的信任评估模型，对直接信任和间接信任进行基于权重的修正，具有良好的容错性及动态适应性，但采用单一信任因子计算信任值，不能准确反映节点真实的信任属性。Feng 等[14]基于改进的 D-S 证据理论，提出一种信任管理方案(trust management scheme，TMS)，解决了信任的主观性问题，为了保持信任及能耗的平衡关系，仅当没有直接信任时才使用间接信任，该方法虽然减少了能耗，但得到的信任值并不准确。姚雷等[15]从网络通信特性、数据相关属性、自身物理属性三方面定义多种信任要素，利用层次分析法确定各要素的权重，并通过多层次模糊综合评判获取综合信任值，克服了信任评估的主观性，具有较高的恶意节点识别率，然而信任要素数目过多导致算法复杂度的增加。上述有关信任模型的研究中都存在一个有待改进的方面，即忽略了如何保证信任信息的安全性问题。

针对上述文献中提到的问题，本文提出一种结合模糊集合与 D-S 证据理论的安全 WSN 信任评估模型。根据传感器网络中常见的攻击方式、主要任务及信任因子与网络能耗之间的矛盾，定义了三种典型信任因子来计算节点直接信任，既避免计算单一信任因子造成节点信任属性的不完整性，又能解决计算过多信任要素带来的复杂度增加问题；利用模糊集合理论将节点信任进行模糊划分，避免了先验分布的主观假设；综合考虑直接信任与间接信任，能抑制网络中的恶意节点对信任值的影响。同时将基于身份的密码机制与信任管理机制进行有效结合，解决信任信息传递的安全性问题。

1 相关基础理论

1.1 信任关系的模糊分类

传感器节点之间的信任度是模糊、不确定的，主要因为：(1) 信任的分类是基于多值逻辑；(2) 某一确定的信任值可能隶属于不同的信任度，不是仅属于其中的某一信任度。因此利用模糊隶属度，我们提出一种有效的方法对主观信任关系进行量化分析。

节点信任的模糊分类如下：首先，将信任度划分为三类，即不可信、不确定及可信；其次据上述三类信任度，构造三个模糊子集 T_1、T_2 及 T_3，对应隶属度函数分别为 $u_1(t)$、$u_2(t)$ 及 $u_3(t)$ 且 $u_1(t)+u_2(t)+u_3(t)=1$，如图 1 所示。

1.2 D-S 证据理论

D-S 证据理论基于有限集合 Ω，Ω 由互斥且穷举的基本命题构成。2^{Ω} 是 Ω 的幂集。文中我们

将 Ω 定义为 $\{T,-T\}$，其中 T 和 $-T$ 分别代表两种信任状态，即节点可信和节点不可信，对应 2^{Ω} 为 $\{\Phi,\{T\},\{-T\},\{T,-T\}\}$，其中 Φ 代表空集，$\{T\}$，$\{-T\}$，$\{T,-T\}$ 分别表示“节点可信”、“节点不可信”、“节点状态不确定”的命题。基于 2^{Ω} 可以定义基本置信度函数 m：

$$\begin{cases} m(\Phi)=0 \\ \sum_{A\subseteq\Omega} m(A)=1, A\neq\Phi \end{cases} \tag{1}$$

式(1)中，A 为 2^{Ω} 中任意可能命题。

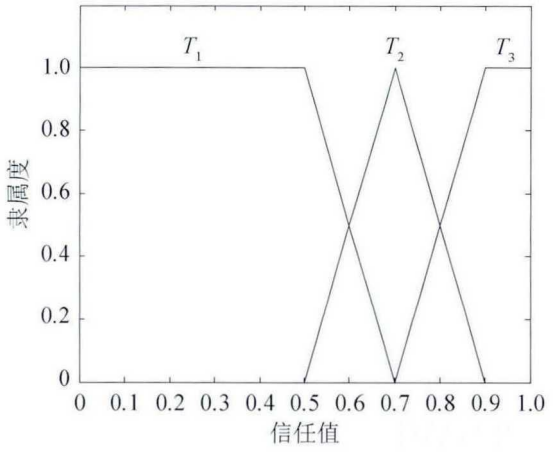

图 1 节点信任值的隶属度函数

Fig. 1 The membership function of node's trust value

2 结合模糊集合和 D-S 证据理论的信任评估

2.1 直接信任的评估

WSN 中常见的攻击方式主要有选择性转发攻击、黑洞攻击、篡改攻击、冒充攻击、重放攻击[16]等，为了抵御各种不同的攻击，在计算节点信任值时需要综合考虑各种能体现上述攻击行为特征的信任因子，如发送率因子、新鲜性因子、一致性因子、转发率因子、完整性因子等[17]。然而，信任因子数目与网络能耗之间存在着明显的矛盾，即信任因子越多，其计算得到的信任值就越准确，相应地，网络能耗就会越大。WSN 中节点的主要任务就是感知监测区域内数据信息并将其传递到基站，因此数据正确完整的转发尤为重要。此外，无线信道的干扰及恶劣环境可能会导致节点不可用。综合考虑上述攻击行为、网络主要任务及信任因子数目与网络能耗之间的矛盾等因素的影响，本文从通信特性、数据属性、物理属性 3 个方面分别选择其中典型的信任因子，即转发率因子、完整性因子及可用性因子，假设节点 i 和节点 j 互为邻居节点，节点 i 对节点 j 进行信任评估，3 个信任因子分别定义如下：

(1) 转发率因子 $FF_{i,j}(t)$：传感网络中节点的主要任务是感知监测区域内的数据并将其传递到基站，考虑到能量有限，WSN 中的节点无法直接与基站进行通信，需要其邻居节点的多跳转发。假设节点每收到一个转发数据包，就产生一个 ACK 反馈信息进行确认。根据节点数据包的转发情况，可以判断节点是否存在选择性转发攻击、黑洞攻击等。转发率因子定义如式(2)，其中 $TP_{i,j}(t)$ 是需要转发的数据包数目；$ACK_{i,j}(t)$ 是发送的反馈信息包数目，即邻居节点成功转发数据包的数目：

$$FF_{i,j}(t)=\frac{ACK_{i,j}(t)}{TP_{i,j}(t)} \tag{2}$$

(2) 完整性因子 $IF_{i,j}(t)$：为了防止网络中恶意节点发起篡改攻击，篡改转发数据包，需要对转发数据包的完整性、正确性进行评估。发送数据包后，源节点会在一定时间内监听其下一跳邻居节点是否对数据包进行了篡改，即是否正确转发了该数据包。完整性因子定义如式(3)，其中，$FP_{i,j}(t)$ 为需要转发的数据包数目；$IP_{i,j}(t)$ 为未经篡改、正确转发的数据包数目：

$$IF_{i,j}(t)=\frac{IP_{i,j}(t)}{FP_{i,j}(t)} \tag{3}$$

(3) 可用性因子 $AF_{i,j}(t)$：在某些情况下，无线信道的干扰及恶劣的环境会导致传感器网络中节点不可用。节点 i 通过发送“HELLO”数据包来检测节点 j 能否接收到该数据包，如果节点 i 收到来自节点 j“ACK-HELLO”数据包，那就证明节点 j 是可用的。节点可用性计算公式如式(4)，其中 $ACK_{i,j}(t)$ 是被响应的“HELLO”数据包数；$NACK_{i,j}(t)$ 是未

被响应的"HELLO"数据包数：

$$AF_{i,j}(t)=\frac{ACK_{i,j}(t)}{ACK_{i,j}(t)+NACK_{i,j}(t)} \tag{4}$$

基于上述 3 类信任因子，评价节点 i 采用加权平均的方法计算被评价节点 j 的直接信任值，则节点 i 对节点 j 在当前时刻的直接信任值计算如下：

$$CDT_{i,j}^{D}(t)=\omega_1 FF_{i,j}(t)+\omega_2 IF_{i,j}(t)+\omega_3 AF_{i,j}(t) \tag{5}$$

其中 ω_1、ω_2、ω_3 是加权系数，可以根据网络的具体应用要求针对性设置，且满足 $\omega_1+\omega_2+\omega_3=1$。本文仿真实验分别设置 $\omega_1=0.3$，$\omega_2=0.3$，$\omega_3=0.4$。

考虑到 on-off 攻击的影响，利用历史直接信任对上述直接信任进行修正，即直接信任更新如下：

$$DT_{i,j}^{D}(t)=\beta CDT_{i,j}^{D}(t)+(1-\beta)HDT_{i,j}^{D}(t) \tag{6}$$

式(6)中，$DT_{i,j}(t)$ 为当前信任周期修正后的直接信任值；$HDT_{i,j}(t)$ 为上一更新周期的历史直接信任；β 为自适应时间因子，用来权衡当前信任和历史信任所占比重，定义如下：

$$\beta=\begin{cases}\beta_s & CDT_{i,j}^{D}(t)\geq HDT_{i,j}^{D}(t)\\ \beta_l & CDT_{i,j}^{D}(t)<HDT_{i,j}^{D}(t)\end{cases} \tag{7}$$

式中：$0<\beta_s<\beta_l<1$，β_s 取值较小，防止恶意节点通过伪装欺骗较快积累自身信任，即防止恶意节点发起 on-off 攻击，β_l 取值较大，体现对节点恶意行为的严厉惩罚。

2.2 间接信任的获取

间接信任即第三方节点 k 关于被评价节点 j 的直接信任，是评价节点 i 通过查询第三方节点 k 得到的。为避免信任的循环递归且减少网络的通信负担，间接信任的获取限制在评价节点与被评价节点的共同邻居节点内进行，即只有评价节点 i 和被评价节点 j 的共同邻居节点 k (k=1,2,…,q)才能提供节点 i 关于节点 j 的间接信任。当第三方节点 k 收到评价节点 i 关于被评价节点 j 的信任查询信息时，k 直接将其关于被评价节点 j 的直接信任作为推荐信任传递给节点 i。为保证网络的连通性，WSN 中的节点通常密集部署，因此大部分评估节点都能获得对被评估节点的间接信任值。若没有共同的邻居节点，将直接信任值作为对被评价节点 j 的综合信任值。

间接信任的获取过程即信任的传输过程，如何保证信任信息的安全性至关重要。现有传感器网络信任模型在信任传递过程中，一般假设存在一条安全通道，如何应用、如何保证信任信息的安全性还有待改进。为解决这一问题，本文将基于身份的密码体制与所提信任管理机制进行有效融合，即，当第三方节点 k 收到评价节点 i 的信任查询信息 $ID_i\|ID_j\|X_j\|\varepsilon$ 后，返回用自己与评价节点 i 的共享秘钥加密的信任响应消息 $ID_k\|ID_i\|K_{ik}(X_j,\varepsilon)$，其中 ID_i、ID_j 及 ID_k 分别表示评价节点 i、被评价节点 j 及第三方节点 k 的身份信息，X_j 是节点 j 信任信息的标志，ε 是时间戳，K_{ik} 是评价节点 i 和第三方节点 k 的共享密钥。节点通过上述方法对所传输的信任信息进行加密，有效保证了信任信息在传输中的安全性及可靠性。

2.3 综合信任

2.3.1 信任向量

在节点信任的整合过程中，将节点 i 关于节点 j 的信任值表示成一个向量的形式。节点 i 关于节点 j 的直接信任、间接信任及综合信任的向量表示形式如公式(8)所示。

利用 1.1 节的相关隶属度函数，我们可以分别计算节点 j 关于"不可信"、"不确定"、"可信"3 类信任度的隶属度，$DT_{i,j}(t)$ 的隶属度 u_1^D、u_2^D、u_3^D 及 $IT_{k,j}(t)$ 的隶属度 u_1^k、u_2^k、u_3^k 分别计算如公式(9)所示。

$$\begin{cases}\boldsymbol{VDT}_{i,j}^{D}(t)=(m_{i,j}^{D}(\{T\}),m_{i,j}^{D}(\{T,-T\}),m_{i,j}^{D}(\{-T\}))\\ \boldsymbol{VIT}_{i,j}^{1}(t)=(m_{i,j}^{1}(\{T\}),m_{i,j}^{1}(\{T,-T\}),m_{i,j}^{1}(\{-T\}))\\ \cdots\\ \boldsymbol{VIT}_{i,j}^{q}(t)=\left(m_{i,j}^{q}(\{T\}),m_{i,j}^{q}(\{T,-T\}),m_{i,j}^{q}(\{-T\})\right)\\ \boldsymbol{VT}_{i,j}(t)=\left(m_{i,j}(\{T\}),m_{i,j}(\{T,-T\}),m_{i,j}(\{-T\})\right)\end{cases} \tag{8}$$

$$\begin{cases} u_1^D = u_1\left(DT_{i,j}(t)\right) \\ u_2^D = u_2\left(DT_{i,j}(t)\right) \\ u_3^D = u_3\left(DT_{i,j}(t)\right) \end{cases} 和 \begin{cases} u_1^k = u_1\left(IT_{k,j}(t)\right) \\ u_2^k = u_2\left(IT_{k,j}(t)\right) \\ u_3^k = u_3\left(IT_{k,j}(t)\right) \end{cases} \quad (9)$$

如果我们把节点信任分类的隶属度函数作为命题$\{-T\}$，$\{T,-T\}$，$\{T\}$的基本置信度函数，那么$u_1(t)$、$u_2(t)$及$u_3(t)$分别代表信任证据对“不可信”、“不确定”、“可信”3 种命题成立的支持程度，也就是说，直接信任中的组成元素$m_{i,j}^D(\{T\})$、$m_{i,j}^D(\{T,-T\})$、$m_{i,j}^D(\{-T\})$分别等于u_1^D、u_2^D、u_3^D，类似地，$\boldsymbol{VIT}_{i,j}^k(t)$的组成元素$m_{i,j}^k(\{T\})$、$m_{i,j}^k(\{T,-T\})$、$m_{i,j}^k(\{-T\})$分别等于$u_1^k$、$u_2^k$、$u_3^k$。

2.3.2 分信任值的修正

由于网络中恶意节点的存在，评价节点可能会得到虚假的推荐信息，此外，评价节点自身也可能是受环境的影响容易损坏，成为受损节点提供错误的信任值，因而直接信任值$DT_{i,j}^D(t)$的正确性也需要考虑。考虑到上述问题，利用证据距离度量法，对节点的直接信任和间接信任进行基于权重的修正，将直接信任值和间接信任值统称为分信任值。

将节点 i 收集到的节点 k (k=1,2,…,q)关于节点 j 的 q 个间接信任值$\boldsymbol{VIT}_{i,j}^k(t)=\vec{\boldsymbol{m}}^k=\left(m_{i,j}^k(\{T\}),m_{i,j}^k(\{T,-T\}),m_{i,j}^k(\{-T\})\right)$称为节点 i 关于节点j 综合信任的第 1,2, …,q 个分信任，并称节点 i 关于节点 j 的直接信任值$\boldsymbol{VDT}_{i,j}^D(t)=\vec{\boldsymbol{m}}^D=\left(m_{i,j}^D(\{T\}),m_{i,j}^D(\{T,-T\}),m_{i,j}^D(\{-T\})\right)$为第$q$+1 个分信任。利用证据距离公式，计算得到这 q+1 个分信任值两两之间的距离 $d_{u,v}$ (u, v=1,2,…,q+1)，表示任意两个证据之间的冲突程度。

$$d_{u,v}=\sqrt{\frac{1}{2}\left(\left\|\vec{\boldsymbol{m}}^u\right\|^2+\left\|\vec{\boldsymbol{m}}^v\right\|^2-2\left\langle\vec{\boldsymbol{m}}^u,\vec{\boldsymbol{m}}^v\right\rangle\right)} \quad (10)$$

式中：$\vec{\boldsymbol{m}}^u$ 和 $\vec{\boldsymbol{m}}^v$ 分别表示第 u 个和第 v 个分信任值向量，$\left\|\vec{\boldsymbol{m}}^u\right\|$和$\left\|\vec{\boldsymbol{m}}^v\right\|$分别为上述两个分信任值向量的模，$\left\langle\vec{\boldsymbol{m}}^u,\vec{\boldsymbol{m}}^v\right\rangle$为这两个分信任值向量的内积。

根据公式(10)就可以得到任意 2 个分信任值之间的相似度 $s_{u,v}=1-d_{u,v}$，即证据之间相互支持的程度，从而得到相似度矩阵 $\boldsymbol{S}$，如公式(11)所示。

$$\boldsymbol{S}=\begin{bmatrix} 1 & s_{1,2} & \cdots & s_{1,q+1} \\ s_{2,1} & 1 & \cdots & s_{2,q+1} \\ \vdots & \vdots & \vdots & \vdots \\ s_{q+1,1} & s_{q+1,2} & \cdots & 1 \end{bmatrix}_{(q+1)\times(q+1)} \quad (11)$$

根据 D-S 证据理论，如果一个证据和其他大多数证据相似度越高，相应地，其得到的支持程度也越高，即该证据对最终的融合结果会产生比较大的影响，也就是说证据的权值与所有其他证据对其综合支持度成正相关。因此，可以得到如下权重公式：

$$\chi_u=\sum_{v=1,u\neq v}^{q+1}s_{u,v}\Big/\sum_{u=1}^{q+1}\sum_{v=1,u\neq v}^{q+1}s_{u,v} \quad (12)$$

利用式(12)中权重，即可得到修正后的分信任值，如式(13)所示。

$$\begin{cases} m'_{u,j}(\{T\})=\chi_u m_{i,j}^u(\{T\}) \\ m'_{u,j}(\{T,-T\})=\chi_u m_{i,j}^u(\{T,-T\}) \\ m'_{u,j}(\{-T\})=\chi_u m_{i,j}^u(\{-T\}) \end{cases} \quad (13)$$

2.3.3 信任值的综合

基于修正后的直接信任和间接信任，并根据 Dempster 组合规则，节点 i 可以按照公式(14)对其进行融合，从而得到被评价节点j的综合信任值为：$\boldsymbol{VT}_{i,j}(t)=\left(m_{i,j}(\{T\}),m_{i,j}(\{T,-T\}),m_{i,j}(\{-T\})\right)$。

$$\begin{cases} m_{i,j}(A)=m'_{1,j}(A)\oplus m'_{2,j}(A)\oplus\cdots\oplus m'_{q+1,j}(A) \\ \qquad\qquad A\neq\Phi, A\subseteq\Omega \\ m_{i,j}(\Phi)=0 \end{cases} \quad (14)$$

如果节点j满足以下条件，即

$$\begin{cases} m_{i,j}(\{T\})-m_{i,j}(\{-T\})>\theta \\ m_{i,j}(\{T,-T\})<\delta \\ m_{i,j}(\{T\})>m_{i,j}(\{T,-T\}) \end{cases} \quad (15)$$

那么节点 i 就认为节点j是可信节点，否则，认为节点j是“不确定”或者“不可信”的节点，从而拒绝与其进行通信。

3 性能分析与仿真实现

3.1 安全性分析

针对网络固有攻击的分析：

(1) 冒充攻击。由于所有信任查询信息的响应信息 $ID_k \| ID_i \| K_{ik}(X_j, \varepsilon)$ 都是利用第三方节点 k 自身及评价节点 i 的共享密钥 K_{ik} 进行加密，攻击者无法获取该共享密钥，因而无法冒充正常节点响应信任查询信息，即不能发起冒充攻击。

(2) 重放攻击。重放攻击即当攻击者截获信任查询信息的响应信息后，过段时间就会重放该截获信息，从而干扰评价节点获得真正的被评估节点信任值。由于响应信息中 $ID_k \| ID_i \| K_{ik}\left(X_j, \varepsilon\right)$ 加入了时间戳 ε，当评价节点收到响应信息的时间戳与发送查询的时间戳不一致，就会丢弃该响应信息。

(3) 篡改攻击。由于响应信息 $ID_k \| ID_i \| K_{ik}(X_j, \varepsilon)$ 利用评价节点与响应节点的共享密钥 K_{ik} 进行加密，而攻击节点无法获取上述共享密钥，因而不能正确解析信息，从而导致其不能篡改信息内容，即不能发起篡改攻击。

(4) 节点背叛攻击。该攻击方式中由于节点具有合法身份，传统基于加密和认证机制的方法难以抵御这种攻击，但是信任管理机制可以根据节点行为来评价节点信誉，当其信任值低于某一预设阈值时，就会被自动隔离出网络。

针对信任模型自身脆弱性所带来攻击的分析：

(1) on-off 攻击。为抵御 on-off 攻击，本文在计算节点直接信任时考虑了历史信任的影响，并定义了自适应权重因子，能有效降低此类攻击的影响，及时识别出恶意节点并排除网络。

(2) bad-mouthing 攻击。只要考虑反馈信任，恶意节点就可能提供不诚实的反馈信任，来诋毁善意节点或鼓吹恶意节点，针对这一问题，本文采用证据距离度量法对信任进行基于权重的修正，分信任值与其他所有分信任的相似度越高，其得到的支持程度就越高，在信任融合中所占的比重就越大，从而有效削弱了恶意推荐对综合信任的影响。

3.2 实验仿真与结果

本文利用 NS2 作为仿真工具来分析本文所提信任模型的性能，具体仿真场景设置如下：100 个节点随机分布在 100m×100m 的正方形检测区域内，节点的通信半径为 20m，基站位于正方形检测区域的中心；设置恶意节点有 70%~100%的丢包率及数据包篡改率，并且向其他节点提供不真实的推荐信任；直接信任值更新周期 $\tau = 10\,\mathrm{s}$，$\beta_s = 0.3$，$\beta_l = 0.8$，$\theta = 0.3$，$\delta = 0.09$。

信任具有动态性，网络中的正常节点很容易被攻击者捕获而成为妥协节点发起恶意攻击危害网络，因此及时识别网络中的恶意节点至关重要；另一方面，恶意节点为达到发起攻击却不被发现的目的，往往会实施策略性攻击行为，即 on-off 攻击，这就要求信任模型具有良好的动态适应性，能快速准确地识别出节点的攻击行为。实验通过对恶意节点 on-off 攻击行为下的直接信任值进行采样来验证模型的动态适应性，采样周期 $T_s = 10\,\mathrm{s}$，采样结果如图 2 所示。网络运行初期恶意节点进行信任补偿以获取较好的信任评价，从第 21 个采用周期开始发起恶意攻击。从图中可以看出，信任补偿阶段 $m(\{T\})$ 缓慢增加，$m(\{T,-T\})$ 缓慢减少，一旦恶意节点发起攻击，$m(\{T\})$ 迅速减低，$m(\{T,-T\})$ 则迅速增加，换句话说，信任积累所需时间要远大于信任丧失所需时间，体现了信任“难以获得，容易丧失”的特点，因而能有效抵御恶意节点突然发起的攻击行为，即 on-off 攻击，及时识别出恶意节点并将其排除。

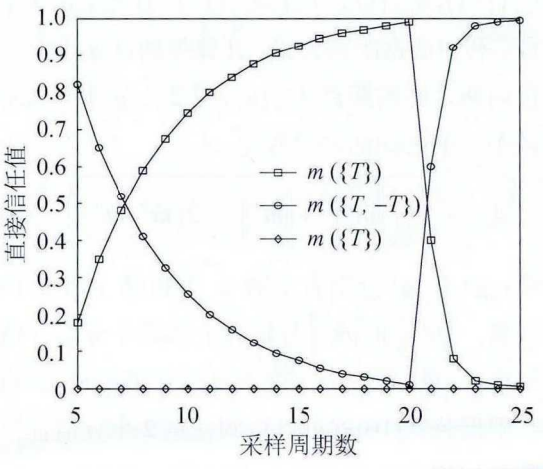

图 2 on-off 攻击下直接信任值变化

Fig. 2 The change of direct trust value under on-off attack

一旦在信任评估中考虑推荐信任即间接信任值，信任评估模型就会面临 bad-mouthing 攻击的威胁。为分析本文模型在抵御 bad-mouthing 攻击方面的性能，将本文模型与 RFSN、TMS 分别在两种情况下进行比较，即恶意节点诋毁正常节点和恶意节点鼓吹其恶意同伙，结果如图 3 和图 4 所示。

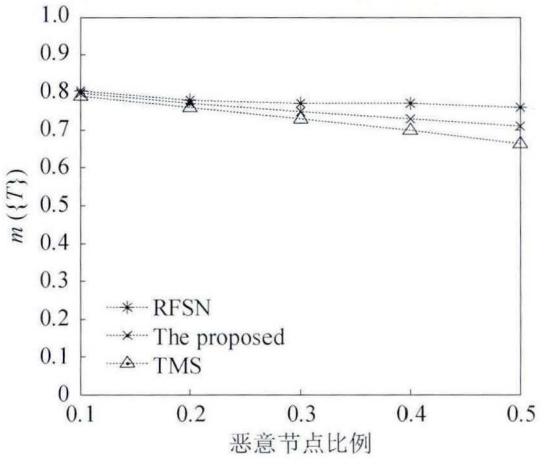

图 3　不同比例的恶意节点诋毁正常节点时的信任值
Fig. 3　The trust value at different proportion of malicious nodes when framing good nodes

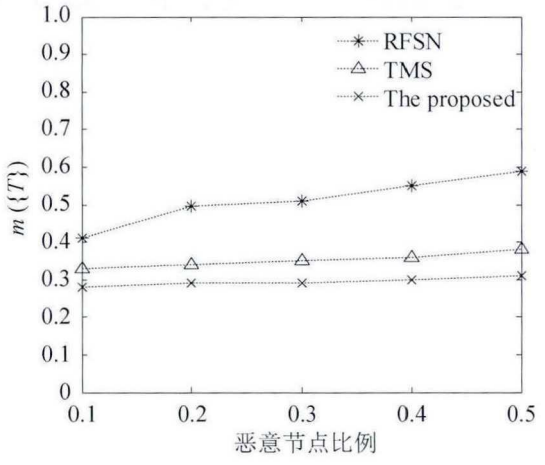

图 4　不同比例的恶意节点鼓吹恶意同伙时的信任值
Fig. 4　The trust value at different proportion of malicious nodes when boosting malicious peer

从图 3 可以看出，当恶意节点发起 bad-mouthing 攻击来诋毁正常节点时，RFSN 中节点信任值所受影响最小，这是因为在该方案中，节点只采纳关于其他节点的善意推荐，但是由此得到的信任往往不够全面，缺乏一定的客观性。此外，从图 4 可以看出，RFSN 方案也不能有效抑制恶意节点对其同伙的鼓吹。而本文方案无论在哪种情况下，其性能都略优于 TMS 方案，其主要原因在于本文方案在计算节点信任时，综合考虑了直接信任与间接信任，因而计算得到的节点信任值更为客观、准确，说明本文方案在抵御 bad-mouthing 攻击方面具有较好的鲁棒性。

为分析网络的安全性，将本文方案与 RFSN 及 TMS 在恶意节点检测率方面进行比较，不同信任机制下的恶意节点检测率如图 5 所示。显然，本文方案优于 RFSN 及 TMS，主要由以下几方面的因素决定。首先，引入模糊集合的概念，利用隶属度函数将信任表示为向量的形式，充分考虑了信任的不确定性及主观模糊性，而且避免了先验分布的主观假设，提高了信任评估的客观性；其次，综合考虑直接信任与间接信任，对其进行基于权重的修正，提高了信任值的准确性以及信任评估模型的鲁棒性；此外，利用 Dempster 组合规则进行信任值的综合，加快了信任评估的收敛速度。因此，本文所提的信任模型能及时、准确地识别恶意节点，提高网络的安全性。

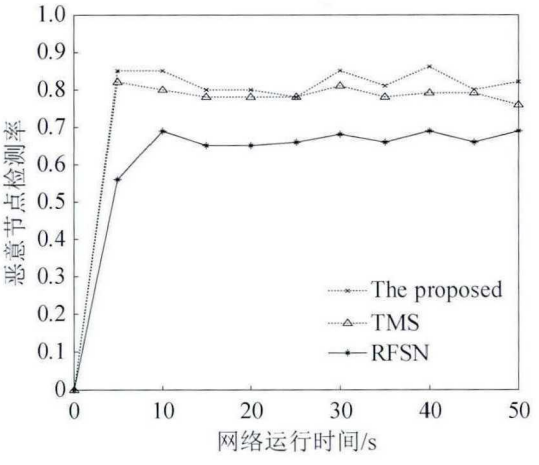

图 5　恶意节点检测率
Fig. 5　The proportions of detected malicious nodes

4　结论

结合模糊集合与 D-S 证据理论，本文提出一种安全的 WSN 信任评估模型。定义了 3 种典型信

任因子来计算节点直接信任，在保证节点信任值准确的前提下降低复杂度；利用模糊集合理论将节点信任进行模糊划分，将隶属度函数作为 D-S 证据理论中的基本置信度函数，融合直接信任与间接信任，具有良好的动态适应性及鲁棒性，能及时、准确地识别网络中的恶意节点，提高网络的安全性能。同时有效的结合基于身份的密码机制和信任管理机制，保证了信任信息在传递中的安全性。

参考文献：

[1] Yick J, Mukherjee B, Ghosal D. Wireless Sensor Network Survey[J]. Computer Networks (S1389-1286), 2008, 52(12): 2292-2330.

[2] Kumar V, Jain A, Barwal P N. Wireless Sensor Networks: Security Issues, Challenges and Solutions[J]. International Journal of Information & Computation Technology (S0974-2239), 2014, 4(8):859-868.

[3] Seo S H, Won J, Sultana S, et al. Effective key management in dynamic wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security (S1556-6013), 2015, 10(2): 371-383.

[4] Tahta U E, Sen S, Can A B. GenTrust: A genetic trust management model for peer-to-peer systems[J]. Applied Soft Computing (S1568-4946), 2015, 34: 693-704.

[5] Han G, Jiang J, Shu L, et al. Management and Applications of Trust in Wireless Sensor Networks: A Survey [J]. Journal of Computer and System Sciences (S0022-0000), 2014, 80(3): 602-617.

[6] Ishmanov F, Malik A S, Kim S W, et al. Trust Management System in Wireless Sensor Networks: Design Considerations and Research Challenges[J]. Transactions on Emerging Telecommunications Technologies (S2161-3915), 2015, 26(2): 107-130.

[7] Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based Framework for High Integrity Sensor Networks [J]. ACM Transactions on Sensor Networks (S1550-4859), 2008, 4(3): 15.

[8] 房卫东, 石志东, 单联海,等. 一种基于 BETA 分布抗 On-off 攻击的信任机制[J]. 系统仿真学报,2015, 27(11): 2722-2728.
Fang W D, Shi Z D, Shan L H, et al. Trusted Scheme for Defending On-Off Attack Based on BETA distribution[J]. Journal of System Simulation, 2015, 27(11): 2722-2728.

[9] Ishmanov F, Kim S W, Nam S Y. A Secure Trust Establishment Scheme for Wireless Sensor Networks [J]. Sensors (S1424-8220), 2014, 14(1): 1877-1897.

[10] Duan J, Gao D, Yang D, et al. An Energy-aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IOT Applications [J]. IEEE Internet of Things Journal, 2014, 1(1): 58-69.

[11] Che S, Feng R, Liang X, et al. A Lightweight Trust Management Based on Bayesian and Entropy for Wireless Sensor Networks [J]. Security and Communication Networks (S1939-0114), 2015, 8(2): 168-175.

[12] Jiang J, Han G, Wang F, et al. An Efficient Distributed Trust Model for Wireless Sensor Networks [J]. IEEE Transactions on Parallel and Distributed Systems (S1045-9219), 2015, 26(5): 1228-1237.

[13] 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.
Cheng J, Feng R J, Xu X F, et al. Trust evaluation model based on D-S evidence theory in wireless sensor networks[J]. Chinese Journal of sensor and actuators, 2009, 22(12): 1802-1807.

[14] Feng R, Che S, Wang X, et al. Trust Management Scheme Based on DS Evidence Theory for Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks (S1550-1329), 2013, 9(6): 1-9.

[15] 姚雷, 王东豪, 梁璇,等. 无线传感器网络多层次模糊信任模型研究[J]. 仪器仪表学报, 2014, 35(7): 1606-1613.
Yao L, Wang D H, Liang X, et al. Research on multi-level fuzzy trust model for wireless sensor networks[J]. Chinese Journal of Scientific Instrument, 2014, 35(7): 1606-1613.

[16] Wahid A, Kumar P. A Survey on Attacks, Challenges and Security Mechanisms in Wireless Sensor Network [J]. International Journal for Innovative Research in Science and Technology (S2349-6010), 2015, 1(8): 189-196.

[17] 吴银锋, 周翔, 冯仁剑,等. 基于节点信任值的无线传感器网络安全路由[J]. 仪器仪表学报, 2012, 33(1): 221-228.
Wu Y F, Zhou X, Feng R J, et al. Secure routing based on node trust value in wireless sensor networks[J]. Chinese Journal of Scientific Instrument, 2012, 33(1): 221-228.