一种分簇无线传感器网络多维节点信誉管理方案

房 方 李景峰 李 杰
(信息工程大学 郑州 450001)

摘 要 目前分簇无线传感器网络的节点信誉管理方案存在信誉值计算、更新及维护代价高,节点抗恶意哄抬及恶意抵毁能力弱等问题。将无线传感器节点分为簇头节点和普通传感器节点,将两类节点在事件感知、报文传输以及数据融合等方面的正常及异常行为作为评价基础,提出一种多维节点信誉管理方案。最后,将该方案和AOMDV反应式路由相结合,设计了一种基于节点可信的路由协议STA。仿真结果表明,该协议能够在不可信环境下实现分簇无线传感器网络中较高的数据传输率和传输成功率。

关键词 无线传感器网络,信誉,信任,感知,传输,融合
中图法分类号 TP301 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.07.033

Multidimensional Node Reputation Management Scheme for Clustered Wireless Sensor Networks

FANG Fang LI Jing-feng LI Jie
(Information Engineering University, Zhengzhou 450001, China)

Abstract At present there are problems in reputation management mechanism for wireless sensor networks (WSNs), such as high cost of calculation, update and maintenance of reputation, poor resistance to "bad mouthing" and "ballot stuffing". Taking the clustered wireless sensor network as the background, sensor nodes were divided into cluster head nodes and ordinary sensor nodes. According to the behaviors of sensor nodes on event perception, packet forwarding and data aggregation, a multidimensional node reputation management scheme was put forward. Applying the scheme to reactive multi-path routing protocol AOMDV, this paper proposed a reliable routing protocol called STA based on trusted nodes. The simulation results show that in distrusted environment, the proposed protocol improves the data forwarding rate and delivery success rate in WSNs.

Keywords Wireless sensor network, Reputation, Trust, Sensing, Delivery, Aggregation

无线传感器网络(WSN)是一种综合了传感器技术、嵌入式计算技术、分布式信息处理技术和无线通信技术的多跳自组织网络[1],可用于环境监测、军事目标追踪和灾难救援等。然而WSN中的节点一旦被敌方俘获,节点内部存储的密钥信息就可能被敌方获取,从而妥协成为恶意节点,通过发动内部攻击对网络安全造成危害。因此,如何尽早识别恶意节点,并及时将其排除在网络之外就显得尤为重要。

针对该问题,学者们提出使用信誉与信任管理方案来评估节点可信度,依据评估结果识别恶意节点,从而抵御内部攻击。文献[2,3]提出一种线性信任机制,其主要思想是利用线性函数或概率的方法来计算自组织网络中的节点可信度。Suat ozdemir[4]提出无线传感器网络中基于声誉的数据融合体系RDAT,但该方案缺少认证机制,且使用了间接信誉,对Sybil攻击、诽谤攻击等网络攻击抵抗力较差。Arnab Raha和Mrinal Kanti Naskar[5]等人仅考虑了节点的间接信誉值。Ganeriwal等人提出的RFSN模型[6,7],整合直接信誉值和间接信誉值得出综合信誉值,但其仅能够抵御由低信誉值节点发起的网络攻击,不能有效抵抗高信誉值节点的恶意诽谤和哄抬,且综合节点直接、间接信誉值的计算代价较大。杨光[8]等人指出S. Ganeriwal和M. B. Srivastava[6,7]提出的无线传感器网络信任模型存在缺陷,该模型可消除低信誉节点的恶意诋毁或推荐,无法消除高信誉节点的恶意诋毁或推荐,因此提出了节点恶意行为评测识别模型MA&TP-BRSN(multipleattacks&thirdparty-BRSN)。

综上所述,无线传感器网络中节点信誉管理机制主要存在以下问题:(1)间接信誉获取难以做到公平公正;(2)信誉值计算复杂,资源代价较高;(3)信誉值评估片面;(4)抗节点恶意诋毁或哄抬攻击能力差。针对上述问题,本文以单跳分簇无线传感器网络为背景,依据传感器节点在进行事件感知、报文传输以及数据融合时的正常或异常表现行为,提出了分簇无线传感器网络中一种多维节点信誉管理方案,详细描述了节点信誉值的初始化、更新和存储以及恶意节点的惩罚与救赎等关键步骤。将该信誉管理方案应用于现有的多径路由协议AOMDV[9],得到一种信任增强的新路由协议。STA仿真结果表明,该协议与RDAT[4]相比,在网络存在不可信节点的情况下有较好的数据传输率和传输成功率,在很大程度上提

到稿日期:2013-08-29 返修日期:2013-12-16 本文受郑州市科技攻关项目(0910SGYG211)资助。
房 方(1984-),女,硕士生,主要研究方向为无线传感器网络,E-mail:546230579@qq.com;李景峰(1977-),男,副教授,硕士生导师,主要研究方向为无线传感器网络和信息安全;李 杰(1987-),男,硕士生,主要研究方向为无线传感器网络。

高了网络整体性能。

1 网络拓扑结构设定

本节给出单跳分簇无线传感器网络的拓扑结构，如图 1 所示。

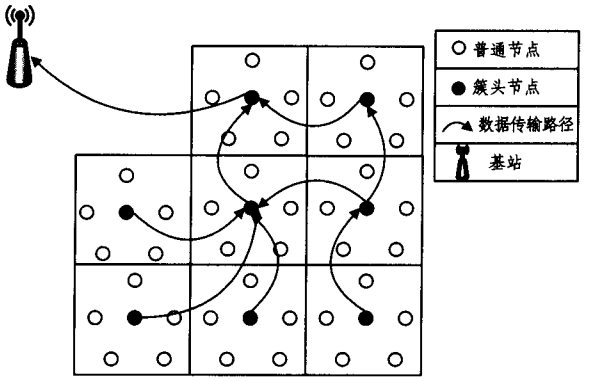

图 1 单跳分簇无线传感器网络拓扑结构

其中的重要概念解释如下：

(1)无线传感器网络被部署后，划分为若干个互不交叠的簇。每个簇由一个簇头节点和 n 个普通节点构成。簇头节点负责传输和融合数据，普通节点负责感应和传输数据。

(2)各簇规模足够小，每个节点具有全局唯一标识符，其传输范围可覆盖整个簇，簇内任意两节点均可单跳通信。相邻簇的簇头节点可直接传输报文。

2 多维节点信誉管理方案

本方案使用节点信誉值表征节点可信度，设计了多维节点信誉管理方案，通过对构成节点信誉值的信任因素进行分类，同时对信誉值计算方法进行改进，提高了节点信誉值评估的客观性和公正性。

2.1 信任维度选择

节点信誉值由直接信誉值和间接信誉值共同构成。由于本方案中各簇规模足够小，节点距离足够近，同一簇内任意两节点可实现单跳通信，因此在此仅考虑直接信誉值。

由于簇内节点的主要行为包括事件感知、报文传输和数据融合，因此选择与上述 3 种行为对应的信任因素来评估节点信誉值，分别称为感知信誉值(T_S)、传输信誉值(T_T)和融合信誉值(T_A)。

由于簇内普通节点只负责事件感知和数据传输，因此约定普通节点的信誉值由感知信誉值和传输信誉值构成，记为 $T_{SN}=T_S+T_T$。这里，T_S 和 T_T 由簇内普通节点和簇头节点共同进行评价。另外，由于簇头节点通常不负责事件感知任务，因此约定簇头节点的信誉值由融合信誉值和传输信誉值构成，记为 $T_{CH}=T_A+T_T$。这里，T_A 和 T_T 由与其发生过交互的相邻簇头节点进行评价。

2.2 节点信誉值初始化

本文提出的方案中，将节点的感知信誉、传输信誉及融合信誉的初始值均设为 0.5，即节点最初都为不确定节点。在无线自组网及无线传感器网络中恶意节点毕竟只占少数，对新加入节点的猜疑是导致整个系统性能不高的重要原因[10]，因此在证实新节点不可信之前将其设定为不确定节点会使系统更有效。我们用公式 $T=0.5+rt$ 来计算节点的各类信誉值，其中 rt 代表节点在最近一段时间内累积的信誉值，取值范围为(0,1)，则 T 的取值范围为(0.5,1.5)。若 $rt<0.5$，则此类信誉值不可信；若 $rt=0.5$，则此类信誉值不确定；若 $rt>0.5$，则此类信誉值可信(这里并不是指节点的总体信誉值，而是某一类信誉值，如传输信誉值)。节点信誉评价机制如图 2 所示。

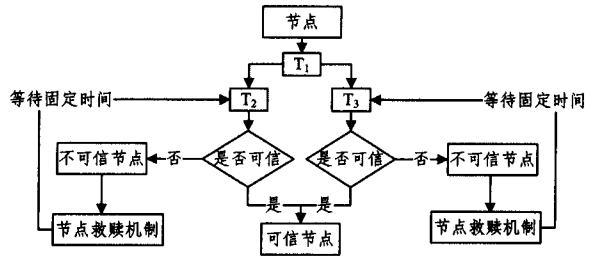

图 2 节点信誉评价机制

其中，T_1 为某类节点的总信誉值，T_2 和 T_3 则依节点类别分别代表了 2.1 节中所定义的感应信誉值、传输信誉值或融合信誉值。若节点为普通节点，T_2 和 T_3 取值为 T_S 和 T_T；若节点为簇头节点，T_2 和 T_3 取值为 T_A 和 T_T。当 $T_1\geqslant 2$ 时可能存在 T_2 和 T_3 一个大于 1、一个小于 1 的情况。一般认为，节点某一类信誉值极端小会直接导致该节点不可信，因此，当节点的某一类信誉值 $rt<0.5$ 时，则认为节点为不可信节点，并将该节点的总信誉值记为 $rt<0.5$，继而进行节点的惩罚与救赎。

以普通节点 T_{SN} 为例：$T_{SN}=T_S+T_T$，若 $T_{SN}<2$，则普通节点必为不可信节点；若 $T_{SN}=2$，则依某一类信誉值是否存在 $rt<0.5$ 的情况判断普通节点为不可信节点或不确定节点；若 $T_{SN}>2$，则依某一类信誉值是否存在 $rt<0.5$ 的情况判断普通节点为不可信节点或可信节点。以簇头节点 T_{CH} 为例：$T_{CH}=T_A+T_T$，若 $T_{CH}<2$，则簇头节点必为不可信节点；若 $T_{CH}=2$，则依某一类信誉值是否存在 $rt<0.5$ 的情况判断簇头节点为不可信节点或不确定节点；若 $T_{CH}>2$，则依某一类信誉值是否存在 $rt<0.5$ 的情况判断簇头节点为不可信节点或可信节点。

2.3 节点信誉值列表

为了方便节点在传输数据时选择可信度较高的下跳节点，普通节点在本地维护一张信誉值列表，用于保存簇内其他节点的信誉值；与此相对，簇头节点维护的信誉值列表除簇内其他节点的信誉值外，还需存储与之交互的其他簇头节点的融合信誉值及传输信誉值。

每个节点保存两类与信誉相关的信息：一类信息是节点信誉列表，包含相关节点的信誉值；另一类信息是不可信节点的黑名单。

2.4 节点信誉值的更新

以簇 C_a 为例，其普通节点 i 的信誉值表示为 $T_{C_{a_i}}$，包括感知信誉值 $T_S^{C_{a_i}}$，传输信誉值 $T_T^{C_{a_A i}}$。簇头节点 A 对 i 进行评价时，其感知信誉值表示为 $T_S^{C_{a_A i}}$，传输信誉值表示为 $T_T^{C_{a_A i}}$；簇内其他普通节点 j 对 i 进行评价时，其感知信誉值表示为 $T_S^{C_{a_j i}}$，传输信誉值表示为 $T_T^{C_{a_j i}}$，其中$(i,j=1,2,\cdots,n;i\neq j)$。

簇 C_a 中簇头节点 A 的信誉值表示为 $T_{C_{a_A}}$；包括融合信

誉值 $T_A^{C_{a_A}}$，传输信誉值 $T_T^{C_{a_A}}$。与簇 C_a 有过交互的相邻簇 C_b 的簇头节点 B 对簇头节点 A 进行评价的融合信誉值为 $T_A^{C_{a_{BA}}}$，传输信誉值为 $T_T^{C_{a_{BA}}}$。

节点的信誉值应该与节点每次完成网络活动的时刻以及节点参与网络活动的重要性有关，因此本文引入以下概念：

(1)节点参与网络活动的时间因素(u)：节点每次参与网络活动后都会计算一次信誉值，参与活动距离当前时刻越近，则信誉值越可信。设节点共参与 Q 次网络活动，其中任意一次活动记为 u。

(2)网络活动重要性(V)：我们将网络活动的重要性分为非常重要、重要和一般 3 个等级，分别用 3、2、1 来表示；节点参与的活动等级越高，其信誉值也就越高。

(3)每次完成网络活动后节点的信誉值($T_{C_{a_i}}^u$)：设簇 C_a 内普通节点 i 当前已参与过 Q 次网络活动，u 为任意一次，则第 u 次参与活动结束后，节点的信誉值表示为 $T_{C_{a_i}}^u$。

由于贝叶斯信誉系统在统计方面具有灵活性，其简易性适用于资源有限的无线传感器网络，且能成功识别异常行为节点[11]，因此本文采用 beta 信誉体系来计算节点的各类信誉值。

普通节点信誉值的更新：

由于 $T=0.5+rt$，故第 u 次参与活动结束后，普通节点 i 的信誉值可表示为：

$$T_{C_{a_i}}^u=\frac{(T_{S.u}^{C_{a_{Ai}}}+\sum_1^{n-1}T_{S.u}^{C_{a_{ji}}})+(T_{T.u}^{C_{a_{Ai}}}+\sum_1^{n-1}T_{T.u}^{C_{a_{ji}}})}{n}$$

$$=0.5+\frac{(rt_{S.u}^{C_{a_{Ai}}}+\sum_1^{n-1}rt_{S.u}^{C_{a_{ji}}})+(rt_{T.u}^{C_{a_{Ai}}}+\sum_1^{n-1}rt_{T.u}^{C_{a_{ji}}})}{n}$$

$$(i,j=1,2,\cdots,n;i\neq j) \tag{1}$$

若感知信誉值和传输信誉值至少有一类存在 $rt<0.5$ 的情况，则该节点不可信，不需要进行信誉值的综合计算，直接将其总信誉值记为信誉值最低的那类信誉值。

假设簇 C_a 内普通节点 i 已参与过 u 次网络活动，u 为任意一次，设

$$w^u=\frac{\lambda^u V^u}{\sum_{u=1}^{Q}\lambda^u V^u} \tag{2}$$

为节点参与第 u 次网络活动后 $T_{C_{a_i}}^u$ 在其最终信誉值中所占的比重，满足 $\sum_{u=1}^{Q}\lambda^u V^u=1$ 且 $\lambda^1<\cdots<\lambda^u<\cdots<\lambda^Q$，体现距离节点参与网络活动时间越近，其给出的信誉值越真实，所占的比重也就越大的原则，我们称 λ^u 为衰减因子，λ^u 的计算方法如下：

$$\lambda^u=t^u/\sum_{u=1}^{Q}t^u \tag{3}$$

其中，t^u 为节点 i 第 u 次参与网络活动所用的时间。

普通节点 i 第 u 次参与网络活动的重要性 V^u，分别按照上文给出的不同的重要性等级来评定。

综上所述，簇 C_a 内普通节点 i 完成 u 次网络活动时的信誉值，即当前信誉值为：

$$T_{C_{a_i}}=\sum_{u=1}^{Q}w^u T_{C_{a_i}}^u \tag{4}$$

综合普通节点的感知和传输两类因素，本文规定当 $T_{C_{a_i}}<2$ 时，普通节点 i 必为不可信节点；当 $T_{C_{a_i}}=2$ 时，依普通节点 i 中某一类信誉值是否存在 $rt<0.5$ 的情况判断节点为不可信节点或不确定节点；当 $T_{C_{a_i}}>2$ 时，依普通节点 i 中某一类信誉值是否存在 $rt<0.5$ 的情况判断节点为不可信节点或可信节点。

s 和 f 分别代表了节点进行感应、传输或融合的成功或失败的次数，其值均为正整数，无上限。对簇 C_a 中普通节点 i 来讲，节点 i 的感知行为是否良好，要基站通过用户反馈才能判定。若 $|d_i^{C_a}-d_{AVE}^{C_a}|\leqslant THR_S$（$d_i^{C_a}$ 和 $d_{AVE}^{C_a}$ 分别为簇 C_a 内普通节点 i 的感应值和 n 个普通节点传输的平均值，THR_S 为预先设定的感应数据门限值），则将节点 i 的数据 $d_i^{C_a}$ 直接上传给簇头节点 A，此时 $s_S^{C_{a_{ji}}}+1$，且 $s^{C_{a_{Ai}}}s+1$。否则，将数据 $d_i^{C_a}$ 加上 ID 标记后上传至簇头节点，直至基站。最后由基站通过用户反馈判断该值是否可信，若可信则将节点 i 的 ID 号发回簇内，这时 $s_S^{C_{a_{ji}}}+1$，且 $s_S^{C_{a_{Ai}}}+1$，否则 $f_S^{C_{a_{ji}}}+1$，且 $f_S^{C_{a_{Ai}}}+1$，这里$(i,j=1,2,\cdots,n;i\neq j)$。节点 i 的传输行为是否良好，与节点传输数据的丢包率以及节点是否进行正确的路由传输有关。本文规定若节点 i 的丢包率达到 50%，或节点 i 没有将数据正确上传给簇头节点 A，则 $f_T^{C_{a_{ji}}}+1$，且 $f_T^{C_{a_{Ai}}}+1$，否则 $s_T^{C_{a_{ji}}}+1$，且 $s_T^{C_{a_{Ai}}}+1$。

簇头节点信誉值的更新：

由于 $T=0.5+rt$，故第 u 次参与活动结束后，簇头节点 A 的信誉值可表示为：

$$T_{C_{a_A}}^u=\frac{\sum_1^N(T_{A.u}^{C_{a_{BA}}}+T_{T.u}^{C_{a_{BA}}})}{N}=0.5+\frac{\sum_1^N(rt_{A.u}^{C_{a_{BA}}}+rt_{T.u}^{C_{a_{BA}}})}{N} \tag{5}$$

若融合信誉值和传输信誉值至少有一类存在 $rt<0.5$ 的情况，则该节点不可信，不需要进行信誉值的综合计算，直接将其总信誉值记为信誉值最低的那类信誉值。

其中，B 为与簇 C_a 有关交互的相邻簇 C_b 的簇头节点，N 为参与簇头节点 A 信誉评价的相邻簇的总和。同理，簇头节点 A 共参与过 Q 次网络活动，其中 u 为任意一次，则簇头节点 A 完成 u 次网络活动后的信誉值

$$T_{C_{a_A}}=\sum_{u=1}^{Q}w^u T_{C_{a_A}}^u \tag{6}$$

因此，当 $T_{C_{a_A}}<2$ 时，簇头节点必为不可信节点；当 $T_{C_{a_A}}=2$ 时，依簇头节点中某一类信誉值是否存在 $rt<0.5$ 的情况判断簇头节点为不可信节点或不确定节点；当 $T_{C_{a_A}}>2$ 时，依簇头节点中某一类信誉值是否存在 $rt<0.5$ 的情况判断簇头节点为不可信节点或可信节点。

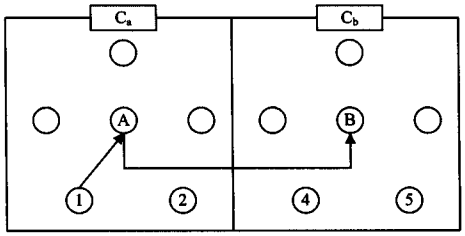

图 3　本簇及相邻簇的数据传输

对簇 C_a 中簇头节点 A 来讲，A 要上传其对簇 C_a 中各普通节点的融合值 $d_A^{C_a}$，及普通节点所感应的数据中的最大值 $d_{MAX}^{C_a}$ 与最小值 $d_{MIN}^{C_a}$。若 $d_{MIN}^{C_a}\leqslant d_A^{C_a}\leqslant d_{MAX}^{C_a}$，则将簇头节点 A

的融合值 $d_A^{C_a}$ 直接上传给其相邻簇的簇头节点 B，此时 $s_A^{C_aBA}+1$，否则 $f_A^{C_aBA}+1$。簇头节点 A 的传输行为是否良好，与节点转发融合数据的丢包率以及节点是否进行正确的路由传输有关。与普通节点的评价同理，我们约定若簇头节点 A 的丢包率达到 50%，或簇头节点 A 没有将数据正确上传给其下跳簇头节点 B，则 $f_T^{C_aBA}+1$，否则 $s_T^{C_aBA}+1$。

2.5 恶意节点的惩罚与救赎

对节点信誉值进行更新后，将其分为不可信、不确定和可信 3 个级别。可信节点将作为可信路由的选择路径，不确定节点则留待进一步观察。由于无线传感器网络节点众多，而且分布环境较为恶劣，故不能排除邻居节点检测有误或节点暂时失效的问题，因此给予不可信节点二次机会较为合理。发现不可信节点后并不立即将其排除出网络，而是经过一段时间的观察后再让其重新加入网络，使其有机会再次参与网络活动。当某节点被认为是不可信节点时，将其标记为 1，同时启动时钟，设定一个时间 T_0，在该段时间内禁止其加入网络，过了 T_0 其信誉值恢复为初始值，标记为 0。下一次若再次发现该节点不可信，则重复以上步骤，将时间变为 $2T_0$，不合作的次数越多，等待的时间越长，直到把其列入黑名单，最终排除出网络。因此，各节点除保存一份相关节点的信誉值列表外，还保存一份被排除出网络的节点黑名单，以便在进行路由选择时更加快速、有效。

3 信誉管理方案的应用

为了验证本文提出的节点信誉管理方案在识别网络内部不可信节点方面的有效性，我们将该信誉管理方案应用于现有的多径路由协议 AOMDV，得到一种基于节点可信的路由协议 STA。

3.1 AOMDV 协议

AOMDV 多径路由协议因采用跳数最少原则进行路由选择，故多用于能量受限的移动自组网和无线传感器网络。该协议主要包括两个阶段：路由发现和路由维护，这里主要是指路由建立过程中对簇的选择和维护，综合考虑传输路径中路由响应时间及节点的信任度。图 4 示出某时刻数据传输的路由场景：在 STA 路由协议中，源节点所在的簇 C_S 将数据传至目的节点所在簇 C_D，有两条路径可选：1) $C_S \rightarrow C_d \rightarrow C_D$；2) $C_S \rightarrow C_a \rightarrow C_b \rightarrow C_c \rightarrow C_D$。源节点依据收到的路由响应时间来决定使用哪条路径进行数据传输，由于前者路由响应时间较短，且传输路径中的簇个数少，传输过程较为节能，因此应选择该路径进行数据传输，但实际上由于簇 C_d 中不可信节点的存在，造成数据被篡改、数据传输率或传输成功率不高，因此应选择数据可信度、数据传输率或传输成功率较高的后者进行路由传输。

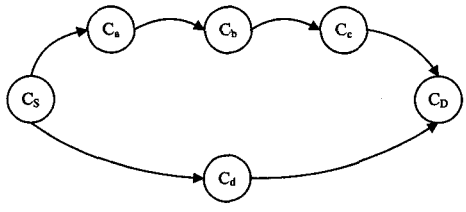

图 4 路由场景

AOMDV 多径路由协议在路由发现的初始化过程中通过在无线传感器网络中洪泛发送路由请求 RREQ 找到目的节点，之后沿着反向路径发送路由回复 RREP，由于最先到达源节点的路由回复 RREP 跳数少、延时短，因此将该路径作为主路径来发送数据，将第二个到达源节点的路由回复 RREP 作为备用路径来发送数据。本文将所提的多维节点信誉管理方案用于 AOMDV 协议，形成基于节点可信的多径路由协议 STA。节点在发送 RREQ 的过程中即根据其存储的邻居节点信誉值列表选择信誉度高于阈值的可信节点进行洪泛传输，并结合路由回复 RREP 的到达时间综合选择主路径和备用路径，对于不可信节点则不向其传输数据。若所有发送 RREQ 的邻节点均未与源节点进行过交互，则将其按初始值进行赋值。同理，依次建立传输路径直至目的节点，最终建立一主一辅两条可信的数据传输路径。

在路由的维护阶段，节点每次完成网络活动后都会引起信誉值的改变，因此及时完成节点信誉值的更新，将不可信节点排除在网络之外是路由维护的重要内容之一。同时，该阶段也将及时识别不能参与网络活动的低能量节点，以免因单个节点失效造成网络连接不畅。

3.2 仿真实验

利用 NS-2 软件构建了仿真实验环境，仿真参数说明如表 1 所列。

表 1 仿真参数说明

仿真参数	值
仿真时间	900s
初始化时间	900s 的前 200s
簇内节点数	N=(n+1) * 簇个数
网络中节点个数最大值	1000
不可信节点比率	30%
源/目的节点对数	20%N
源数据模式/节点	1packet/s
运行场景	1800m * 800m
节点感知半径	15m

无线传感器网络部署到检测区域后，全网被划分为若干个互不交叠的簇，簇内任意两节点均可单跳通信。每个簇由一个簇头节点和 n 个普通节点构成。各簇规模足够小，每个节点具有全局唯一标识符，且其传输范围可覆盖整个簇。运行场景的拓扑大小为 1800m * 800m，节点的感应范围为 15m，簇内节点个数从 10 至 100。仿真运行时间为 900s，其中前 200s 为初始化时间。

我们将 STA 协议与文献[4]提出的基于 RDAT 信誉机制的可信路由协议进行对比，选择全网数据传输率、数据传输成功率作为进行比较的协议性能指标。仿真结果如图 5、图 6 所示。

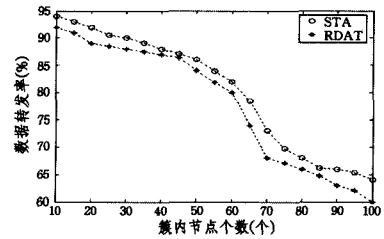

图 5 数据转发率

图 5 表示：当网络中不可信节点比率为 30%时，随着簇

内节点个数的增多，数据的传输率在两种方案下都是逐渐降低的，当簇内节点个数在 40～70 之间时下降较为明显，这是由于节点个数增多造成的路由交叉或重叠妨碍了节点的正常传输。当网络中节点传输受阻时，即使节点传输了数据，其邻居节点仍无法监听到正常的数据传输，从而导致节点评估信誉值的正确性有所下降，但是当簇内节点个数为 100 时，STA 方案中数据传输率仍比 RDAT 略高。

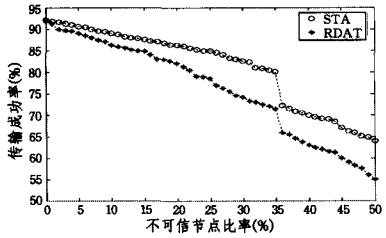

图 6　传输成功率

图 6 表示：设网络中没有不可信节点时，两种协议中数据的传输成功率约为 93%，随着网络内部不可信节点比率的升高，两种协议中数据的传输成功率均有所降低，当不可信节点比率为 15%时，RDAT 协议的传输成功率有明显的下降；当不可信节点比率为 35%时，STA 协议的传输成功率才明显下降为 82.3%，而此时 RDAT 协议则降为 68.8%，且整个过程中，STA 协议始终保持传输成功率高于 RDAT 协议。

3.3　性能分析

该方案从感应、传输和融合 3 个维度考虑，分别针对簇头节点和普通节点进行评估，综合考虑了节点的信誉值，从而更为全面、细致地了解了节点信誉。

该方案所得出的节点信誉值是局部信誉值，仅保存在本簇的簇头节点、普通节点或其邻簇的簇头节点内。通过与 RDAT 对比得出，当存在不可信节点时数据传输率和传输成功率在 STA 协议中都有所提高，STA 协议在提高整个网络性能上的优势更为明显。同时，节点的信誉评价值加入了用户的反馈，可以适应不同用户对安全性的要求，具有一定的 QoS 保证。

每簇由基站分配两类密钥：一类是簇内密钥 k_{C_a}，由簇 C_a 内所有节点所持有，用于簇内普通节点之间相互监听上传给簇头节点的感应数据，同时防止簇外节点干扰本簇内的数据传输及融合；另一类是簇间密钥 $k_{C_{ab}}$，由相邻簇（设为 C_a 与 C_b）的簇内节点所持有，用于簇间上传数据给下跳簇头节点时形成消息验证码 MAC，以便对上一跳的簇内融合数据进行验证。此外，这两类密钥的使用都是临时的，节点开始一次新的网络活动会重新分配新密钥，保证了节点传输过程的可认证性及安全性。

对于不可信节点，该方案给予二次机会制。由于无线传感器网络节点众多、网络拓扑动态变化且部署环境恶劣，为避免链路问题等造成的节点行为错误，给这些节点再次参与网络活动的机会，我们采用二次机会制。

结束语　在无线传感器网络中，节点的信誉问题已经引起了广泛的关注，成为无线网络和移动网络的一个重大挑战。本文以单跳分簇无线传感器网络为背景，将传感器节点在事件感知、报文传输以及数据融合这 3 方面的行为作为构建节点信誉机制的基本参考维度，提出了一种分簇无线传感器网络多维节点信誉管理方案，详细描述了节点信誉值初始化、信誉值更新、信誉值存储以及恶意节点惩罚与救赎等主要步骤。将本方案应用于现有的 AOMDV 多径路由协议得出了新的基于节点可信的路由协议 STA。实验证明，STA 协议在簇内节点增多、网络不可信节点比率增大的情况下较大地提高了数据传输率和传输成功率，在很大程度上提升了网络的整体性能。

参 考 文 献

[1] 杨庚，陈伟，曹晓梅. 无线传感器网络安全[M]. 北京：科学出版社，2010

[2] Carruthers R, Nikolaidis I. Certain limitations of reputation-based schemes in mobile environments[C]// Proc of the 8th ACM international symposium Symposium on MSWiM. 2005:2-11

[3] Sen J, Chowdhury P R, Senfupta I. A Distributed Trust Establishment Scheme for Mobile Ad hoc Networkss[C]// Proc of International Conference on Computing: Theory and Applications. 2007:51-58

[4] Ozdemir S. Functional reputation based data aggregation for wireless sensor networks[C]// Proc of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. Avignon, France, 2008:592-597

[5] Raha A, Naskar M K, Chakraborty A. A Novel Indirect Trust based Link State Routing Scheme using a Robust Route Trust Method for Wireless Sensor Networks[C]// Proc of International Conference on Mobility and Security. Istanbul, Turkey, May 2012:1-5

[6] Ganeriwal S, Srivastava M. Reputation based framework for high integrity sensor networks[C]// Proc of the 2nd ACM Workshop on Security of Ad hoc and Sensor networks. Washington D C, 2004:66-77

[7] Ganeriwal S, Balzano L K, Srivastava M. Reputation based frame-work for high integrity sensor networks[J]. ACM Transactions on Sensor Networks, 2008, 4(3):1-37

[8] 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

[9] Marina M K, Das S R. On demand multipath distance vector routing for ad hoc networks[C]// Proceedings of IEEE International Conference on Network Protocols. Vancouver, Canada: IEEE Computer Society Press, 2001:14-23

[10] Frideman E, Resnick P. The social cost of cheap pseudonyms [J]. Journal of Economics and Management Strategy, 2001, 10 (2):177-199

[11] Hani A. Secure data aggregation in wireless sensor networks [D]. Queensland University, 2011