doi:10.11959/j.issn.1000-436x.2017198

基于信任感知的无线传感器网络安全路由机制研究

秦丹阳[1]，贾爽[2]，杨松祥[1]，马静雅[1]，张岩[1]，丁群[1]
（1. 黑龙江大学黑龙江省电子工程重点实验室，黑龙江 哈尔滨 150080；
2. 哈尔滨工业大学通信技术研究所，黑龙江 哈尔滨 150001）

摘 要：针对无线传感器网络节点能量受限及部署环境恶劣所导致的典型网络攻击对数据安全带来的严重影响，提出了一种具有轻量级特性并能同时抵御多种典型网络攻击的信任感知安全路由机制（TSSRM）。在深入分析网络攻击特点的基础上，从节点行为维度与能量维度构建了综合节点信任度计算模型，通过对多项 QoS 指标量化，实现安全路径选择算法的优化。性能分析与仿真结果表明，TSSRM 可以同时实现无线传感器网络的安全性和高效性。
关键词：无线传感器网络；最优路径；安全路由；QoS 度量；信任度
中图分类号：TN915.81 **文献标识码**：A

Research on trust sensing based secure routing mechanism for wireless sensor network

QIN Dan-yang[1], JIA Shuang[2], YANG Song-xiang[1], MA Jing-ya[1], ZHANG Yan[1], DING Qun[1]
(1. Key Lab of Electronic and Communication Engineering, Heilongjiang University, Harbin 150080, China;
2. Communicate Research Center, Harbin Institute of Technology, Harbin 150001, China)

Abstract: Aiming at the serious impact of the typical network attacks caused by the limited energy and the poor deployment environment of wireless sensor network (WSN) on data transmission, a trust sensing based secure routing mechanism (TSSRM) with the lightweight characteristics and the ability to resist many common attacks simultaneously was proposed. Based on the analysis of the characteristics of network attack, the trust degree calculation model was constructed by combining node's behavior with energy, at the same time the security route selection algorithm was also optimized by taking trust degree and QoS metrics into account. Performance analysis and simulation results show that TSSRM can improve the security and effectiveness of WSN.
Key words: wireless sensor network, optimal route, secure routing, QoS metrics, trust degree

1 引言

物联网（IoT）的快速发展不断推动云计算、社交网络和智慧城市的构建。依赖不同类型分布式智能设备的智慧城市可以为城镇居民提供范围环境监测、交通管理以及社会娱乐等广泛的应用[1]。由于低成本、快速部署和自组织的特性，无线传感器网络（WSN）在促进智慧城市的各种服务中起到了至关重要的作用。无处不在的传感器节点既可以收集城市环境的物理信息，又可以在智慧城市环境的背景下控制公共和私人设施[2]。然而，无线传感器网络的开放、分布式和动态特性使多跳路由非常容易受到各种类型的攻击[3]，从而对数据与信息安全带来严重影响。目前已有的安全路由算法往往针对特定的恶意或自私行为攻击，由于其主要依靠加密算法和认证机制，因此并不适用于多跳分布式且

收稿日期：2017-04-18；**修回日期**：2017-09-07
通信作者：秦丹阳，qindanyang@hlju.edu.cn
基金项目：国家自然科学基金资助项目(No.61771186, No.61571181)；黑龙江省自然科学基金资助项目(No.QC2013C061);黑龙江省博士后科研启动基金资助项目(No.LBH-Q15121)；黑龙江大学研究生创新科研基金资助项目(No.YJSCX2016-019HLJU)
Foundation Items: The National Natural Science Foundation of China (No.61771186, No.61571181), The Natural Science Foundation of Heilongjiang Province (No.QC2013C061), The Postdoctoral Research Foundation of Heilongjiang Province (No.LBH-Q15121), The Postgraduate Innovation Research Foundation of Heilongjiang University (No.YJSCX2016-019HLJU)

能量受限的无线传感器网络。

研究表明，信任管理是保证网络路由安全性较为有效的手段。然而，传统的信任感知路由协议存在一定的局限性，主要体现在路由开销和传输时延较大，以及很难确保多跳信息传输的安全性[4]。本文面向 WSN 提出了一种新的信任感知安全路由机制（TSSRM）用于解决网络开销与多跳传输信息安全保障的问题。此外，TSSRM 不仅可以提高网络的安全性能，还具有轻量级特性，尽管引入安全机制来保护数据传输必将产生不可避免的开销；然而，本文所提安全机制的开销比其他采用加密算法的路由方案要少得多。直接信任度、推荐信任度和激励因子的计算也确实会产生相对较大的开销，从而导致节点的开销在某个时刻可能会比较大，但是 WSN 处于监听和睡眠 2 种状态，开销并不处于信息一直进行收发的极端状态，因此，从广域部署的整体平均时刻角度来说，这些开销是可以接受的。同时，攻击的不可预测性是现实世界中的一个主要问题，泛在路由算法在一定程度上不如针对某一种攻击的特定算法好，但是考虑到网络中可能存在多种攻击，本文提出了一种面向泛在环境的安全路由算法以抵抗 WSN 中的多种典型攻击。仿真结果表明，TSSRM 在提高多跳通信网络信息安全性的同时能够有效减小 WSN 中的路由开销。

2　典型网络攻击分析

网络攻击采用的方式和对象不尽相同，本节将分析无线传感器网络中的几种典型网络攻击，并提取其攻击特征，从而为 WSN 的安全保证提供支撑。

网络攻击根据攻击对象不同可以分为路由协议攻击与信任模型攻击。多跳中继的传输方式使路由协议攻击对无线传感器网络造成的危害远大于一般无线通信网络。通常，根据攻击者行为的不同，路由协议攻击可以分为软性攻击和硬性攻击。软性攻击是指恶意节点或自私节点通过伪装或欺骗虚构路径，窃取或破坏中继数据[5]，例如，在路由请求中加入虚假可用信道信息的黑洞攻击、故意丢弃部分数据的灰洞攻击、虚构本地资源的槽洞攻击、通过合谋构建虚假链路的虫洞攻击、通过分析网络流量的嗅探攻击，以及从事多身份伪造的女巫攻击等。硬性攻击是指恶意节点通过破坏现有传输资源从而破坏信息传输的行为[6]，如耗尽被攻击对象资源的 DoS 攻击、篡改路由数据的篡改攻击以及恶意占用带宽的重放攻击等。

虽然信任管理系统通过加密或信用机制可以在一定程度上解决针对路由的部分攻击，但同时也成为新的攻击目标[7]，目前，典型的信任模型攻击包括开关攻击、冲突行为攻击、自私攻击、诽谤攻击以及合谋攻击等[8]。此外，无线通信网络中普遍采用的信任管理算法并不具有普适性，且所引入的大量开销也使其难以直接应用于资源受限的无线传感器网络中[9]。为此，本文所提轻量级安全路由机制将通过行为与能量构建信任度，并结合 QoS 设计路由指标，以较低的开销同时抵御多种典型攻击。此外，女巫攻击和嗅探攻击难以通过基于信任的机制来检测，但是，管理人员可以通过 TSSRM 的监测发现一些异常信息进而发出警告，因此，尽管 TSSRM 无法抵抗这 2 种攻击，但会发挥一定的警示作用。

3　WSN 的信任模型与度量设计

3.1　信任模型的构建

信任检测过程中采用看门狗来检测路由中的恶意行为[10, 11]，传感器节点间相互信任检测的结果作为信任计算依据，$td(x,y)$ 表示被评估节点 y 对于评估节点 x 的信任度。考虑到 WSN 的节点数量较多且服从随机分布，其部署区域传输条件相对恶劣，因此，研究中采用直接信任度、推荐信任度与激励因子相结合的方法对节点的行为进行客观而全面的评价。其中，直接信任度是基于参与数据通信的每个节点的直接观察，而推荐信任度则是没有直接相互作用的分布式节点之间的信任关系。

3.2　信任度计算模型的建立

信任度是信任关系评价的重要依据，本节将采用层次分析法分析并建立信任度计算模型。

3.2.1　节点的直接信任度计算

WSN 中传感器节点的行为往往由邻居节点进行检测，但节点资源受限的本质使该传统方式难以准确判断邻居的可信程度[12]，为此，本研究将结合行为与能量对节点信任度进行综合评价。

1)节点的直接行为信任分析

直接行为信任是基于参与数据传输的每个节点的直接检测，本文给出一种轻量级的量化计算方法，用以评价 WSN 中节点的直接行为信任度为

$$dtd(x,y)^{l}=\omega_1\cdot dtd_{P(y)}(x,y)^{l-1}+\omega_2\cdot dtd_{N(y)}(x,y)^{l-1}+ift(x,y)^{l} \quad (1)$$

其中，$dtd_{P(y)}(x,y)^{l-1}$ 表示节点 x 基于节点 y 过去的正常行为检测所得的节点 y 的信任度。l 表示评价记录的顺序号。$dtd_{N(y)}(x,y)^{l-1}$ 表示节点 x 基于节点 y 过去的恶意行为检测所得节点 y 的信任度。ω_1 和 ω_2 分别对应于正面和负面评价的指数衰减时间因子；$ift(x,y)^{l}$ 表示通过入侵检测对节点 y 的当前行为进行评估的量化值[13]，如式(2)所示。

$$ift(x,y)=\begin{cases}P(y), & 0<P(y)<1\\ 0, & \text{不确定}\\ N(y), & -1<N(y)<0\end{cases} \quad (2)$$

其中，$P(y)$ 和 $N(y)$ 分别表示节点 y 行为的正面和负面评估值。当估计值处于模糊状态，节点行为判断将不再准确，故此时将 $ift(\cdot)$ 的值设置为 0。

开关攻击是信任攻击中最普遍的方式，为此，将式(1)中固定的衰减因子 ω_1 和 ω_2 自适应化，即 $\omega_1=\mathrm{e}^{-\rho_1(t_c-t_{c-1})}$，$\omega_2=\mathrm{e}^{-\rho_2(t_c-t_{c-1})}$，其中，$t_c$ 和 t_{c-1} 分别表示当前时间和前一次交互时间，ρ_1 和 ρ_2 分别表示正面和负面评价的指数衰减强度，且满足 $t_c>t_{c-1}\geqslant 0$，$\rho_1>\rho_2\geqslant 0$。由此看出，直接行为信任度 $dtd(x,y)^{l}$ 将随 t 的增加而减小。当 $\omega\to 0$ 时，即近次交互结果比前次交互结果更加重要。由于在实际环境中，开关攻击节点往往表现时好时坏用以获得更高的信誉。此时，通过衰减因子自适应调整，降低节点正常行为 ω_1 值，提高节点恶意行为 ω_2 值，从而保证恶意行为记录时间长于正常行为记录时间。

2)节点的直接能量信任分析

在传统安全模型中，网络中节点将选择高信任度的节点作为中继进行信息转发，这加剧了高信任度节点能量的消耗，从而引起网络负载不均匀甚至出现网络分割的现象。因此，所构建的计算模型将增加能量信任作为信任度的衡量维度。节点 y 在收、发信息过程中消耗的能量分别如式(3)和式(4)所示[14]。

$$Receiving\_Cost(k,d)=Eelec\cdot k \quad (3)$$

$$Sending\_Cost(k,d)=Eelec\cdot k+Eamp\cdot kd^{2} \quad (4)$$

其中，k 为收发分组比特数，d 为节点 x 与节点 y 之间的距离，$Eelec$ 为节点 y 传输数据时的单位比特能耗，$Eamp$ 为传输过程中为达到一定信噪比所消耗的能量，$Eelec$ 和 $Eamp$ 在本文中是预设的。

因此，节点 y 进行数据转发时总的能耗 EC 为

$$EC=2Eelec\cdot k+Eamp\cdot kd^{2} \quad (5)$$

若网络节点初始能量为 EB，则节点 y 剩余能量 ES 为

$$ES=EB-EC \quad (6)$$

当节点的剩余能量 ES 达到能量信任阈值 E_{th}，则说明该节点有能力合作，为能量可信节点；否则，无论该节点行为信任度多高，也无法参加信息传输。由此，定义节点 y 的能量信任度 ET_y 为

$$ET_y=\begin{cases}1, & ES\geqslant E_{\text{th}}\\ 0, & ES<E_{\text{th}}\end{cases} \quad (7)$$

网络节点的直接信任度 $s\_dtd(x,y)^{l}$ 计算模型将同时考虑节点的行为信任与能量信任，如式(8)所示。

$$s\_dtd(x,y)^{l}=\frac{1}{2}\omega_1\cdot dtd_{P(y)}(x,y)^{l-1}+\frac{1}{2}\omega_2\cdot dtd_{N(y)}(x,y)^{l-1}+\frac{1}{2}ift(x,y)^{l}+\frac{1}{2}ET_y \quad (8)$$

由于节点的行为和能量对信任度的计算同等重要，所以，在本文中，不考虑特殊应用情况时，$itd(x,y)^{l}$ 和 ET_y 的权重被均等分配，然而，在实际应用中，$itd(x,y)^{l}$ 和 ET_y 的权重可以根据实际情况进行适当调整。

3.2.2 节点的推荐信任度计算

推荐信任是目标节点连通域中其他邻居提供的信任关系。与直接信任度构建模型类似，推荐信任度也由推荐行为信任度与推荐能量信任度构成。由于能量为客观参量，因此，推荐能量信任度与直接能量信任度相同。这里只需考虑节点的推荐行为信任度。若网络中目标节点 y 的直接连通域为 C_y，$itd(x,y)^{l}$ 表示节点 x 根据 C_y 内所有节点提供的推荐信息计算得到的间接推荐信任度，如式(9)所示。

$$itd(x,y)^{l}=\frac{\sum_{z\in C_y,z\neq x}\left(dtd(x,z)^{l}\cdot dtd(z,y)^{l}\right)}{n-1} \quad (9)$$

其中，n 表示邻居节点数量，考虑到诽谤攻击与合

谋攻击可以避开直接信任度的检查，故有必要对 C_y 内所有节点提供的推荐信息进行校验。节点 x 对于目标节点 y 的相异性校验度 $cs(x,y)^l$ 为

$$cs(x,y)^l=\frac{itd(x,y)^l+dtd(x,y)^l}{\sum_{z\in C_y,z\neq x}dtd(x,z)^l+1} \tag{10}$$

对于目标节点 y 直接连通域中任意邻居节点 z，有 $\left|dtd(z,y)^l-cs(x,y)^l\right|>\delta$，则该节点 z 的推荐信息将不被节点 x 采纳。相异校验阈值 δ 为与具体网络环境和信息相关的既定值。由此，可以检测出可信任的节点集合中的恶意节点进而将其所提供的虚假推荐从网络中排除。

与直接信任度的计算类似，节点 x 获得关于目标节点 y 的推荐信任度为

$$\begin{aligned}s\_itd(x,y)^l&=\frac{1}{2}itd(x,y)^l+\frac{1}{2}ET_y\\&=\frac{1}{2}\frac{\sum_{z\in C_y,z\neq x}\left(dtd(x,z)^l\cdot dtd(z,y)^l\right)}{n-1}+\frac{1}{2}ET_y\end{aligned} \tag{11}$$

其中，$itd(x,y)^l$ 和 ET_y 的权重被均等分配，如式(11)所示。

3.2.3　激励因子的设计

考虑到 WSN 中的节点能量有限性以及恶意节点攻击的易受性，本文建立激励机制，在鼓励节点参与合作的同时对恶意节点进行惩罚。由于信息交互具有时效性，定义最大有效历史记录时间 τ，并根据 τ 内节点间的交互定义激励因子。由于激励因子 e_{xy} 最终用于解决二值问题，因此采用 0-1 分布，即伯努利分布进行模型构建为

$$e_{xy}=1-\frac{F_{xy}^{\tau}}{F_{xy}^{\tau}+S_{xy}^{\tau}} \tag{12}$$

其中，S_{xy}^{τ} 和 F_{xy}^{τ} 分别为最大有效历史记录时间 τ 内直接交互成功和失败次数。

3.2.4　基于 AHP 的信任度计算模型

结合节点的直接信任、推荐信任以及激励因子，使用层次分析法（AHP, analytic hierarchy process）建立了综合信任度的计算模型，如图 1 所示。

AHP 是将与决策总是有关的元素分解成目标、准则、方案等层次，在此基础之上进行定性和定量分析的决策方法。本文引用 AHP 的 1~9 标度法以计算每个信任度影响因素的权重，如表 1 所示。

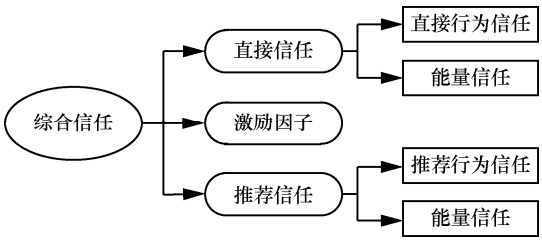


图 1　基于 AHP 的信任模型

表 1　　AHP 的 1~9 标度法

标度	2 个因素相互比较
1	具有相同的重要性
3	一个因素比另一个因素稍微重要
5	一个因素比另一个因素明显重要
7	一个因素比另一个因素强烈重要
9	一个因素比另一个因素极端重要

基于 WSN 资源受限的本质，本文提出了一种轻量级的信任度计算方法，目标节点 y 对于节点 x 的综合信任度 $td(x,y)^l$ 为

$$td(x,y)^l=\alpha\cdot s\_dtd(x,y)^l+\beta\cdot s\_itd(x,y)^l+\gamma\cdot e_{xy} \tag{13}$$

其中，α、β 和 γ 是与安全策略相关的权衡因素，且满足 $\alpha+\beta+\gamma=1$，$\alpha,\beta,\gamma>0$。采用 AHP 的 1~9 标度法可以求得[15]：$\alpha=0.698\,6$，$\beta=0.237\,0$，$\gamma=0.064\,4$。综合信任度 $td(x,y)^l$ 满足[0,1]，越高的 td 值表明节点越值得信任。

3.3　路径的信任度计算

为了不失一般性，所给出的路径信任度计算模型将不区分 WSN 所采用的路由算法。当网络中的节点根据所采用的路由协议完成路由发现过程后，将不会直接选定路径并进入信息发送阶段，而是先计算该路径的信任度。一般来说，路径的信任度计算应满足以下规律[16]：1) 信任度不会随信息多跳传播而增加；2) 目的节点为可信节点且初始信任度设置为 1。由此，对于节点 x 与其下游节点 y 间的单跳链路 r 的信任度 $td(r)$为

$$td(r)=\prod\left(\left\{td(x,y)\middle|x,y\in r,x\to y\right\}\right) \tag{14}$$

WSN 中任意源节点到目的节点的路径往往由多条链路构成，其信任度计算模型如图 2 所示，n_0 和 n_7 分别为源节点和目的节点。从 n_0 到 n_7 共存在 5 条路径，其信任度分别为 $td(n_0,n_1,n_2,n_3,n_7)=0.72$、$td(n_0,n_1,n_2,n_6,n_7)=0.63$、

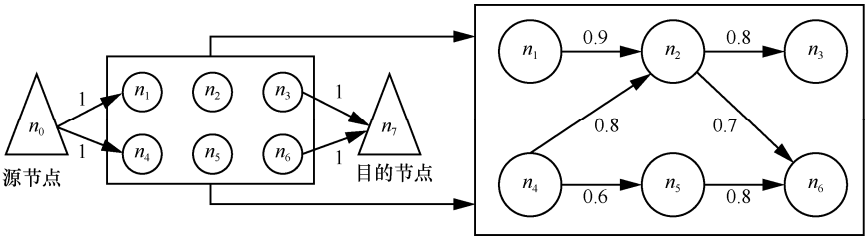


图 2 多跳路径信任度计算模型

$td(n_0,n_4,n_5,n_6,n_7)=0.48$、$td(n_0,n_4,n_2,n_6,n_7)=0.56$、$td(n_0,n_4,n_2,n_3,n_7)=0.64$，由此可知，最可靠路径为 $n_0\to n_1\to n_2\to n_3\to n_7$。

3.4 路由度量的设计

确定最终传输路径的依据，即路由度量，由路径信任度 $td(r)$ 及多种 QoS 度量 $q_1(r),q_2(r),\cdots,q_n(r)$ 共同组成，可以表示为有序集合 $m(r)\triangleq\left[td(r),q_1(r),q_2(r),\cdots,q_n(r)\right]'$，集合中参数的顺序体现量化排序的优先级。考虑到 QoS 参数的不唯一性以及 $td(r)$ 与 $q(r)$ 的半闭合关联特性，本文研究在构建路由度量计算模型时引入半环理论[17]。

定义 1 半环是一种代数结构 $\left(S,\oplus,\otimes,\bar{0},\bar{1},\leqslant\right)$，其中，$S$ 是一个集合，对于 $\forall a,b,c\in S$，$\oplus$、$\otimes$ 和 $\leqslant$ 是具有以下特性的二元运算。

$$a\oplus b=b\oplus a,(a\oplus b)\oplus c=a\oplus(b\oplus c),a\oplus\bar{0}=a \tag{15}$$

$$(a\otimes b)\otimes c=a\otimes(b\otimes c),a\otimes\bar{0}=\bar{0},a\otimes\bar{1}=a \tag{16}$$

$$a\leqslant b,c\leqslant d\Rightarrow a\oplus c\leqslant b\oplus d,a\otimes c\leqslant b\otimes d,$$
$$a\leqslant b\Leftrightarrow\exists c\in S:a\oplus c=b \tag{17}$$

由此可知，信任度的半环可以表示为代数结构 $\left(T,\oplus_T,\otimes_T,\bar{0}_T,\bar{1}_T,\leqslant\right)$，其中，$T$ 是信任度的集合。$\otimes_T$ 和 $\oplus_T$ 代表沿着一条路径计算信任度和跨越多条路径计算信任度的运算符。而 QoS 的半环可以表示为代数结构 $\left(Q,\oplus_Q,\otimes_Q,\bar{0}_Q,\bar{1}_Q,\leqslant\right)$，其中，$Q$ 是 QoS 度量的集合。$\otimes_Q$ 和 $\oplus_Q$ 代表沿着一条路径计算 QoS 和跨越多条路径计算 QoS 的运算符。

3.5 最优可信路由选择算法

选择最优路由需要确定最优路由度量 $m(r)$，而 $m(r)$为信任度与 QoS 共同构成的有序集合，为此，先考虑信任度的量化排序。根据所构建的信任度半环代数结构模型，WSN 中节点 n_1 到达节点 n_n 的路径的信任度集合 $TD(r)$ 为

$$TD(r)=\oplus_T\left[td\left(r(n_1,n_z)\right)\otimes_T td\left(r(n_z,n_n)\right)\right] \tag{18}$$

其中，$n_z\in r(n_1,n_n)$，运算符 $\otimes_T$ 表示“×”，运算符 $\oplus_T$ 表示“sort(·)”。由此，$m(r)$中的第一行参数 $TD(r)$为按路径信任度降序排列的集合向量。定义当前最大的信任度值 $td_i(r_i)$（记为 td^*）所对应的路径 $r_i(n_1,n_n)$为当前最可信路径，记为 $r^*(n_1,n_n)$。

然而，最可信路径未必满足 QoS 指标要求，为此，还需兼顾多项 QoS 度量，即 $m(r)$中 $q_1,\cdots,q_n$（如时延、吞吐量、抖动、负载开销等）满足环境要求。本文算法通过半环代数模型排序以筛选满足网络信任度要求的路径有序集合后，若任意节点 n_x 能找到非空候选最优可信路径集合 $R^*(n_x,n_n)=\left\{r_i(n_x,n_n),\cdots\right\}$，则 n_x 将按照不同 QoS 度量的重要性进行排序，进而接着按半环模型历经路由选择过程。直到获得同时满足信任度及 QoS 度量指标的最优路径。最优可信路由算法的详细过程示于算法 1。

算法 1 最优可信路由算法伪代码

1)begin

2)添加 n_n 到 N^* % n_n 表示目的节点，N^* 表示到 n_n 存在最优路径的节点集合

3)while $N\neq N^*$ % N 表示网络中所有节点的集合

4) for 节点 $n_x\in N-N^*$ % n_x 表示源节点

5) 确定 $m\left(r(n_x,n_n)\right)=\left[q_0,q_1,\cdots,q_t\right]'$ % $m\left(r(n_x,n_n)\right)$表示路由度量，$q_0=TD\left(r(n_x,n_n)\right)$ 有最高优先级

6) for $n_z\in\Gamma(n_x)$，% $\Gamma(n_x)$ 表示能够选取当作信息传递下一跳的候选节点集合

7) if $td(n_x,n_z)\otimes_T td\left(r(n_z,n_n)\right)\geqslant td\left(r(n_x,n_n)\right)_{\text{th}}$ % $td\left(r(n_x,n_n)\right)_{\text{th}}$ 表示路径的信任阈值

8) 添加 $\left(n_x,r(n_z,n_n)\right)$ 到 $R^*_{Q_0}(n_x,n_n)$ %

$R^*_{Q_0}(n_x,n_n)$表示最优路径的候选集合

9)　　end if
10)　　end for
11)　　if $R^*_{Q_0}(n_x,n_n)=0$
12)　　将 n_x 从网络中逐出
13)　　end if
14)　　for j=1:t
15)　　$R^*_{Q_j}(n_x,n_n)=\oplus_{Q_j} r^*_{Q_{j-1}}(n_x,n_n)$，$r^*_{Q_{j-1}}(n_x,n_n)\subseteq R^*_{Q_{j-1}}(n_x,n_n)$
16)　　end for
17)　　if $R^*_{Q_t}(n_x,n_n)=0$
18)　　将 n_x 从网络中逐出
19)　　else 添加 n_x 到 N^*
20)　　return $r^*_P(n_x,n_n)$，$r^*_P(n_x,n_n)\subseteq R^*_{Q_t}(n_x,n_n)$
21)　　end if
22)　　end for
23) end while

4　TSSRM 机制

根据所构建的路由度量与最优可信路径选择算法，提出了基于信任感知的无线传感器网络安全路由机制（TSSRM, trust sensing based secure routing mechanism）。

4.1　网络的初始化过程

考虑簇状拓扑的无线传感器网络，选择初始信任度较高的节点作为簇头，节点的信任度越高，其能量也就越高，节点生存期越长，这样的簇头选择更有利于簇结构的稳定。由 6 个节点构成的簇状拓扑网络模型的簇头选择过程如图 3 所示。在图 3(a)的网络初始化阶段，节点是非聚类的，且各节点都具有随机的初始信任度 TD_s，满足 $0.5\leqslant TD_s\leqslant 1$。每个节点将监听相邻节点的行为，并交换彼此的初始信任度，用以根据簇头选择机制选举新簇头。图 3(b)给出了模型中各节点的信任度，其中，TD_s 为 0.8 的节点接收到的邻居节点的 TD_s 分别为 0.7、0.9、0.6、0.6 和 0.5。比较可知，具有较高信任度的邻居为 TD_s=0.9 的节点，故该节点与 TD_s=0.9 的节点关联从而成为其成员节点。考虑到广域部署时簇间可能存在的地理交叠，故经过有限次比较后，可以选择相邻节点中具有最高 TD_s 的节点作为簇头，如图 3 所示。

4.2　路由的构建过程

根据 TD_s 确定簇头节点后则完成了网络初始化，此时需要构建传输链路。本文所提出的 TSSRM 建立步骤如图 4 所示。

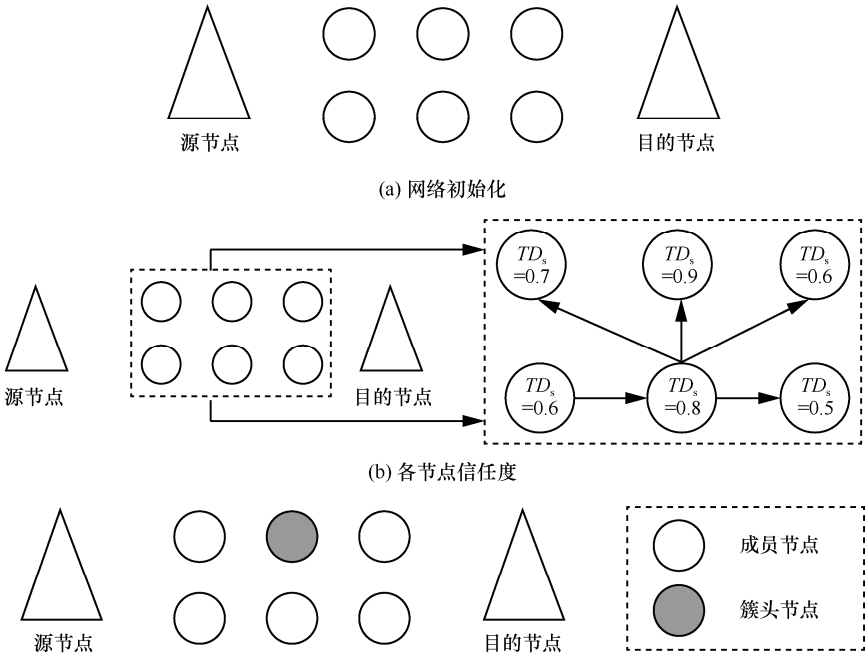


图 3　簇头的选择过程

步骤 1　当源节点 n_0 有数据分组发送到目的节点 n_{11} 时，则初始化信任推导过程并发送信任请求数据分组 *TR* 到其邻居节点（如节点 n_2），可以表示为 $TR=\left\langle ei_{\mathrm{id}},ed_{\mathrm{id}},td\left(r\right)_{\mathrm{th}},ts,s,hl\right\rangle$，其中，$ei_{\mathrm{id}}$ 和 ed_{id} 分别表示评估节点和被评估节点的身份标识；$td\left(r\right)_{\mathrm{th}}$ 表示路径的信任度阈值；*ts* 表示时间标记；*s* 表示信任请求分组编号；*hl* 代表 *TR* 的跳数计数器，计数值为正整数且随转发次数增加而不断减小。为了减少信任传递引起的泛洪开销，*hl* 一般不宜设置过大。为便于说明路由构建过程，利用 ei_{id} 标识节点 n_0，ed_{id} 标识节点 n_2。节点 n_2 接收信任请求数据分组后需要先进行新鲜度检查，如果是重复请求则丢弃，否则将以广播形式转发该请求到 n_2 的所有邻居节点。

步骤 2　n_2 的邻居节点（n_2、n_3 和 n_6）接收到信任请求数据分组后将通过反向路径向节点 n_0 发送信任回复。然而，如果信任请求数据分组中跳数计数器 *hl* 的值递减为 0，那么所有收到请求的邻居节点将丢弃该请求，不再广播转发。

步骤 3　获得由 n_2 的邻居节点提供的参数后，节点 n_0 将通过所提出的直接信任、推荐信任及激励因子相结合的方式评价节点 n_2 的信任状态。然后，节点 n_0 根据信任路径约束条件确定节点 n_2 是否可信从而能够作为中继节点。根据所构建的信任度计算模型，节点 n_0 可以获得可信转发集合（n_2、n_3）并向该集合中的节点发送路由请求。

步骤 4　收到路由请求的任意中间可信节点，如果路由表中存在到达 n_{11} 的最优路径，将向 n_0 发送路径回复，从而使 n_0 获得到达 n_{11} 的最优路径，此时转到步骤 6。如果收到路由请求的可信节点路由表中没有到达 n_{11} 的最优路径，此时将重新执行步骤 1 到步骤 3 以找出下一个可信节点。

步骤 5　如果节点 n_{11} 收到路由请求，该节点将根据算法 1 由反向路径发送路径回复给节点 n_0。

步骤 6　源节点 n_0 将通过所构建的最优路径发送数据分组到目的节点 n_{11}。

考虑到直接信任推导模型主要取决于自身的检测系统，因此，并不会产生较大的通信开销。然而，推荐信任模型由于涉及推荐节点间的信息交互，因此，与通信开销的大小密不可分。本文所构建的 TSSRM 只选择被评估节点邻居节点的推荐，有效控制了推荐范围，显著减少了信息传输过程中

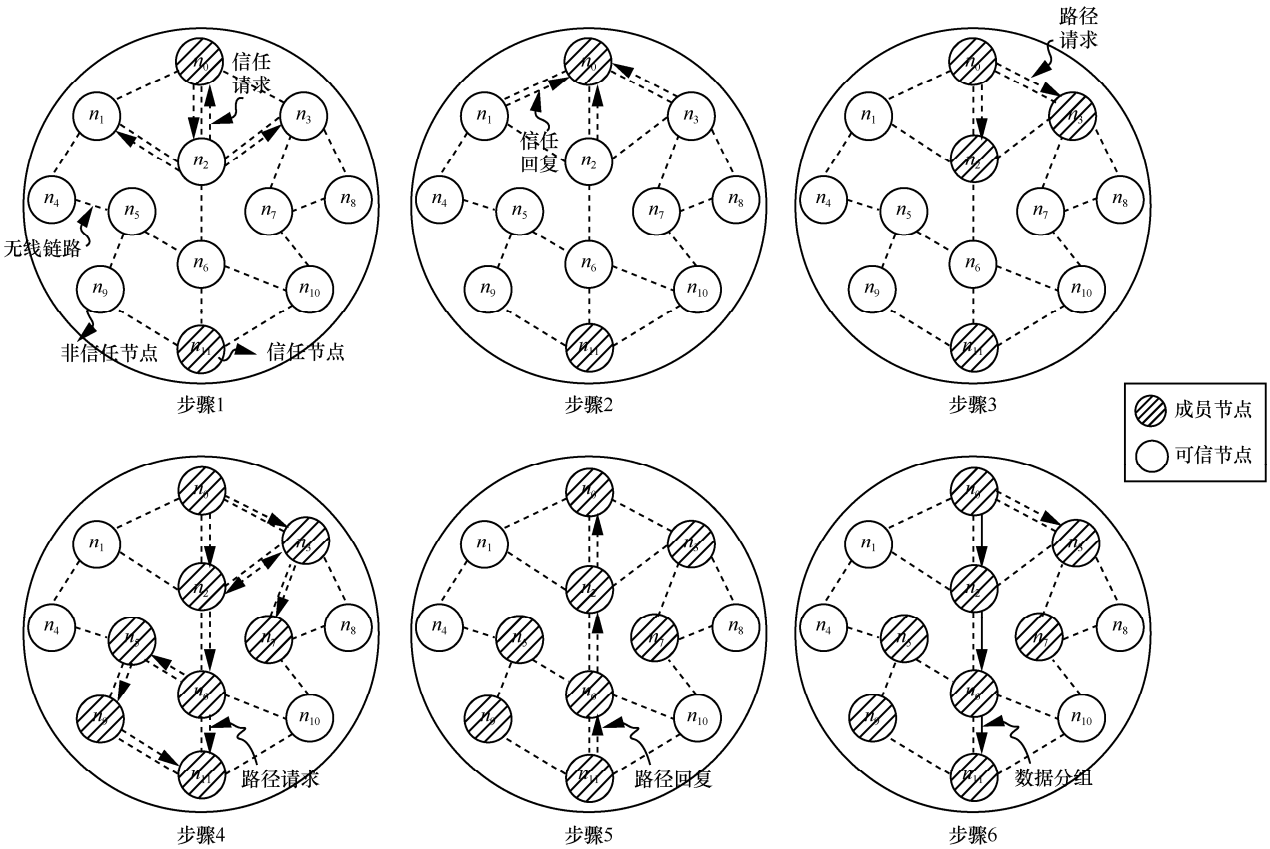


图 4　TSSRM 路由构建过程

的通信开销。此外，所采用的直接信任、推荐信任与激励因子相结合的方式，可以有效检测出实际应用常见的 WSN 节点为了节省能量而放弃中继转发的自私行为，从而快速将攻击节点或自私节点从可信任路径中逐出。

5　仿真结果与性能评估

本研究采用 NS2[18]仿真器分析 TSSRM 的性能。设置每次仿真时间为 500 s，恶意节点在模拟场景中可以发起灰洞、篡改、开关和诽谤攻击，基本路由协议采用 GPSR，其他缺省，仿真参数如表 2 所示。

表 2　　仿真参数

参数	数值
通信距离	40 m
数据分组发送间隔	5 s
节点初始能量	1 000 J
传感器节点数量	100
数据分组长度	100 B
能量阈值	400 J
初始信任度	[0.5,1]
非信任值间隔	[0,0.45]
监测范围	200 m×200 m
检测的错误率	0.1
$P(a)$	0.01
$N(a)$	−0.1
ω_1 , ω_2	0.90, 0.98
δ	0.15
$td(r)_{\text{th}}$	0.45

5.1　TSSRM 的计算开销分析

TSSRM 的计算开销主要集中在信任度的计算上。为了分析信任度的计算复杂度，令 SA 表示标量加法的代价，SS 表示标量减法的代价，SM 表示标量乘法的代价，SD 表示标量除法的代价。在计算节点信任度的过程中，直接信任度的计算开销为 $3SA+2SM$，间接信任度的计算开销为 $SA+SM$，激励因子的计算开销为 $SA+SS+SD$，因此，信任度的总计算开销为

$$C_{\text{total}}=5SA+3SM+SS+SD \tag{19}$$

5.2　TSSRM 的交付率与信任度分析

恶意节点发起 50%数据分组损失的灰洞攻击及篡改攻击场景下的网络平均分组交付率分别如图 5 和图 6 所示。

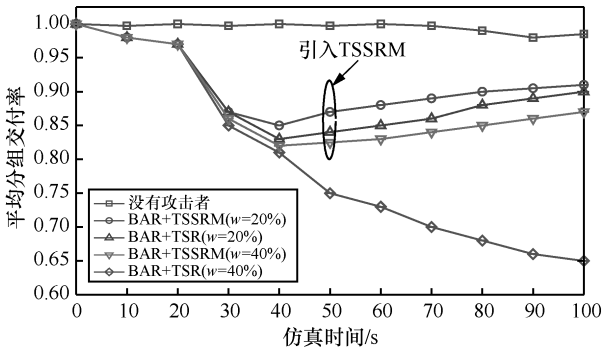


图 5　灰洞攻击下的平均分组交付率

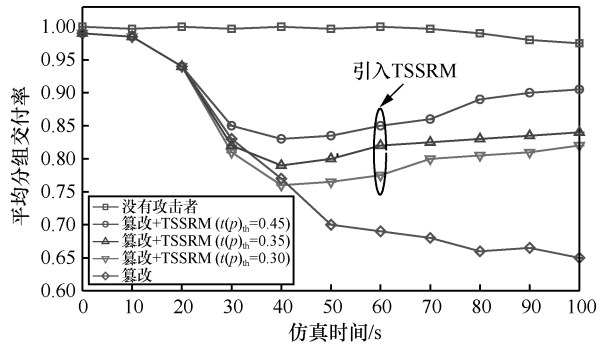


图 6　篡改攻击下的平均分组交付率

通过对无攻击环境、有攻击而不采用 TSSRM 以及不同阈值 TSSRM 条件下的对比可以看出，恶意节点发起的灰洞攻击和篡改攻击都会导致平均分组交付率将下降并逐渐恶化。引入 TSSRM 后可有效提高平均分组交付率，且阈值设置越高改善效果越明显。然而，在实际应用中过高的阈值设定将提高信任标准，从而减少可信节点及链路的数量，这有可能导致可信链路集合为空的现象。因此，路径信任度阈值需要根据部署规模与节点密度合理选取。

常用的信用机制及检测算法往往难以有效处理开关攻击与诽谤攻击。由于结合了行为维度与能量维度，且在综合信任度构建过程中引入了自适应指数衰减时间因子，因此，TSSRM 可以有效地标识上述 2 种攻击行为，如图 7 和图 8 所示。如图 7 所示，如果网络中无异常现象时（20~70 s）信任度通常随时间增大。然而，当恶意节点发起开关攻击（70~100 s）时，信任度显著下降。当一种自适应指数衰减时间因素引入到信任评价模型中时，随着时间的推移，对恶意节点信任度的判断越精准，信任

评估的准确度越高，因为自适应指数衰减时间因素使恶意行为记录时间长于正常行为记录时间。例如，未引入自适应衰减时间因素，发起开关攻击的恶意节点的信任度为0.58，然而由TSSRM测量的信任度为0.36（在90 s时，恶意节点的比例(w)等于50%）。

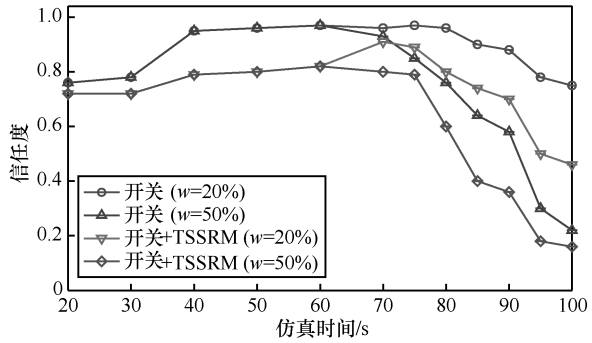


图7　开关攻击下的信任度

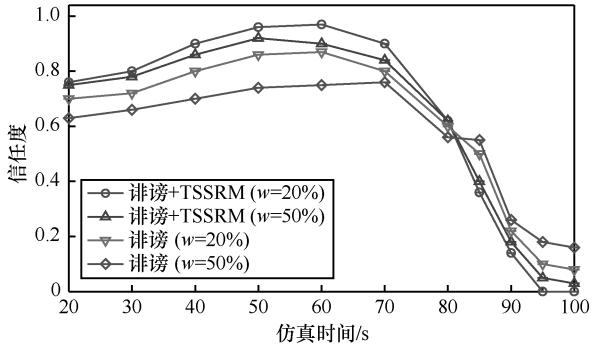


图8　诽谤攻击下的信任度

图8表明，基于所提出的不一致性检查可以有效标记并排除诽谤攻击。诽谤攻击节点可以提供有关好/坏行为的正面/负面建议。因此，在诽谤攻击下，评估正常节点的行为时（20~70 s），信任度相对较低，反之亦然。当引入不一致性检查方案后，再次评估正常节点的行为时，信任度将会增加，因为不一致性检查方案可以过滤掉大部分虚假建议，使信任评估的准确度得以提高。未引入不一致性检查方案，测得正常节点的信任度为0.82，然而由TSSRM测量的信任度为0.97（在60 s时，恶意节点的比例等于20%）。

5.3　TSSRM的有效性与安全性分析

为了不失一般性，考虑TSSRM的有效性与安全性时将在BAR[19]和GPSR协议基础上分别引入TSSRM，从而进行性能仿真与分析。

不同网络密度环境下的TSSRM能量开销情况如图9所示。洪泛机制是提高路径建立成功率的最有效机制，然而广播和重播过程中的控制信息往往带来较大的能耗开销。TSSRM由于采用了高效的信任计算模型，因此，在保证传输成功率的前提下能够显著减少网络路由开销。仿真结果表明，当平均邻居节点数量为16时，TSSRM的能耗比带有2跳限制的洪泛机制节省80.55%，与不采用任何洪泛机制与安全机制的BAR相似。因此，TSSRM可以在保证传输成功率的条件下降低能量开销。

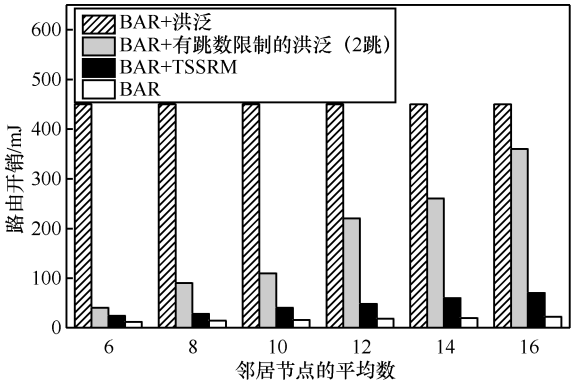


图9　基于BAR的不同算法路由开销

路由建立效率情况如图10所示。对比可知，TSSRM在建立路由前需要进行信任校验，因此所需时间略长于采用直接路由构建的GPSR，但是却远低于其他同等性能机制。与具有2跳数限制的洪泛相比，当邻居节点的平均数为16时，TSSRM建立安全可信路由所需时间可节省39.78%。

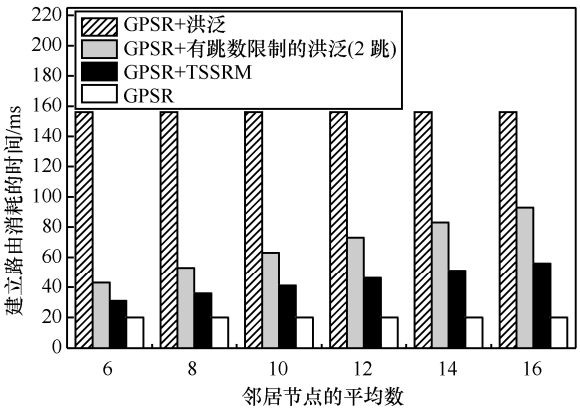


图10　基于GPSR的不同算法建立路由的时间代价

为了验证TSSRM的安全性，假设恶意节点在网络上发起灰洞、篡改、开关以及诽谤攻击（从20 s开始）。每种攻击发生的概率为25%。仿真中

改变恶意节点的数量，分析其对平均分组交付率的影响。如图 11 所示，在现有的路由协议加入 TSSRM，平均分组交付率增加约 40%。如在 100 s 处，通过引入 TSSRM 到现有的路由协议，当恶意节点比例为 20%时，平均分组交付率从 56%增加到 90%，当恶意节点比例为 40%时，平均分组交付率从 39%增加到 83%。

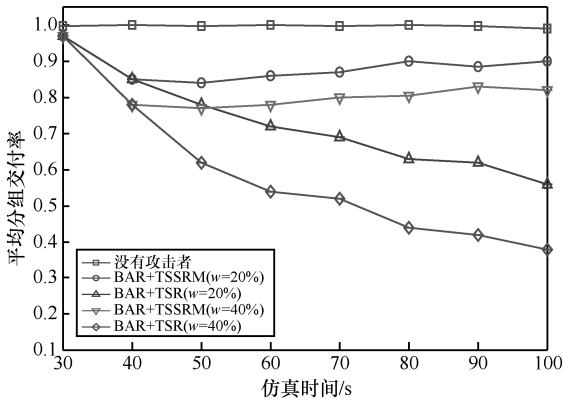


图 11　不同节点密度下的平均分组交付率

TSR[20]是只考虑直接信任度的信任评估机制。将 TSR 与 TSSRM 加入到典型的路由协议中以比较两者的性能。信任评估的正确性基于入侵检测机制的精度，假如可以精确地检测到节点的所有行为，那么间接信任数据是没有必要的。然而，在实际条件下实现它几乎是不可能的。因此，考虑到检测误差率，将检测精度设置为 0.1。如图 12 所示，当恶意节点在网络上（从 30 s 开始）发起攻击时，平均分组交付率将显著下降。由于一些错误检测事件可能会发生在仿真场景中，与 TSR 相比，TSSRM 可将平均分组交付率提高约 10%；其原因在于 TSSRM 兼顾直接信任与推荐信任，为错误检测事件提供更好的抵抗能力。

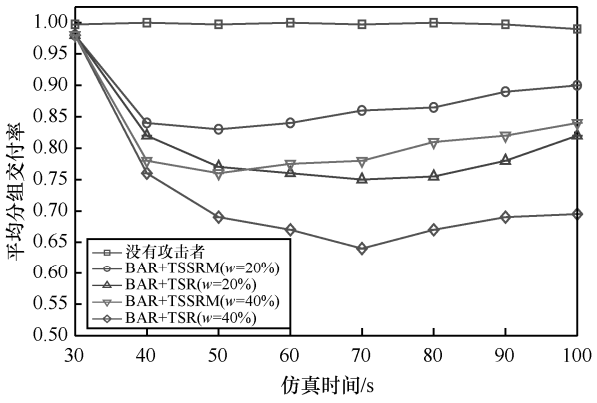


图 12　推荐信任影响下的平均分组交付率

6　结束语

无线传感器网络是现代移动通信系统的重要组成，而信任感知路由协议是提高无线传感器网络安全性的有效方法，因此，对于信任感知路由协议的研究十分重要。本文首先利用半环理论提出一个优化的路由算法，这个算法考虑了信任度和其他 QoS 指标，然后提出基于信任感知的安全路由机制。仿真结果表明，TSSRM 不依赖于所采用的路由协议，并能在原有路由体系有效抵御网络攻击，通过引入 TSSRM 到现有的路由协议，平均分组交付率得到明显提高，可见在安全保证的前提下提高了网络的性能。未来研究将面向无线传感器网络的分布式入侵检测系统，为后续研究节点间的信任度和泛在路由提供新的思路。

参考文献：

[1] 付帅, 马建峰, 李洪涛, 等. 无线传感器网络中匿名的聚合节点选举协议[J]. 通信学报, 2015, 36(2) : 1-10.
FU S, MA J F, LI H T, et al. Anonymous aggregator election protocol for wireless sensor networks[J]. Journal of Communications, 2015, 36(2): 1-10.

[2] 盛敏, 田野, 李建东. 无线传感器网络与自组织网络的研究现状[J]. 中兴通讯技术, 2010, 6(4): 29-37.
SHENG M, TIAN Y, LI J D. The research situation of wireless sensor networks and ad hoc networks[J]. ZTE Communications, 2010, 6(4): 29-37.

[3] 陈正宇, 杨庚, 陈蕾, 等. 无线传感器网络数据融合研究综述[J]. 计算机应用研究, 2011, 10(5): 6-8.
CHEN Z Y , YANG G, CHEN L, et al. Summary of wireless sensor network data fusion research[J]. Application Research of Computers, 2011, 10(5): 6-8.

[4] SAMUNDISWARY P, DANANJAYAN P. Performance analysis of trust based AODV for wireless sensor networks[J]. International Journal of Computer Applications, 2010, 4 (12): 6-12.

[5] 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.
TANG L Y, CHEN Z. Trust management in wireless sensor networks[J]. Journal of Software, 2008, 19(7): 1716-1730.

[6] 陈鸿龙, 王志波, 王智, 等. 针对虫洞攻击的无线传感器网络安全定位方法[J]. 通信学报, 2015, 36(3): 106-113.
CHEN H L, WANG Z B, WANG Z, et al. Secure localization scheme against wormhole attack for wireless sensor networks[J]. Journal of Communications, 2015, 36(3): 106-113.

[7] MOHAMMAD A K A, GADADHAR S. Enhancing cooperation in MANET using neighborhood compressive sensing model[J]. Egyptian Informatics Journal, 2016, 6(19): 1-15.

[8] SUN Y, HAN Z, LIU K J R. Defense of trust management vulnerabilities in distributed networks[J]. IEEE Journals and Magazines, 2008, 46(2): 112-119.

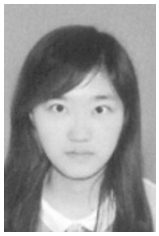
[9] CORDASCO J, WETZEL S. Cryptographic versus trust-based methods for MANET routing security[J]. Electronic Notes in Theoretical Computer Science, 2008, 197(2): 131-140.

[10] 易丽华. “看门狗”技术的实现[J]. 仪表技术, 2011, 6(7): 55-57.
YI L H. Watchdog theory and realization[J]. Instrumentation Tech-

nology, 2011, 6(7): 55-57.
[11] JAY R, SUNIL V, CHIRAG G. Securing VANET by preventing attacker node using watchdog and bayesian network theory[J]. Procedia Computer Science, 2016, 79(6): 649-656.
[12] ZHANG M C, XU C Q, GUAN J F, et al. B-iTRF: a novel bio-inspired trusted routing framework for wireless sensor networks[C]//2014 IEEE Wireless Communications and Networking Conference (WCNC). 2014:2242-2247.
[13] LU G. Design and implement of intrusion detection system network security[M]. Procedia Computer Science, 2003: 11-16.
[14] XU P F, CHEN Z G, DENG X H. Research on neighboring graphs based topology control in wireless sensor networks[M]. Electronic Industry Press, Beijing, 2006: 13-17.
[15] 常建娥, 蒋太立. 层次分析法确定权重的研究[J]. 武汉理工大学学报, 2007, 29(1): 153-156.
CHANG J E, JIANG T L. Research on the weight of coefficient through analytic hierarchy process[J]. Journal of Wuhan University of Technology, 2007, 29(1): 153-156.
[16] SUN Y L, YU W, HAN Z. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 305-315.
[17] 田俊峰, 陈小祥, 刘涛. 一种基于半环理论的可信性评估模型[J]. 计算机工程与应用, 2008, 44(15): 88-91.
TIAN J F, CHEN X Y, LIU T. Trust evaluation model based on semiring[J]. Computer Engineering and Applications, 2008, 44(15) : 88- 91.
[18] 王强, 焦俊, 孔文, 等. 基于 NS2 的固定和移动节点的无线传感网络的仿真[J]. 合肥学院学报（自科版）, 2015, 25(2): 24-28.
WANG Q, JIAO J, KONG W, et al, The Simulation of wireless sensor networks which includes Fixed nodes and mobile node based on NS2[J]. Journal of Hefei University(Natural Science Edition), 2015, 25(2): 24-28.
[19] MAHMOUD M E, SHEN X. Trust-based and energy-aware incentive routing protocol for multi-hop wireless networks[C]//The IEEE International Conference on Communications (ICC ’11). 2011, 6: 1-5.
[20] MARCHANGL N, DATTA R. Light-weight trust-based routing protocol for mobile ad hoc networks[J]. IET Information Security, 2012, 6(2): 77-83.

作者简介：

秦丹阳（1983-），女，江苏苏州人，博士，黑龙江大学副教授、硕士生导师，主要研究方向为无线传感器网络、群智感知以及视觉定位等。

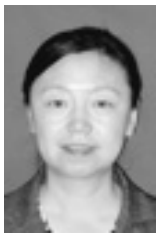


贾爽（1992-），女，黑龙江绥化人，哈尔滨工业大学博士生，主要研究方向为无线传感器网络信息安全与定位技术等。

杨松祥（1993-），男，山东烟台人，黑龙江大学硕士生，主要研究方向为无线传感器网络信息安全等。

马静雅（1993-），女，黑龙江伊春人，黑龙江大学硕士生，主要研究方向为无线传感器网络信息安全等。

张岩（1994-），女，黑龙江绥化人，黑龙江大学硕士生，主要研究方向为无线传感器网络信息安全等。



丁群（1957-），女，黑龙江哈尔滨人，黑龙江大学教授、博士生导师，主要研究方向为无线传感器网络、安全通信密钥、混沌加密技术等知等。