容忍入侵的无线传感器网络模糊信任评估模型

王良民[1]，郭渊博[2]，詹永照[1]

（1. 江苏大学 计算机科学与通信工程学院，江苏 镇江 212013；
2. 解放军信息工程大学 电子技术学院，河南 郑州 450004）

摘 要：针对无线传感器网络的“数据感知融合”和“数据转发”两类关键服务面临的内部攻击，提出了一种基于信任—信心值的二元组模糊信任评估模型，可有效识别路由和数据分组丢弃攻击，并通过限制数据的篡改范围，实现对难以发现的数据篡改攻击的容忍。以示例给出并分析了基于模糊信任模型的容忍入侵机制，以仿真实验说明了模糊信任模型针对路由和数据分组丢弃攻击在入侵节点与普通节点分类上的效果；最后分析了模糊信任模型对网络性能的影响，并阐述了与相关工作的异同。

关键词：无线传感器网络；容忍入侵；可信模型；模糊信任

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2010)12-0037-08

Fuzzy trust model for wireless sensor networks with intrusion tolerance

WANG Liang-min[1], GUO Yuan-bo[2], ZHAN Yong-zhao[1]

(1. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China;
2. School of Electronic Technology, Information Engineering University of PLA, Zhengzhou 450004, China)

Abstract: To protect key services of wireless sensor networks of data fusion and package forward, a fuzzy trust model based on trust and confidence and its evaluation algorithms were presented, in which the value of confidence was used to describe the impreciseness of the value of the trust. Then the simulation and the example were given to show the performances of using the model to detect or tolerate the insidious attacks. Finally, the package drop ration of the networks with the trust evaluation system was simulated and the comparison with the related work was discussed.

Key words: wireless sensor networks; intrusion tolerance; trust model; fuzzy trust

1 引言

无线传感器网络常用于无人照料的恶劣甚至恶意环境下执行监测任务，这种敌意环境下存在大量的攻击行为，通常分为外部攻击和内部攻击[1, 2]。一些轻量级的密码学系统(如 SPINS[3])可通过认证有效地阻止外部攻击。然而，由于传感器节点计算能力、通信能力和电池电量极端有限，且在无固定

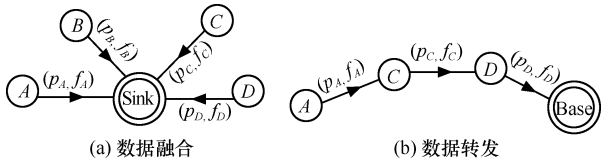
收稿日期：2010-01-19；**修回日期**：2010-09-09

基金项目：国家自然科学基金项目（60703115）；国家高技术研究发展计划（“863”计划）基金资助项目（2007AA01Z405）；国家社科基金资助项目（09CTJ006）；中国博士后科学基金资助项目（200801357, 20070420955）；江苏省博士后科研基金资助项目（0702003B）；江苏省青蓝工程基金资助项目；江苏大学科研启动经费基金资助项目（07JDG080）

Foundation Items: The National Natural Science Foundation of China(60703115); The National High Technology Research and Development Program of China (863 Program) (2007AA01Z405); The National Social Science Foundation of China (09CTJ006); The Ph.D. Programs Foundation of China (200801357, 20070420955); The Postdoctoral Science Foundation of Jiangsu Province (0702003B); Qing Lan Project for Excellent Youth Scholars of Jiangsu Province; The Talents Foundation of Jiangsu University (07JDG080)

基础设施的情况下自组织的工作，这导致传统的访问控制、入侵检测等第一、二代安全技术的效用非常有限，总存在透过认证结构的内部攻击行为[1,4]，这些内部攻击节点作为网络内部成员入侵，隐秘性强且难以发现。信任模型[5~8]、容忍入侵技术[4,9~11]等利用传感器网络节点冗余布置的特点，研究部分成员被入侵的情况下保证系统关键任务的顺利执行，被视为解决相关问题的第三代安全技术。

无线传感器网络通常用来监测外界环境，网络的关键服务是环境感知并将感知数据传输到基站。这两项关键任务可分解为由图 1 所示的两类工作场景：一类是数据融合，汇聚(簇头)节点将同一区域内各个节点采集的信息进行聚合；另一类是分组转发服务，将接收到的分组通过网络中间节点转发给基站，分组包含路由分组和数据分组。针对这两类关键服务，无线传感器网络的内部攻击可以分为路由分组丢弃、数据分组丢弃和篡改数据 3 种。路由分组丢弃[5~8, 12,13]是指恶意节点通过选择性转发路由数据分组，破坏网络的关键服务。Mohammad[13]指出节点可忠实地转发路由数据，而选择性地转发感知数据，从而“不能信任信任模型”——只考虑路由丢弃行为的可信模型，提出通过增加对数据分组的监察扩充信任模型的证据种类，防范数据丢弃攻击。伪造数据攻击是指内部攻击节点通过忠实地转发路由及数据分组，但是更改数据内容，目前的信任模型尚未考虑此类问题的解决方法。本文设计一种模糊信任评估模型，利用二元组扩充信任模型的能力，在保持现有模型路由与数据转发攻击检测能力的基础上，可通过容忍入侵评估机制限制数据篡改攻击能力，从而保证无线传感器网络数据聚合和数据转发这两项关键任务。



(a) 数据融合　　(b) 数据转发

图 1　传感器网络中的关键服务

2　信任评估模型

基于模糊信任的信任模型，用二元组分别表示传统意义上的信任值与对该信任值的信心——对该信任值确定性的一个模糊判断；然后给出了该二元组赋值的评估方法。

2.1　基于二元组的模糊信任模型

模糊信任模型中，主体对客体的评价由 2 个数字组成：信任值和信心值。信任值是主体关于客体是否执行行动的不确定性猜测，用[0, 1]上不确定的概率数表示，其物理意义是该客体正确执行任务的概率。信心值也是[0, 1]上连续的实数，用以模糊地度量主体对自己给出的信任值的信心——因为经验数据和客体行为的不一致性、变化性方面的因素，导致主体对信任值的信心具有很大的主观性。

定义 1　若信任的主体为 S，与客体 A 进行交互，S 赋予 A 的信任值 t_{SA} 是一个有序二元组，形如式(1)。

$$t_{SA}=(p, f) \tag{1}$$

其中，$p\in[0, 1]$是主体 S 对客体 A 在下一个任务中是否执行行动进行猜测的信任概率，而 $f\in[0, 1]$是 S 对 p 准确性进行模糊表达的信心值。

信任值是主体对客体的可信赖性的评估，信心值是主体对自己给出概率是否准确的模糊表达。根据定义 1，一个高信任值可能意味着客体在测试样本集里具有良好的记录，而一个高的信心值意味着客体通过了主体设置的测试次数，表明客体和主体进行了很长时间的交互，而且其行为具有较好的连贯性与一致性[12]。

2.2　信任评估

对于任何一个节点来说，它首先依据自己对邻居节点的监控，计算其作为主体关于该被监控邻居节点(客体)的直接信任值，模糊信任模型中信任—信心的二元组直接信任计算方法如下。

定义 2　记主体 S 与客体 A 进行交互的事件全集为 $E=\{e_1, e_2, \cdots, e_n\}$，集合 $V=\{v_1, v_2, \cdots, v_n\}$，其中 v_i 对应于事件 e_i 是否成功，用 1 表示成功，–1 为伪造或篡改数据的转发，0 为丢弃处理的转发事件，$P(E)$为 E 的幂集，$X\in P(E)$，是主体 S 持有的证据事件。则主体对客体的信任 t_{SA} 为

$$t_{SA}(X)=(p(X), f(X)) \tag{2}$$

其中，$p(X)$是已知$|X|$次交互中成功 $\sum_{e_i\in X, v_i>0} v_i$ 次，第$(|X|+1)$次也出现成功的概率，记 $p(X)$的概率分布函数为$\pi(p)$，则

$$p(X)=\mathrm{E}\left(\pi\left(p\left|\frac{\sum_{e_i\in X, v_i>0} v_i}{|X|}+1, 2-\frac{\sum_{e_i\in X, v_i>0} v_i}{|X|}\right.\right)\right) \tag{3}$$

信心值 $f(X)$由式(4)给出。

$$f(X)=\begin{cases}\dfrac{|X|}{|E|}, & \forall e_i\in X, 有 v_i\geqslant 0\\ \dfrac{|X|}{2|E|}, & \exists e_i\in X, 使得 v_i=-1\end{cases} \tag{4}$$

定义 2 中$\{e_i|\ v_i=1$ 或 $v_i=-1\}\subseteq X\subseteq E$，通过对信任赋值模型的分析，可以得到下面性质。

性质 1　根据 Bayes 定理假设 S 与 A 之间交互成功的先验概率服从均匀分布 $U(0, 1)$，定义 2 的信任概率可简化为

$$p(X)=\frac{\left(\sum_{e_i\in X, v_i>0} v_i\right)+1}{|X|+2} \tag{5}$$

证明　记 u 为主体 S 与客体 A 进行$|X|$次交互后成功的次数，即

$$u=\sum_{e_i\in X, v_i>0} v_i$$

根据 Bayes 定理假设 S 与 A 之间交互成功的先验概率服从均匀分布 $U(0, 1)$，记为$\pi(p)$。当 S 与 A 发生$|X|$次交互后，出了新的事件 R，R 为“$|X|$次交互出现 u 成功”，则有：

$$p(R|\ p=p)=p^u(1-p)^{|X|-u}$$

由全概率公式的连续形式，得到

$$p(R)=\int_0^1 p(R\mid p=p)\pi(p)\mathrm{d}p=\frac{(|X|-u)!u!}{(|X|+1)!} \tag{6}$$

后验概率表示时间 R 发生后的更新概率，根据 Bayes 定理，其密度函数为

$$p(p\mid R)=\frac{\Gamma(u+(|X|-u)+2)}{\Gamma(u+1)\Gamma((|X|-u)+1)}p^u(1-p)^{|X|-u}$$

从而，p 的后验概率密度函数不再是均匀分布，而是 Beta 分布 $Beta(u+1,|X|-u+1)$。

由式(6)的概率密度函数对未来成功事件进行预测，则$p(X)$为“已知$|X|$次交互中成功 u 次，第$(|X|+1)$次也出现成功的概率”，从而得到：

$$\begin{aligned}p(X)&=\mathrm{E}\left(Beta(p|u+1,|X|-u+1\right)\\&=\int_0^1 p(X\mid p=p)p(p\mid R)\mathrm{d}p\\&=\frac{u+1}{|X|+2}\end{aligned}$$

性质 2　式(4)定义的信心函数 $f(X)$是模糊测度，可以表示主体对所赋信任值的不确定性。

性质 2 表明信心值作为信任值的模糊度量，可以表示主体对所赋信任值的不确定性，这使得信任定义满足了 Sun[6]关于信任关系必须满足的不确定性公理。

3　模糊信任评估系统

给出了无线传感器网络的模糊信任评估系统的工作流程，对证据的汇聚、信任的传递以及信任的合成与更新等进行了明确的描述。

3.1　信任评估系统结构

信任评估系统最终的信任决策是由基站完成，基站根据路径信任结构中路径上各节点信度的迭加决定了不同路径的信度。无线传感器网络中的关键服务如图 1 所示，分为数据汇聚和数据转发。因此，信任关系可以分为簇内信任和路径信任 2 类。簇内信任是指邻居节点间直接依靠本地的监控证据和交互证据获得；而路径信任则需要邻居节点的推荐。

图 2 给出了这种路径信任结构的信任评估系统的框架结构。在这种结构中，存在着 2 个问题，第一个问题是数据源节点是否可信，第二个是信任路径的发现问题。数据源节点的可信度来自数据源节点临近节点所形成的信任簇；而信任路径的发现则依靠中继节点的推荐信任。

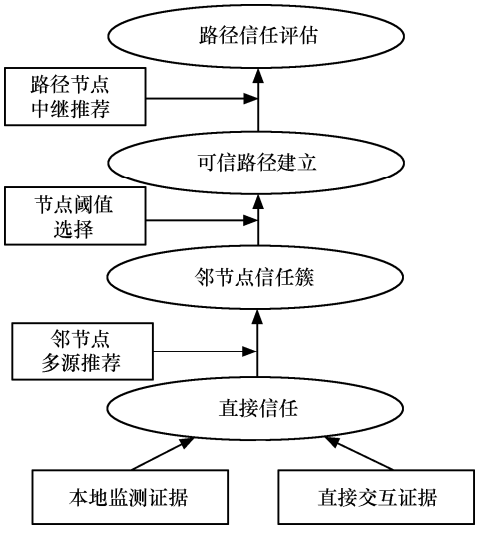


图 2　信任评估系统

3.2　推荐信任

根据图 2，定义⊗运算来求解路径信任中的中继推荐问题。这样，基站与数据源节点之间的信任

路径就变成了中继信任的推荐序列，可以用⊗运算的迭加完成。

定义 3 如果主体 S 对客体 A 的信任值来自中间节点 M 的推荐，则称所获得的信任值 t_{SA} 来自 M 的中继推荐，记为

$$t_{SA}=t_{SM}\otimes t_{MA} \tag{7}$$

在信任网络图 $G=(V,E)$中，⊗为定义在集合 $T=\{t_{AB}\mid A,B\in V\}$上的二元运算：

$$\begin{aligned} t_{SM}\otimes t_{MA}&=(p_{SM},f_{SM})\otimes(p_{MA},f_{MA})\\ &=(p_{SM}\times p_{MA},f_{SM}\times f_{MA}) \end{aligned} \tag{8}$$

由于 p 值和 f 值都在[0,1]上，根据式(8)很容易看到，中继推荐信任值不高于推荐节点对被推荐客体的信任，也不高于主体对推荐节点的信任值。这符合 Sun[6]指出的信任关系必须满足串联传递不会增加信任值的公理。

3.3 信任合成

一个节点对其他节点的信任值，可能需要 2 个方面的信任合成。一个是来自多个节点的推荐汇聚，定义⊕算子求解；另一个是自身直接信任和间接信任的合成，在本节参照社会关系中的信任推荐给出合成方法。

定义 4 在信任网络 $G=(V,E)$中，如果主体 S 对客体 A 的信任值来自多个邻节点 $N_i(i=1,\cdots,n)$的推荐，则称所获得的信任值 T_{SA} 来自 $N_i(i=1,\cdots,n)$的多源推荐，其中每一个 N_i 被称为推荐源。记为

$$t_{SA}=\mathop{\oplus}_{1\leqslant i\leqslant n}(t_{SN_i}\otimes t_{N_iA}) \tag{9}$$

其中，⊗、⊕为定义在集合 $T=\{t_{AB}\mid A,B\in V\}$上的二元运算，⊗由式(8)定义，⊕的定义由式(10)给出：

$$\begin{aligned} t_{SA}^1\oplus t_{SA}^2&=(p_{SA}^1,f_{SA}^1)\oplus(p_{SA}^2,f_{SA}^2)\\ &=\begin{cases}(p_{SA}^1,f_{SA}^1) & ,\ f_{SA}^1>f_{SA}^2\\ (p_{SA}^*,f_{SA}^1) & ,\ f_{SA}^1=f_{SA}^2\\ (p_{SA}^2,f_{SA}^2) & ,\ f_{SA}^1<f_{SA}^2\end{cases} \end{aligned} \tag{10}$$

其中，t_{SA}^1 和 t_{SA}^2 分别是通过不同推荐源计算所得的信任值，其中

$$p_{SA}^*=p_{SA}^1\frac{f_{SA}^1}{f_{SA}^1+f_{SA}^2}+p_{SA}^2\frac{f_{SA}^2}{f_{SA}^1+f_{SA}^2} \tag{11}$$

Sun[6]指出信任关系必须满足的第 3 个公理是多路径并联传播不会降低信任值。当然，定义 4 的多源推荐定义是基于二元组定义，如果综合信任值和信任值的质量——信心值，如用(*p***s*)表示完全意义上的信任评估值，则定义 4 满足这个第 3 公理。

定义 5 参照社会关系中的信任推荐给出了直接信任和推荐信任合成模型。这种合成中的主要问题是一个节点如何看待自身经验以及其他节点推荐值的重要性。

定义 5 设主体 S 对客体 A 的直接信任值 $t_1=(p_1,f_1)$，而相关节点的推荐信任值 $t_2=(p_2,f_2)$，则信任合成后，主体对客体的信任值：$t_{SA}=(p,f)$，其中，

$$f=\begin{cases}f_1 & ,\ f_1\geqslant f_2\\ f_1+(1-f_1)(f_2-f_1), & f_1<f_2\end{cases} \tag{12}$$

$$p=fp_1+(1-f)p_2 \tag{13}$$

在信任—信心值模型中，信心值表示数据本身的质量，定义 5 的合成模型主要是参考了社会关系中的经验：在现实社会关系中，主体 S 对客体 A 给出一个直接的信任概率 p_1，他通常只会在自己的基础上参考他人推荐值进行微调，这种微调主要是针对自身信心不足部分的弥补；如果他对这个信任概率的信心值 f_1 很高，他人的低信心值不会影响到他自己对这个信任概率的信心，而如果他人信心值较高，他对这个基于微调的概率值也就有了相对高一些的信心值。

3.4 信任更新

网络系统运行一段时间后，就经历一组事件(记为 n 次)，需要考虑信任的更新。假设 S 和 A 再次进行了 n 次事件，如定义 2 所述，其中有监察记录的事件为集合 X，若考虑 2 个周期里所有的事件为经验集合，继续利用 Beta 分布的期望值重新计算，则信誉更新需要用到上一个周期的监察记录，而保留这种记录将不断增加存储空间需求，同时增大了信任重新计算的运算量。通过引入遗忘因子 λ，在求得最近一个周期的信任值 T'之后，与前一个周期保留的信任值 T 之间进行求和，则更新后的 $T=(p,f)$可以用式(14)求得。

$$T=(1-\lambda)T+\lambda T'=((1-\lambda)p+\lambda p',(1-\lambda)f+\lambda f') \tag{14}$$

考虑到最近获得的信息应赋予更高的权重，通常 $\lambda>0.5$，本文实验中 $\lambda=0.6$。

4 数据篡改攻击的容忍机制

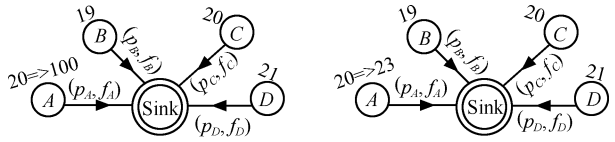
“信任—信心”二元组的信任评估系统，可以

有效防御入侵节点发起的篡改数据攻击，达到容忍入侵的效果，这是本文方法区别于其他信任模型的显著优点之一。本节通过示例介绍模型应对伪造数据攻击，并给出了其有效性的分析。

4.1　数据篡改攻击

数据聚合通常是节点以簇的形式，将来自同一区域内采集的信息进行聚合，如图 3 所示，Sink 节点承担了簇内数据集合和转发的任务。假设信任机制已经排除了恶意节点充当 Sink 节点的可能，然而 Sink 节点可能得不到正确的数据。

通常，节点的数据聚类是求平均值，入侵节点还可以进行一种篡改数据的攻击。如图 3(a)所示，若入侵节点 A 报告的数值为 100，B、C、D 分别为 19、20、21，则 Sink 平均后获得平均值为 40，而实际环境值可能更接近 B、C、D 三者的平均值 20，这样一个节点伪造数据，导致了聚合数值错误，从而达到了攻击网络关键服务的目的。



(a) 大范围篡改　　(b)智能篡改

图 3　数据篡改攻击

图 3(a)中 A 对数据篡改范围过大，很多常用的聚类分析方法都能将 A 剔除。但是，由于无线传感器节点的智能性，还会出现智能攻击方式。如图 3(b)所示，智能节点 A 小范围调整其值，也能引入高达 4%的误差。通常的数据聚合方法已经很难排除 A，除非更为精准的智能算法，但是需要较大的运算量。

4.2　基于模糊信心值的攻击容忍机制

在模糊信任评估模型中，簇头节点根据簇内节点提供的数据与中心值的差异，调整对其评估值的信心。实验中，用式(15)来计算对节点 i(如图 3(a)所示，i 为 A, B, C, D 中 4 个节点之一，n 为 4)的信心值。

$$f_i' = \begin{cases} \dfrac{\left|\dfrac{1}{w_i - w}\right|}{\dfrac{1}{n}\left(\sum\limits_{i=1,..n}\left|\dfrac{1}{w_i - w}\right|\right)} f_i & , |w_i - w| > \dfrac{1}{n}\sum\limits_{i=1,\cdots,n}|w_i - w| \\ f_i & , |w_i - w| \leqslant \dfrac{1}{n}\sum\limits_{i=1,\cdots,n}|w_i - w| \end{cases} \tag{15}$$

式(15)中 f_i 是节点 i 原来的信心值，f_i' 对节点 i 进行数据可靠性检查后新的信心值，w_i 是节点 i 汇报的感知值，w 是簇内感知数据的中心值，其值由式(16)给出。

$$w = \frac{\sum\limits_{i=1,\cdots,n} w_i}{\sum\limits_{i=1,\cdots,n} (w_i)^0} \tag{16}$$

簇头在利用式(15)计算获得对于所有节点的信心值 f_i 后，利用式(17)求基于信任值的加权平均值，将其作为环境感知数据汇报。

$$w' = \frac{\sum\limits_{f_i > \theta_f} (p_i w_i)}{\sum\limits_{f_i > \theta_f} p_i} \tag{17}$$

式(17)中 θ_f 为系统设定的信心阈值，在本文实验中，其值为(0.6+ε)，ε 为一极小量。以图 3(a)为例，在极端情形下，所有参与这些关键任务的节点信任度和信心度均为 1，式(15)计算获得 A 的模糊信心值仅为 0.5，因此节点 A 将被从聚合任务中淘汰，从而最终结果为 20。而针对图 3(b)，式(15)~式(17)的方法计算量非常小，不用采用计算量很大的模式聚类方法，此时节点 A 的信心值为 0.555，被排除，从而新的聚合值为 20。

依托图 3 的例子，从函数的角度剖析式(15)~式(17)，图 4 给出在其他节点数据值 w_i 固定的情况下，攻击节点 A 选择的数值 w_1 与 f_1 之间的变化关系。

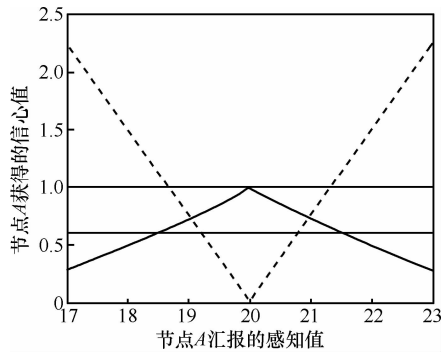


图 4　数据聚合方法的容侵性说明

图 4 中，随着节点 A 汇报的感知值 w_1 在区间[17, 23]之间变化，虚线显示了攻击节点篡改数据幅度 $|w_1 - w|$ 的变化情况；实线表示信心值 f_1 的变化趋势，由图可知随着攻击者篡改数据的幅度增长，其信心值 f_1 显著下降；如果 w_1 取值在区间[18.5, 21.5]之外，表示信心值低于阈值 0.6，这表示将会视为无效数

据而被排除，这将攻击者所能篡改的数据幅度有效地限制在 1.5 以内；此外，在此例中，当攻击者的数据篡改幅度靠近 1.5 时，信心值 f_1 乘以 0.6 的系数，因此该数据引进的最大篡改幅度 0.9，经过 4 个点求平均值后为 0.225，从而式(15)~式(17)成功地将攻击者所能带来的相对误差限制在 1%左右。

上述实例及分析表明，式(15)~式(17)限制了入侵节点数据欺骗能力，若入侵节点篡改数据范围过大，则可能被淘汰出任务集；即使入侵节点通过精心选择最大欺骗能力的数据，式(15)~式(17)也有效地降低了恶意数据的影响力，体现了该聚类方法的容忍入侵性。

5 仿真实验与结果分析

前面详述了模糊信任评估模型以及其符合 Sun[6]关于信任模型的公理性要求，并且具有限制、容忍数据伪造攻击的能力，这是本模型的特色之处。本节通过仿真实验给出模糊信任系统的一些通用性能，如在攻击检测、网络性能方面的实际能力以及与相关工作相比较的特点。

5.1 攻击节点检测实验

本实验重在考虑模糊信任评估模型在应用中能否发现具有攻击行为的节点，攻击行为分为 3 类，第一是路由分组丢弃，第二是数据分组丢弃，第三是数据篡改。实验考察网络运行一段时间后，各种类型的攻击节点在信任—信心值的分布上，能否形成正常节点与恶意节点明显区分的聚类格局。实验过程中，每个节点发给邻居分组后，在一个合理的时延内，解析该邻居节点转发的分组，通过这种监测分析机制，观察其是否转发了该分组，本实验在 NS2 仿真平台上通过修改 recv(Packet*, Handler*)函数接受分组处理的相关流程，在调用 forward(aodv_rt_entry*, Packet*, double)函数后解析邻居转发的分组实现监控。

在实验中，对于路由和数据分组丢弃，很难区分是信道问题，还是节点的主观选择，因此对不转发路由和数据分组，一律将定义 2 中的 v_i 赋值为 0；而对于篡改数据的行为，根据 2 种不同的关键情况区别对待：在数据转发的路径上，则每发现一次，直接将信心值减半，即定义 2 的赋值方式；在执行数据聚合任务时，则依照式(15)处理。为便于观察，实验选取正方形平面为节点部署区域，均匀划分为 10×10 方块，每个方块规定为一个簇，每个簇 5 个节点。随机选择 30 个簇，在其中 10 个簇中各选择一个节点设为选择转发路由分组的恶意节点，其丢弃路由分组的概率为 50%，远远大于正常的网络分组丢失率；同样，在 10 个簇中，设置一个选择转发数据分组的节点，其分组丢失的概率也为 50%；剩下的 10 个簇中，每簇选择一个篡改伪造数据的节点，这些节点忠实地转发路由分组和数据分组，修改数据分组内容，在实验中，并未严格执行数据比对，而是随机选定恶意节点，定义其为恶意篡改节点，对其信任信心值进行调整。

设置信任更新周期为 20min，每个周期内随机选择 10 个区域提供监测传输数据给基站，每个周期内需要进行一次簇头选举，被选中的 10 个区域还需要发现通往基站的路由，路由建立后每分钟传输一次数据给基站。在这个实验中，方块内 5 个节点根据能量均衡准则，在达到信任阈值的前提下，实行轮值簇头机制；为增加分组的数量，提供检测依据，路由算法采用每分组回复的 AODV 路由算法，仅仅增加了监测机制，针对各个节点进行信任评估，而评估值不影响节点加入路由的概率。节点信任、信心初值均设置为(0.6, 0.7)之间的随机量，不取相同值的目的是让所有节点分散分布在平面上，可以给出更为直观的聚类图，阈值设置为 0.6,从而使得最初所有的节点都能参与簇头选举和路由转发。图 5 分别给出了开始状态、1 个周期后、5 个周期后、20 个周期后各个节点信任—信心值的分布图。

由图 5 可知，在第一个周期里，绝大多数路由转发攻击节点进入了低信任值的区域，这是由于所有节点都参与了成簇活动，而在本实验中，簇头协商协议的分组被当成路由分组进行监控的，此外，所有簇头都参与了路由转发分组，为此路由丢弃攻击的节点进行了攻击行为，很快就暴露出来了。而参与数据分组转发能进行丢弃及篡改的机会较少，必须进入选定的路径上才能进行攻击，因此要到 20 个周期以后才能逐渐被发现。然而，这些恶意节点没有被及时发现，并非方法本身的缺陷，而是该节点尚未进行恶意行为。在 20 个周期后，将 10 个路由转发攻击及数据转发攻击的节点聚类在[0, 0.6]×[0, 1]区间内，而把篡改数据攻击的节点聚类在[0, 1] ×[0, 0.6]区间内，而这 2 个区间都被阈值 0.6 限制而不能参与网络任务。这表明本文的信任管理系统，可有效地将各类具有攻击行为的入侵节点聚类，与正常节点分开，具有较强的入侵检测能力。

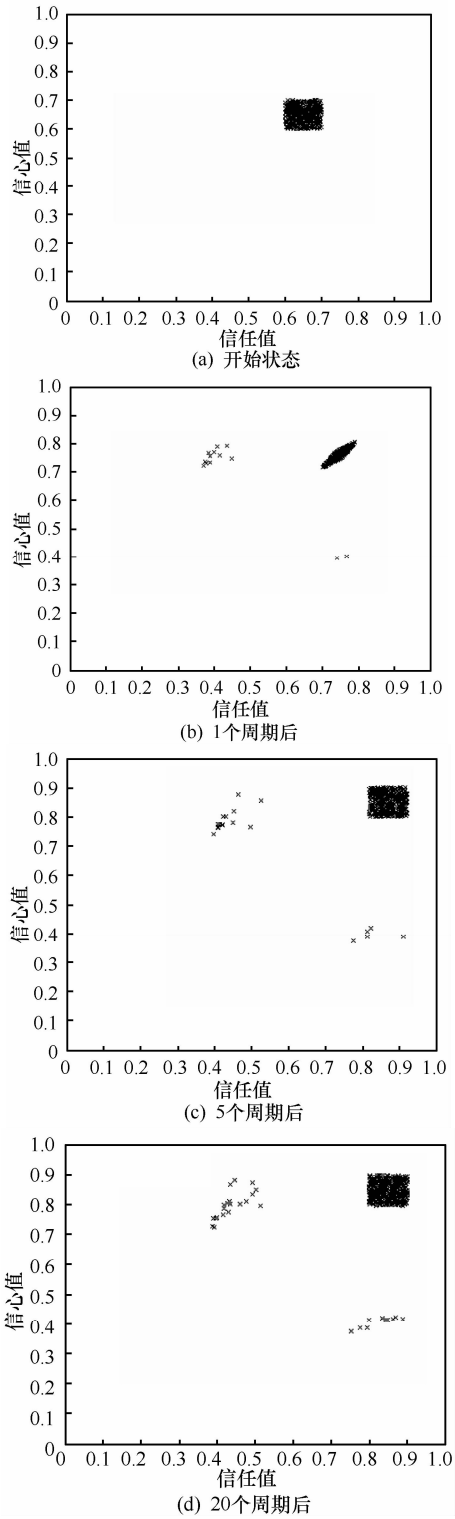


图 5　入侵节点信任值聚类

5.2　网络性能比较

本节采用 2 组对比实验重点考察网络中的分组丢失率，一组在选取路径时，不考虑信任—信心值；另一组则在每个周期开始重新选取路由时，信任—信心值低于阈值的节点不再参与网络任务。得到的网络分组丢失率的变化曲线如图 6 所示。

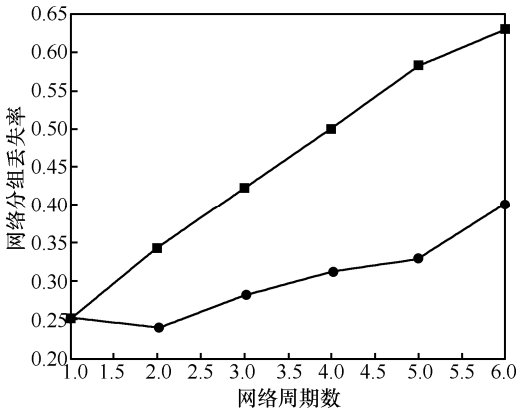


图 6　网络分组丢失率比较

图 6 中可以看出，在第一周期，2 组实验分组丢失率非常接近，因为实验在第一周期允许所有的节点参与路由选取；而此采用模糊信任系统的网络分组丢失率明显低于不考虑节点属性的网络系统。图 6 中，采用模糊信任系统的网络最初分组丢失率甚至有下降趋势，而在第 5 个周期后，其分组丢失率上升的趋势甚至高于没有采用信任系统的网络，这是由于网络中节点的冗余程度造成的。最初(第二个周期)网络中部分节点不参与运行时，使其冗余度下降，因此网络性能会略有上升；而当越来越多的节点，甚至 50%的节点(第 5 个周期)不参与网络任务时，网络过于稀疏，数量很少的节点承担了全部的网络传输任务，通信频度高，因此分组丢失率大大上升。总体来说，在一定冗余的网络中，存在比例相对较少的恶意节点时，采用模糊信任系统的网络，可以排斥不信任节点，使得网络性能大大提高。

5.3　相关工作

信任评估用于表示关系的基本属性，在很多领域得到大量的研究与应用，不同的领域往往使用不同的方法和技巧，在基于无线 ad hoc 网络的信任模型研究中，Sun[6]等提出信任模型必须满足的公理属性，并在此基础上提出了一个基于熵的信任模型；George 等[12]提出的基于半环代数理论的信任模型，采用的有向图与半环的计算方法，有较好的动态行为适应能力和恶意行为检测能力。但是这 2 种方法中用到的信任链的方法建立聚合推荐信任度，收敛速度较慢限制了该方法的可扩展性。在无线传感器网络中，节点能力使得无法维持一个全网的信誉系统，从而要求信任模

型的计算只能具有轻量级的时空复杂度；而无线传感器网络大规模布置的应用场景又要求模型具有很强的可扩展性。相关问题，文献[5]给出了一个较为全面的综述。

本文信任模型的特点是采用 Zhang[14]关于邻居节点相互进行监测的假设，并在 NS2 中实现了这一机制，对数据转发及数据篡改攻击的监视。Zhang[14]将观测图(observability graph)传输到基站，并由基站统一进行集中式的警报推理，本文则将信任评估和决策放在局部进行，利用网络任务分层及所定义的简单算子，更为有效地降低了运算量和全局通信量。这种邻居节点相互进行监测的方法，完善了 George [12]的二元组模型，使其可以完成 3 种类型内部攻击的检测，具备了 Sun [6]认为用于入侵检测的信任评估模型应具备的公理化属性。Bayes 方法的信任概率计算简单，不存在 Sun [6]基于熵的信任链计算复杂度问题。相对于现有关于无线传感器网络信誉模型[7,8,13]，本文模型更全面地考虑了 3 种类型的攻击，并给出了系统的解决方法，尤其是对于篡改数据的攻击，当前文献主要是用数据聚类的方法来进行容错处理[15]，而无法处理对于图 3(b)那样蓄意的智能攻击所带来的误差扩大。文献[8]提出对节点信任评估和通信评估分治，用不同的节点完成，和本文用信心值评估信任值的质量，在思想上具有一致性，即避免因评估质量造成评估系统的误判，但是该文的信任评估建立在攻击分类检测的基础上，和本文用信任评估进行攻击检测，在用法和假设前提上，具有较大差别。

6 结束语

设计了一类基于信任—信心值的二元组信任评估模型，以信心值的形式模糊描述信任值准确程度的不确定性，并给出模型中参数的评估方法。基于该模型的信任系统，可以检测无线传感器网络中存在的路由、数据分组丢弃及数据篡改等 3 种类型的内部攻击；对于智能数据篡改攻击，可限制其篡改数据的幅度，实现对该攻击的容忍入侵。

参考文献：

[1] PERRIG A, STANKOVIC J, WAGNER D. Security in wireless sensor networks[J]. Communications of the ACM, 2004, 47(6): 53-57.

[2] KARLOF C, WANGER D. Secure routing in wireless sensor networks: attacks and countermeasures[J]. Elsevier's Ad Hoc Networks Journal, 2003, 1(2-3):293-315.

[3] PERRIG A, SZEWCZYK R, *et al*. SPINS: security protocols for sensor networks[J]. Wireless Network, 2002, 8(5):521-534.

[4] MA R, XING L, MICHEL E. Fault-intrusion tolerant techniques in wireless sensor networks[A]. DASC06[C]. Washington, DC, US, 2006. 85-94.

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

[6] SUN Y, YU W, *et al*. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2008, 19 (7): 1716-1730.

[7] 肖德琴, 冯健昭, 张焕国. 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.
XIAO D Q, FENG J Z, ZHANG H G. Reputation formal model based on wireless sensor networks[J]. Computer Science, 2007,34(6):84-87.

[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, 2007,28(6):84-87.
YANG G, YIN G S, YANG W,*et al*. Reputation model based on behaviors of sensor nodes in WSN[J]. Journal on Communications,2007,28(6):84-87.

[9] 王良民, 马建峰, 王超. 无线传感器网络拓扑的容错度与容侵度[J]. 电子学报, 2006, 34(8): 1446-1451.
WANG L M, MA J F, WANG C. Tolerance of intrusion and fault for topology of wireless sensor network[J]. Acta Electronica Sinica,2006, 34 (8): 1446-1451.

[10] DENG J, HAN R, MISHRA S. INSENS: intrusion-tolerant routing for wireless sensor networks[J]. Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, 2006, 29 (2): 216-230.

[11] 王良民, 马建峰. 基于再生技术的无线传感器网络容侵拓扑控制方法[J]. 计算机研究与发展, 2009, 46 (10):1678-1685.
WANG L M, MA J F. Self-regeneration based method for topology control with intrusion tolerance in wireless sensor networks[J].Journal of Computer Research and Development,2009, 46 (10):1678-1685.

[12] GEORGE T, BARAS J. On trust models and trust evaluation metrics for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006,24(2):318-328.

[13] MOHAMMAD M, SUHASH C, RAMI A. Can we trust trusted nodes in wireless sensor networks[A]. Proceeding of International Conference on Computer and Communication Engineering[C]. Kuala Lumpur, Malaysia, 2008. 1227-1232.

[14] ZHANG Q, YU T, *et al*. A framework for identifying compromised

（下转第 54 页）