无线传感器网络中基于组合框架的贝叶斯信任模型 *

鄢 旭[1], 陈 晶[2], 杜瑞颖[2], 刘松松[2]
(1. 江西旅游商贸学院 计算机学院,江西 330100; 2. 武汉大学 计算机学院, 武汉 430072)

摘 要: 针对无线传感器网络的特性,提出一种基于组合框架的贝叶斯信任模型(Bayes trust model based on combinatorial frame, BTM-CF)。该模型将通信可信与数据可信、直接通信和间接通信的信任区分开来,搭建多种信任综合评估的组合框架,进一步完善信任评估的考虑因素;利用贝叶斯定理处理通信可信与数据可信之间的关系,减少了信任机制建立、维护和更新本身消耗的能量,满足了节能的需求。通过对实验结果的分析,BTM-CF 能够敏感地识别自私节点或被盗用节点,当网络中存在多个节点盗用时,算法具有较好的健壮性。

关键词: 信任模型; 贝叶斯定理; 无线传感器网络
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)03-1078-06
doi:10.3969/j.issn.1001-3695.2012.03.077

Bayes trust model based on combinatorial frame in WSNs

YAN Xu[1], CHEN Jing[2], DU Rui-ying[2], LIU Song-song[2]
(1. *School of Computer*, *Jiangxi Tourism & Commerce College*, *Jiangxi* 330100, *China*; 2. *School of Computer*, *Wuhan University*, *Wuhan* 430072, *China*)

Abstract: This paper aimed at the traits of WSNs, and proposed a BTM-CF in WSNs. The BTM-CF protocol distinguished the direct and indirect communication, communication trust and data trust, as a result of this approach, it created the combinatorial frame to estimate trust synthetically for improving the trust factors. It utilized the Bayes theorem to deal with relationship of the data and communication trust, it also reduced the energy used for establishing, maintaining and updating trust. Through the comparison of experimental data, it slows that BTM-CF can identify selfish and embezzled nodes effectively, and the proposed arithmetic has a good robustness even when there are a huge number of malicious nodes.

Key words: trust model; Bayes theorem; wireless sensor networks(WSNs)

0 引言

无线传感器网络是由大量低成本且具有传感、数据处理和无线通信能力的传感器节点组成的,它独立于基站或移动路由器等基础通信设施,通过特定的分布式协议自组织形成网络。它能够协作地实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息,并对这些信息进行处理,使需要这些信息的用户在任何时间、任何地点和任何环境条件下(尤其是仅适合无线通信条件下)获取大量详实而可靠的信息,因而可以被广泛地应用于国防军事、国家安全、环境监测、交通管理、医疗卫生、制造业、反恐抗灾等领域[1]。

随着无线传感器网络应用的日趋增多,各种网络威胁、欺骗也开始流行起来。不同于一般的网络安全问题,传感器节点往往部署于野外,使得网络节点很容易被获取并被盗用,仅仅依靠密码技术的硬安全方法无法很好地解决此类问题。网络信任就是在这样的背景下提出来的,其通过研究节点之间的信任关系来确定节点的异常行为。在无线传感器网络中,节点间信任的建立是无线传感器网络进行节点正常通信的必要条件。因为无线传感器节点的操作、管理和生存竞争都依赖于传感器节点之间的协作和相互信任[2,3]。

当前研究者提出的信任模型主要在以下两个方面有所侧重[4]:

a)信任值初始化和异常行为判定。主要的思想是对观测得到的数据可以设置一个阈值,如果观测得到的数据超出了预先确定的阈值,则认为行为异常。

b)评估信任度。广大研究者采用了各种方法进行讨论,其中包括基于等级的[5,6]、基于权重的[7,8]、基于概率的[9,10]、基于神经网络的[11]、基于博弈论的[12]、基于模糊逻辑的[13,14]、基于群体智能的[15]和基于有向及无向图的[16]方法等。

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。针对关键服务,无线传感器网络的内部攻击可以分为分组丢弃、报文重发、篡改数据等。分组丢弃和报文重发是指恶意节点通过选择性转发或重发路由和数据分组,破坏网络的关键服务。篡改数据是指恶意节点修改并转发路由和数据分组,使得网络中其他节点接收错误信息。目前的信任模型尚未考虑针对两类攻击的组合框架。为了保证无线传感器网络能在节点被盗用情况下的安全正常

收稿日期: 2011-08-04; **修回日期**: 2011-10-08 **基金项目**: 国家自然科学基金资助项目(60903196, 60903175);国家新一代宽带无线移动通信网络重大专项(2010ZX03006-001-01); 江西省教育厅资助项目(GJJ10661);湖北省教育厅资助项目(D20114401)

作者简介: 鄢旭(1969-),男,副教授,硕士,主要研究方向为网络安全;陈晶(1981-),男,副教授,博士,主要研究方向为网络安全、无线网络(ever_cs@163.com);杜瑞颖(1964-),女,教授,博士,主要研究方向为网络安全、无线网络; 刘松松(1987-),男,硕士研究生,主要研究方向为网络安全、无线网络.

运行,本文提出一种基于组合框架的贝叶斯信任评估模型。该模型首先考虑到无线传感器网络节点中单跳和多跳邻居的区别,将通信可信与数据可信、直接通信和间接通信的信任利用贝叶斯定理进行组合评估;其次从节能角度出发,减少信任机制建立、维护和更新本身消耗的能量,从而能够更好地适应无线传感器网络多跳、能量受限的特点。

1　相关工作

Buchegger 等人[6] 提出了一个能容错的等级制系统,即指控或者奖励。每个节点为其他节点维持一个信誉等级和信任等级,并及时与其他节点交换第一手的信息;然后基于接收到的信息来更新信誉信息,并根据信誉信息评估信任等级。该系统介绍了信任等级重新评估以及信誉逐渐消失的过程。在该模型中,通过时间来确定证据的比重,对过去收到的观察报告给予较低的比重,而且各节点只公布第一手的信息,使得评估体系不够完善。

Crosby 等人[7] 提出一种无线传感器网络中基于信任的分布式框架和信任簇头选举机制。该模型利用了信任节点的直接和间接信息,针对丢包率、数据报文和控制报文数量三种参数,利用权值机制进行建模。每个节点存储一张周围邻居的信任表,并将信任列表报告给簇头。该方案同样没有考虑二手信息,所以信任评估过程较为主观。Hung 等人[8] 给出了一个基于信任的路由机制,能够找出基于数据包信任要求的转发路径,其也使用了权值机制,定义 WSNs 中的信任为转发包过程中的可信赖程度,但该模型集中关注通信可信度方面。

Crosby 等人[10] 利用 Beta 分布来表示信任的变化。该模型通过在 t 时段成功与不成功的交互数量来更新节点的信任值,并在抵抗 Sybil 攻击时保护用户匿名性,使用权重机制来确定直接或者间接的(好的和坏的)信息的权重。通过直接和间接的信息计算信任值以区分合作与不合作行为。对于可靠节点的二手信息给予更高的权值。信任值的计算结果与门限值进行对比,如果超过门限值,该节点被认为是可以信任的;否则拒绝合作。但是,该模型仅仅传递正面信誉信息,虽然可以限制流言攻击,但由于缺少负面信誉信息的交换,使得信任模型效率不高,能够适用的攻击类型受到限制。

Chen 等人[12] 提出一种网络环境下基于概率密度的信任博弈模型,将信任模型与研究网络环境相结合,把整个信任系统分为证据收集、基于概率密度的信任度量以及服务博弈三部分。证据收集模块利用数据挖掘和关联规则匹配进行信任证据的判断与评估。信任度量模块将信任细分为信任度和确定度,并按照熵原理使用概率密度函数来表现。通过服务博弈模块将度量结果结合支付矩阵进行博弈分析,计算出服务提供者行为的混合纳什均衡策略。对于拒绝合作的成员将会被逐步地清除出去。

Kim 等人[14] 运用模糊逻辑建立运算规则,计算节点间的信任关系。应用模糊逻辑来量化信任度有两个优点:a)在检测节点的安全参数时,fuzzy 推理可以量化不确定性或不精确数据;b)针对不同的应用,开发不同的函数和推理规则,而不需改变 fuzzy 推理引擎。但是该信任模型的缺点是:由于采用了模糊逻辑,在计算信任关系时容易丢失一些信息,造成信任关系计算不精确,该模型不提供间接信任关系计算。

Theodorakopoulos 等人[16] 的模型使用半环的理论来评估信任,信任关系被模型化为一个有向图中的路径问题,其中节点表示实体,边表示信任关系。在此模型中,用户可以使用来自于中间节点的二手信息来形成自己对别人的观点,那么用户不需要与其他节点建立直接的连接就可以进行评估。

2　假设条件

a)本文所采用的无线传感器网络为密集型网络,即大量的传感器节点密集部署,部署后传感器节点不随意移动。

b)攻击者有能力截获任何一个传感器节点,包括簇首和簇成员节点。并且攻击者具有和传感器网络中其他节点相当的计算和通信能力。

c)监测区域内节点在最大功率下可以直接与汇聚节点(或基站)进行通信。监测区域内节点的稳定功率远小于最大功率,在通信稳定时期,节点以稳定功率工作,持续监测周围现象,若覆盖范围无法到达汇聚节点,将采取多跳路由方式。

d)通信信道是对称的,即在信噪比一定的情况下,从节点 A 到节点 B 传输一个信息所消耗的能量与从节点 B 到节点 A 传输一个信息所消耗的能量相同[17]。

3　基于组合框架的贝叶斯信任模型

为了更好地节省节点能耗,采用稳定的多跳无线传感器网络分簇路由算法,簇内节点通过单跳路由同簇首节点通信,通过信息捎带的方式在通信时交换信任信息。本文提出基于框架的贝叶斯信任模型(BTM-CF),其节点的信任评价由通信可信度和数据可信度两部分组成。其中:通信可信度是指其他节点对于同该节点建立连接的可信度,数据可信度是指其他节点对于信任该节点传输的数据的可信度。首先由历史通信可信度和数据可信度生成节点信誉;然后按照贝叶斯定理进行信任计算生成节点的信任值。另外,节点也分为两类:第一类节点每次仅通过单跳路由和另一节点通信,第二类节点既通过单跳路由通信,也通过多跳路由同单跳不可达的节点通信。对于第一类节点来说,仅存在直接通信和直接数据,而无须统计间接通信和间接数据,从而可以节省能量消耗。BTM-CF 的模型如图 1 所示。

下面将分别介绍通信可信度、数据可信度以及 BTM-CF 信任度的计算方法。

1)通信可信度

所谓通信可信度,是基于一个节点与网络内的其他节点在路由信息之间的协作计算出的信任值。通信可信度可用图 2 简洁表示。

本文中由于信任值 $R \in [0,1]$,且各节点之间的信任值分布呈现随机性,根据熵原理,可以发现信任值的概率分布函数符合 Beta 分布。Beta 概率密度函数的表达式为

$$f(\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1} \tag{1}$$

用 p 表示某事件发生的概率,则有

$$p \sim \mathrm{Beta}(\alpha,\beta) \tag{2}$$

则由式(1)(2)可以得出事件的概率密度函数为

$$f(p|\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \tag{3}$$

其中:$0\leqslant p\leqslant 1,\alpha>0,\beta>0$。如果已知之前事件发生的次数为 m,事件不发生的次数为 s,那么在 Beta 分布中,有 $\alpha=m+1$,$\beta=n+1$。基于本文的实际应用目的,节点对应矩阵的取值有 $\Gamma=[\Gamma_{a,b}]=\begin{pmatrix}1001\\0110\\0110\\1001\end{pmatrix}$。由此可以推断出,如果节点 a 和节点 b 直接通信,则有 $\Gamma_{a,b}=\Gamma_{b,a}=1$;否则等于 0。

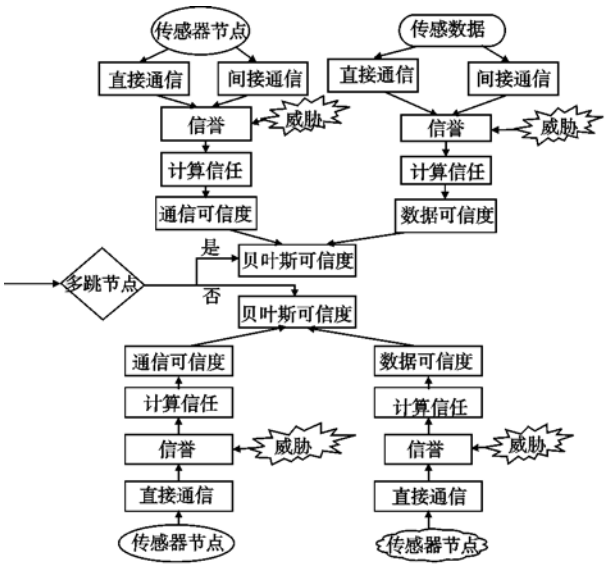

图1　基于组合框架的贝叶斯信任模型

对于节点 A 来说,信誉 R_{ab} 是节点 B 保存的节点 A 的信誉,该信誉以 Beta 模型体现,带有两个参数 α_{ab} 和 β_{ab}。α_{ab} 表示节点 A 成功与节点 B 通信或从节点 B 获取信息的数量,β_{ab} 表示 A 与 B 不成功通信的数量。节点 A 保存的节点 B 的信誉由式(4)定义:

$$R_{ab}=\mathrm{Beta}(\alpha_{ab},\beta_{ab}) \tag{4}$$

将信誉的期望作为信任值,由此也得到式(5):

$$T_{ab}=E(R_{ab})=E[\mathrm{Beta}(\alpha_{ab},\beta_{ab})] \tag{5}$$

定理 1　信任值 R 的概率分布函数可以写为 $f(x)=\frac{(m+n+1)!}{m!\ n!}x^m(1-x)^n$。其中:$m=\alpha-1$, $n=\beta-1$, $0\leqslant x\leqslant 1$, $\alpha>0$, $\beta>0$, α 和 β 分别表示正面证据数和负面证据数,收集到的证据总数为 $\alpha+\beta$。

证明　考虑基于熵原理并添加适当的约束条件推求这个概率密度分布函数,可以看出它是下面三个约束条件与熵原理的应用结果。

a)变量 x 的对数平均值为固定值(等价于几何平均值为常数):

$$u=\int_0^1(\ln x)f(x)\,\mathrm{d}x \tag{6}$$

b)$(1-x)$ 的对数平均值也是固定值:

$$v=\int_0^1\ln(1-x)f(x)\,\mathrm{d}x \tag{7}$$

c) 作为概率密度,当然还有

$$1=\int_0^1 f(x)\,\mathrm{d}x \tag{8}$$

根据上面的三个约束式和熵原理,利用拉格朗日方法,构造的 F 函数是

$$F=\int_0^1-f(x)\ln f(x)\,\mathrm{d}x+C_1[(\int_0^1 f(x)\,\mathrm{d}x)-1]+C_2[(\int_0^1\ln x f(x)\,\mathrm{d}x)-u]+C_3[(\int_0^1\ln(1-x)f(x)\,\mathrm{d}x)-v] \tag{9}$$

求 F 对未知的概率密度 $f(x)$ 的偏微分,并且令它等于 0(利用熵原理),得到

$$f(x)=e^{C_1-1}x^{C_2}(1-x)^{C_3} \tag{10}$$

通过式(3)和(5),可得

$$e^{C_1-1}=1/B(C_2+1,C_3+1) \tag{11}$$

将等式(6)代入(5),可得

$$f(x)=\frac{1}{B(C_2+1,C_3+1)}x^{C_2}(1-x)^{C_3} \tag{12}$$

通过 u、v 的约束式即等式(1)(2)可以求出 C_2 和 C_3,最后可以得到概率密度分布函数

$$f(x)=\frac{1}{B(\alpha,\beta)}x^{\alpha-1}(1-x)^{\beta-1}$$
$$0\leqslant x\leqslant 1,\ \alpha>0,\ \beta>0 \tag{13}$$

$B(\alpha,\beta)$ 的含义是 $B(\alpha,\beta)=\int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\,\mathrm{d}x$。并且 $B(\alpha,\beta)=\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}$。其中:$\Gamma(x)$ 为 Gamma 分布,所以概率分布函数可以写为 $f(x)=\frac{(m+n+1)!}{m!\ n!}x^m(1-x)^n$,其中 $m=\alpha-1$, $n=\beta-1$, $0\leqslant x\leqslant 1$, $\alpha>0$, $\beta>0$, α 和 β 分别表示正面证据数和负面证据数,收集到的证据总数为 $\alpha+\beta$。

以上表述的是节点 A 通过直接与节点 B 通信获得的信任值,而在无线传感器网络中,为了节省能耗,保障通信的可靠性,某两个节点不可避免的需要通过多跳路由的形式通信,这就引出了间接通信信息的概念。所谓间接通信,是指节点 A 经由节点 C 与节点 B 进行通信,节点 A 从节点 C 得到节点 C 保存的节点 B 的信誉 R_{cb},及参数 α_{cb}、β_{cb}。得到新的信任信息之后,节点 A 需要将新的信任信息与其原本保存的信息进行一个综合评价,由此可以引出式(14):

$$NR_{ab}=\mathrm{Beta}(N\alpha_{ab},N\beta_{ab}) \tag{14}$$

其中:

$$N\alpha_{ab}=\alpha_{ab}+\frac{2\times\alpha_{ab}\times\alpha_{cb}}{(\beta_{ac}+2)\times(\alpha_{cb}+\beta_{cb}+2)+(2\times\alpha_{ac})} \tag{15}$$

$$N\beta_{ab}=\beta_{ab}+\frac{2\times\alpha_{ac}\times\beta_{cb}}{(\beta_{ac}+2)\times(\alpha_{cb}+\beta_{cb}+2)+(2\times\alpha_{ac})} \tag{16}$$

$$E[\mathrm{Beta}(N\alpha_{ab}+1,N_{ab}\beta+1)]=\frac{(N\alpha_{ab}+1)}{(N\alpha_{ab}+N_{ab}\beta+2)} \tag{17}$$

其中:$N\alpha_{ab}$ 表示最新的 α_{ab};$N\beta_{ab}$ 表示最新的 β_{ab};CT 表示通信可信度。

2)数据可信度

数据可信度是基于无线传感器网络节点实际接收的有效数据计算出的信任值。数据可信度模型如图 3 所示。

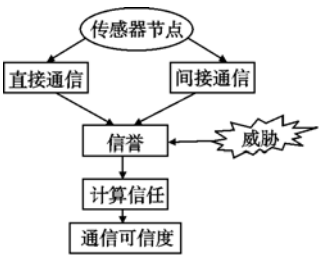

图2　通信可信度计算模型

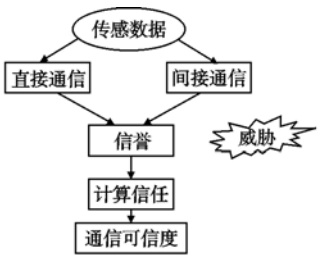

图3　数据可信度计算模型

在仅考虑获取直接信息的情况下,数据可信度中的信誉和信任分别由式(10)和(11)表示:

$$R_{ab} = N(m_{ab}, s_{ab}^2) \tag{18}$$

$$T_{ab} = P\{|q_{ab}| < e\} = P\{-e < q_{ab} < +e\} = f\left(\frac{e - m_{ab}}{s_{ab}}\right) - f\left(\frac{-e - m_{ab}}{s_{ab}}\right) \tag{19}$$

其中:μ_{ab}表示错误数据的平均值,$\mu_{ab} = \frac{(\mu_0/\sigma_0^2) + (k\overline{y_{ab}}/\tau^2)}{(1+\sigma_0^2) + (k/\tau^2)}$,$\tau$是节点传输误差;$\overline{y_{ab}}$为节点 A 向节点 B 传递错误数据的平均值;k 传感器网络中所有节点的传输误差系数;σ_{ab}^2表示方差。

$$\sigma_{ab}^2 = \frac{1}{(1/\sigma_0^2) + (k/\tau^2)} \tag{20}$$

考虑到间接获取的信息,平均值表示为 $N\mu_{ab}$,方差 $N\sigma_{ab}^2$,由高斯分布可得:

$$N\mu_{ab} = \frac{(\mu_0/\sigma_0^2) + \sum_{i=1}^{n}\frac{(\mu_{ib} + \mu_{ai})}{(\frac{1}{T_{ai}} - 1)}\varphi + (k\overline{y_{ab}}/\tau^2)}{(1/\sigma_0^2) + \sum_{i=1}^{n}\frac{1}{(\frac{1}{T_{ai}} - 1)}\varphi + (k/\tau^2)} \tag{21}$$

$$N\sigma_{ab}^2 = \frac{1}{(1/\sigma_0^2) + \sum_{i=1}^{n}\frac{1}{(\frac{1}{T_{ai}} - 1)\varphi} + (k/\tau^2)} \tag{22}$$

由以上公式可得出考虑直接信息和间接信息的情况下,数据可信度由式(23)表示:

$$DT = \varphi\left(\frac{\varepsilon - N\mu_{ab}}{N\sigma_{ab}^2}\right) - \varphi\left(\frac{-\varepsilon - N\mu_{ab}}{N\sigma_{ab}^2}\right) \tag{23}$$

3)贝叶斯信任度计算

由前面的分析可知,BTM-CF 将信任值分为通信可信度和数据可信度两个部分。如何将两部分信任值结合起来便是接下来需要研究的问题,本文采用开销较小的贝叶斯算法对两部分信任进行融合(图 4),以满足无线传感器网络能量受限的特点。

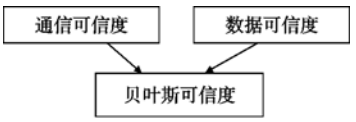

图4　贝叶斯信任度

由贝叶斯算法可以得出节点信任值:

$$P(T|DT, CT) = \frac{P(DT|T, CT) \times P(T|CT)}{P(DT|CT)} \tag{24}$$

当两节点仅进行了通信而没有传输数据时,有

$$P(DT|T, CT) = P(DT|T) \tag{25}$$

由此可得

$$P(T|DT, CT) = \frac{P(DT|T) \times P(T|CT)}{P(DT|CT)} \tag{26}$$

由贝叶斯式可得

$$P(DT|T) = \frac{P(T|DT) \times P(DT)}{P(T)} \tag{27}$$

由此可得

$$P(T|DT, CT) = \frac{P(T|DT) \times P(T|CT) \times P(DT)}{P(DT|CT) \times P(T)} \tag{28}$$

忽略不重要的影响因素和常数,可得

$$P(T|DT, CT) = P(T|DT) \times P(T|CT) \tag{29}$$

本文提出的贝叶斯信任模型,信任度的计算分为两类,即对于簇内节点来说,通信可信度和数据可信度分别为

$$CT_{ab} = E(R_{ab}) = E[\mathrm{Beta}(\alpha_{ab} + 1, \beta_{ab} + 1)] = \frac{(\alpha_{ab} + 1)}{(\alpha_{ab} + \beta_{ab} + 2)} \tag{30}$$

$$DT_{ab} = P\{|\theta_{ab}| < \varepsilon\} = P\{-\varepsilon < \theta_{ab} < +\varepsilon\} = \varphi\left(\frac{\varepsilon - \mu_{ab}}{\sigma_{ab}}\right) - \varphi\left(\frac{-\varepsilon - \mu_{ab}}{\sigma_{ab}}\right) \tag{31}$$

簇首节点的通信可信度和数据可信度分别为

$$CT_{ab} = E(NR_{ab}) = E[\mathrm{Beta}(N\alpha_{ab} + 1, N_{ab}\beta + 1)] = \frac{(N\alpha_{ab} + 1)}{(N\alpha_{ab} + N_{ab}\beta + 2)} \tag{32}$$

$$DT_{ab} = \varphi\left(\frac{\varepsilon - N\mu_{ab}}{N\sigma_{ab}^2}\right) - \varphi\left(\frac{-\varepsilon - N\mu_{ab}}{N\sigma_{ab}^2}\right) \tag{33}$$

4　实验结果及分析

由于无线传感器网络节点数量多,实验成本高昂。为了验证算法的效率及安全性,与其他无线传感器相关研究一样,本文将在 NS2 仿真实验环境下对算法的各方面性能进行验证。

4.1　对比协议的选择

由于当前研究者从不同角度用不同方法对无线传感器网络的信任模型进行了研究。为了能够说明 BTM-CF 的有效性,本文从信任模型建模方法和信任更新因素两方面进行总结,对一些协议按表 1 和 2 进行归纳。由于 BTM-CF 属于概率算法,同类型模型的比较往往更具有说明意义,所以本文选择同属于概率算法的 CRT[10] 进行比较。

表 1　信任模型建模方法

信任建模方法	参考文献
等级机制	[6]
权值机制	[7, 8]
概率算法	[9,10], BTM-CF
神经网络	[11]
博弈原理	[12]
模糊逻辑	[13, 14]
群体智能	[15]
有向及无向图	[16]

4.2　仿真实验设置

1)场景设置

为了使仿真实验的结果更为准确、真实,在本文实验设计中,目标监测区域为定为 400 m×200 m,监测区域内的传感器节点数目为 300 个;为了全面地验证算法的有效性,在仿真过程中,将设置如下五组实验以便对比;为了使得实验结果更具有可比性,本文仿真路由都采用的是无线传感器网络中的 LEACH 协议[18]。

表 2　实验测试组设置

测试组	攻击节点数目(占每个簇总节点数的%)	攻击持续时间/%	攻击类型
测试组 1	0	0	无
测试组 2	10	100	持续
测试组 3	10	50	间断
测试组 4	20	100	持续
测试组 5	30	100	持续

在测试组 1 中,假设无线传感器网络中不存在攻击,主要是检验 CRT、BTM-CF 在网络性能上带来的影响。在测试组 2 中,假设每个簇中存在一个攻击节点,通过节点在连续攻击和间隔攻击时的信任值波动情况,验证提出模型的可靠性和可行

性。测试组 4 和测试组 5 的设置主要是为了测试提出算法在大规模攻击情况下的健壮性。

2）实验参数设置

传感器节点初始能量设定为 10 J，发送信息和接收信息时电路消耗的能量为 Estatic = 50 nJ/bit，发送信息时，信号放大器模块消耗的能量为 Eamp = 100 pJ/bit × m^2，在 LEACH 分簇中，第一轮节点成为簇首的概率阈值 $T(n)$ 为最优值 0.05，所有生成的随机数小于阈值的节点成为簇首。

4.3　性能分析

为了分析提出的方案，本文将比较 LEACH、CRT 和 BTM-CF 在不同情况下的性能情况。报文投递率是成功传输报文同所有传输报文的比率，可以有效地反映出算法对保障网络中节点之间安全、可靠通信的能力。在实验验证过程中，主要针对三个方面对算法进行验证：节点信任模型在识别被盗用节点表现出的敏感性；在存在节点盗用的情况下，基于贝叶斯信任模型受盗用节点影响程度；网络中存在多个节点盗用时，算法的健壮性。

1）算法的节点盗用敏感性

为了考察算法对节点盗用的敏感性，主要考察在存在节点盗用情况下节点信任值的变化，在节点信任值的变化考察阶段，主要进行测试组 1、2 设置的实验。

在测试组 1 中，网络内不存在被盗用的节点，三种算法的报文投递率如图 5 所示。由图可以看出，LEACH、CRT 和 BTM-CF 三种算法的报文投递率都相对稳定，LEACH 稳定在 76%-84% 间，CRT 稳定在 68%74% 间，而 BTM-CF 稳定在 71%81% 间。从总体上看，在此情况下三者的报文投递率都比较接近且稳定，其中 LEACH 的均值最高。这是由于 CRT 和 BTM-CF 在 LEACH 协议的基础上增加了一定的通信负载，所以性能略有损失，而且相对于 BTM-CF，CRT 损失更大一些。

在测试组 2 中，簇内有 10 % 的被盗用节点，攻击类型为持续攻击，即被盗用节点持续性地进行无效通信和传送虚假数据。网络中的报文投递率变化如图 6 所示。初始时 LEACH 协议略高于 CRT 和 BTM-CF，随着时间的推移，LEACH 协议的报文投递率逐渐下降，而 CRT 和 BTM-CF 协议逐渐上升。由此可以看出，当网络中存在被盗用节点时，CRT 和 BTM-CF 在一定时间内可以正确识别恶意或异常节点并将之隔离，最终的报文投递率接近于无被盗用节点时，两者具有较好的节点盗用敏感性，从而保证网络的正常通信。由于 CRT 主要关注的是正面证据的收集，所以该协议的收敛速度比 BTM-CF 要快，但是 BTM-CF 的稳定水平要高于 CRT。

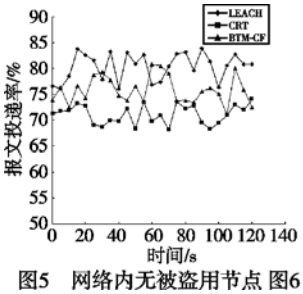

图5　网络内无被盗用节点

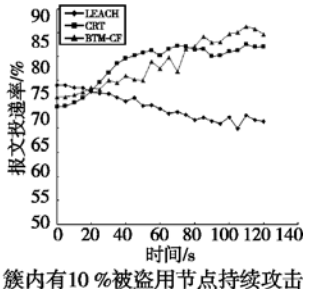

图6　簇内有10 %被盗用节点持续攻击

2）受盗用节点影响程度

在测试组 3 中，簇内有 10 % 的被盗用节点，攻击类型为间断攻击，报文投递率如图 7 所示。从图 7 中可以发现，由于是周期性的间断攻击，两种协议的报文投递率都随着攻击的发生而产生周期性的波动。显然，LEACH 受被盗用节点的影响要严重得多，未发生攻击时，报文投递率可达 40 %50 %，而攻击发生时大约只有 20 %30 %。相对而言，CRT 的情况要好一些，但是由于缺乏负面证据的分析，使得 CRT 在间断攻击的影响下，报文投递率曲线与 LEACH 协议相似，而 BTM-CF 则相对平稳得多，一直保持在 50 %65 % 间。由此可以得出两个结论：a）对于信任模型而言，间断攻击比持续性攻击的影响更大，而且更加难以准确定位；b）BTM-CF 相对于 CRT 具有更强的抗间断攻击能力，在间断攻击的情况下，BTM-CF 的报文投递率更加平滑稳定，而且均值较高。

3）算法的鲁棒性

为了考察算法的健壮性，分别在测试组 4 和 5 中安置了 20 % 和 30 % 的被盗用节点。报文投递率如图 8 所示。

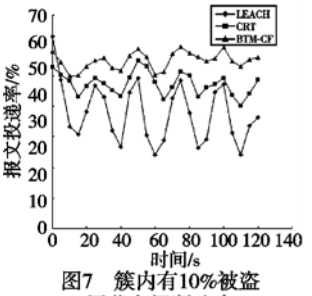

图7　簇内有10%被盗用节点间断攻击

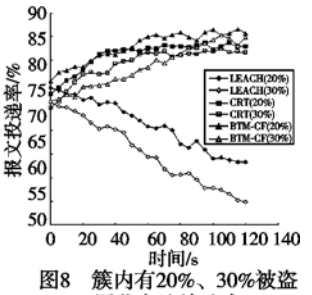

图8　簇内有20%、30%被盗用节点连续攻击

由图 8 的对比实验可以看出，在网络存在盗用节点较多的持续攻击情况下，随着时间的增加，LEACH 协议报文投递率呈下降趋势，而 CRT 和 BTM-CF 的报文投递率逐渐升高并最终达到稳定状态。另外，当网络中被盗用节点数增加时，对于性能会有更大的影响。而随着时间的推移，不论是 20 % 还是 30 % 的被盗用节点，BTM-CF 协议最终报文投递率在 75 % 左右达到稳定，而 CRT 协议最终的稳定状态在 72 % 左右。两种协议在 20 % 盗用节点的场景下，达到稳定的时间更短。但是在持续攻击下，CRT 收敛的时间要短于 BTM-CF。由此可以看出，相对于 CRT，BTM-CF 具有良好的算法鲁棒性但是收敛性稍有不如。

5　结束语

由于无线传感器网络节点多处于无人值守的网络环境中，节点盗用可能成为整个无线传感器网络的致命威胁，有时即使只存在一个恶意或自私节点，也可能造成网络故障甚至是整个网络崩溃。因此，确认网络节点是否可信成为无线传感器网络安全研究的一个重要话题。本文针对无线传感器网络事件发生随机性的特点，依据概率论进行数学分析，提出一种基于组合框架的贝叶斯信任模型，通过将通信可信与数据可信、直接通信和间接通信区分计算，使得提出的模型能够更好地适应无线传感器网络环境。在未来的工作中，拟对该模型作进一步改善，通过博弈论进行机制设计，提高模型的收敛速度，使得模型更加实用、有效。

参考文献：

[1]　MARMOL F G，PEREZ G M. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems [J].

Computer Standards & Interfaces,2010,32(4):185-196.

[2] YAO Z Y,KIM D,DOH Y. PLUS:parameterized and localized trust management scheme for sensor networks security[C]//Proc of the IEEE International Conference on Mobile Ad hoc and Sensor Systems. Piscataway: IEEE Computer Society,2006:437-446.

[3] JI Wen,YANG Shou-bao,WEI Dong,*et al*. GARM:a group-anonymity reputation model in peer-to-peer system[C]//Proc of the 6th International Conference on Grid and Cooperative Computing. New York: ACM Press,2007:32-40.

[4] BOUKERCHEA,LI Xu. ATRM:an agent-based trust and reputation management scheme for wireless sensor networks[C]//Proc of Global Telecommunications Conference. New York:IEEE Press,2005:1857-1861.

[5] JONKER C M,SCHALKEN J J P,THEEUWES J,*et al*. Human experiments in trust dynamics[C]//Proc of the 2nd International Conference on Trust Management. 2004:206-220.

[6] BUCHEGGER S,BOUDEC J Y L. A robust reputation system for peer-to-peer and mobile Ad hoc networks[C]//Proc of P2PEcon'04. Cambridge MA:Harvard University,2004.

[7] CROSBY G V,PISSINOU N,GADZE J. A framework for trust-based cluster head election in wireless sensor networks[C]//Proc of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems. Washington DC:IEEE Computer Society,2006:13-22.

[8] HUNG K S,LUI K S,KWOK Y K. A trust-based geographical routing scheme in sensor networks[C]//Proc of IEEE Wireless Communications and Networking Conference. 2007:3123-3127.

[9] ZOURIDAKI C,MARK B L,HEJMO M,*et al*. A quantitative trust establishment framework for reliable data packet delivery in MANETs [C]//Proc of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks. New York:ACM Press,2005:1-10.

[10] CROSBY G V,PISSINOU N. Cluster-based reputation and trust for wireless sensor networks[C]//Proc of IEEE Consumer Communications and Networking Conference. 2007:604-618.

[11] BAOHUA H,HEPING H,ZHENGDING L. Identifying local trust value with neural network in P2P environment[C]//Proc of the 1st IEEE and IFIP International Conference in Central Asia on Internet. 2005.

[12] CHEN Jing, DU Rui-ying. A trust game method basing on probability model in networks[J]. Chinese Journal of Electronics,2010,38(2):427-433.

[13] CASTELFRANCHI C,FALCONE R,PEZZULO G. Integrating trustfulness and decision using fuzzy cognitive maps[C]//Proc of the 1st International Conference on Trust Management. Berlin:Springer-Verlag,2003:195-210.

[14] KIM T K,SEO H S. A trust model using fuzzy logic in wireless sensor network[C]//Proc of World Academy of Science, Engineering and Technology. 2008:2070-3740.

[15] JIANG T,BARAS J S. Ant-based adaptive trust evidence distribution in MANET[C]//Proc of the 24th International Conference on Distributed Computing Systems Workshop. 2004:588-593.

[16] THEODORAKOPOULOS G,BARAS J S. On trust models and trust evaluation metrics for Ad hoc networks[J]IEEE Journal on Selected Areas in Communications,2006,2(24):318-328.

[17] GUAN Shang-yuan, WU Wei-guo, DONG Xiao-she,*et al*. Survey of trust management in open distributed environments[J]. Computer Science,2010,3(37): 22-28.

[18] BANDYOPADHYAY S,COYLE E J. An energy efficient hierarchical clustering algorithm for wireless sensor networks[C]//Proc of IEEE Wireless Communications and Networking Conference. [S. l.]:IEEE Press, 2003:1713-1723.

(上接第 1077 页)

[9] SIBERT H, DEHORNOY P, GIRAULT M. Entity authentication schemes using braid word reduction[EB/OL]. [2011-08-15]. http://eprint. iacr. org/2002/187.

[10] LAL S,CHATURVEDI A. Authentication schemes using braid groups [EB/OL]. [2011-08-15]. http://arXiv. org/cs. CR/0507066.

[11] 汤学明, 洪帆, 崔国华. 辫群上的公钥加密方案[J]. 软件学报, 2007,18(3):722-729.

[12] KO K H, CHOI D H, CHO M S, *et al*. New signature scheme using conjugacy problem[EB/OL]. [2011-08-15]. http://eprint. iacr. org/2002/168.

[13] THOMAS T, LAL A K. Group signature scheme using braid groups [EB/OL]. [2011-08-15]. http://arXiv. org/cs. CR/0602063.

[14] VERMA G K. Blind signature schemes over braid groups[EB/OL]. [2011-08-15]. http://eprint. iacr. org/2008/027.

[15] VERMA G K. A proxy signature scheme over braid groups[EB/OL]. [2011-08-15]. http://eprint. iacr. org/2008/160.

[16] 张利利, 曾吉文. 基于辫群的代理签名方案[J]. 数学研究, 2008, 41(1):56-64.

[17] LAL S,VERMA V. Some proxy signature and designated verifier signature schemes over braid groups[EB/OL]. [2011-08-15]. http://arXiv. org/cs. CR/09043422.

[18] VERMA G K. A proxy blind signature scheme over braid groups[J]. International Journal of Network Security,2009,9(3): 214-217.

[19] 郑东, 张彤, 陈克非,等. 基于比特承诺的电子彩票方案[J]. 电子学报, 2000, 28(10): 141-142.

[20] 钟鸣, 杨义先. 一种基于比特承诺的部分盲签名方案[J]. 通信学报, 2001,22(9)1-6.

[21] 万武南, 索望, 陈运. 基于 Bit 承诺的合同网模型[J]. 计算机工程, 2009,35(19):1-3.

[22] WANG L C, CAO Z F, CAO F, *et al*. Biased bit commitment and applications[J]. Journal of Information Science and Engineering,2008,24:441-452.

[23] MYASNIKOV A, SHPILRAIN V,USHAKOV A. A practical attack on a braid group based cryptographic protocol[C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag,2005:86-96.

[24] MYASNIKOV A, USHAKOV A. Length based attack and braid groups: cryptanalysis of Anshel-Anshel-Goldfeld key (AAGK) exchange protocol[C]//Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2007:76-88.

[25] GONZALEZ-MENESES J. Improving an algorithm to solve multiple simultaneous conjugacy problems in braid groups[J]. Contemporary Mathematics,2005,372:35-42.

[26] KALKA A G. Representation attacks on the braid Diffie-Hellman public key encryption[J]. Application of Algebra Engineering, Communication and Computer,2006,17:257-266.