基于无线传感器网络的信誉形式化模型*)

肖德琴[1,2] 冯健昭[1] 杨 波[1] 张焕国[2]
(华南农业大学信息学院计算机科学与工程系 广州 510642)[1]
(武汉大学软件工程国家重点实验室 武汉 430072)[2]

摘 要 无线传感器网络的安全威胁不仅发生在节点之间传递信息的时候,还发生在节点产生信息的时候,因此,单靠密码学和认证无法阻止传感器网络内部的攻击以及节点的异常行为。本文提出了一种基于无线传感器网络的信誉形式化模型,该模型形式化地描述了传感器节点信誉的表示、更新和整合。同时,通过对信誉分布和β分布的拟合分析与推理,发现β分布可以很好地描述与实现上述方案,由此设计了一个基于β分布的无线传感器网络信誉系统实例。实验表明,本信誉方案有较好的稳定性,能够抵抗诽谤攻击和信誉欺骗攻击,很好地解决无线传感器网络对数据认证的需求。

关键词 无线传感器网络,数据认证,信誉,β分布

Reputation Formal Model for Wireless Sensor Network

XIAO De-Qin[1,2] FENG Jian-Zhao[1] YANG Bo[1] ZHANG Huan-Guo[2]
(College of Information, South China Agriculture University, Guangzhou 510642)[1]
(State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072)[2]

Abstract Security threat can happen in a wireless sensor network not only while relaying information to the end-user but also while generating information. So, the conventional view of security based on cryptography and authentication alone is not sufficient for the unique characteristics and misbehaviors encountered in wireless sensor networks. A reputation formal model is proposed for wireless sensor networks, it provides a formal description method to sensors for reputation representation, update and integration. On the other side, the beta distribution system is founded to be fit for description reputation system by proving properties of beta reputation system; so, a case system based on beta distribution is developed. Simulation results show this scheme not only can keep stable reputation but also can prevent the system from some attacks as bad mouthing and reputation cheating.

Keywords Wireless sensor networks, Data authentication, Reputation, Beta distribution

1 引言

无线传感器网络(Wireless Sensor Networks, WSN)是当前国际上备受关注的、涉及多学科高度交叉、知识高度集成的前沿热点研究领域。它综合了传感器技术、嵌入式技术、现代网络及无线通信技术、分布式信息处理技术等,能够通过各类集成化的微型传感器协作地实时监测、感知和采集各种环境或监测对象的信息。传感器网络具有十分广阔的应用环境,在军事国防、工农业、城市管理、生物医疗、环境监测、抢险救灾、危险区域远程监控等许多重要领域都有潜在的使用价值。

但是,这些无线传感器网络节点分布非常稠密,由于节点本身受资源的限制导致它们很容易出现故障和差错。不同于计算机网络安全的是,以往的手段注重保障传输安全,即可以实现数据源实体和数据完整性的检测,但不能实现数据合法性的验证。作为信息采集为根本用途的无线传感器网络更加需要对数据的合法性进行验证(简称为数据认证),因为其安全威胁不仅发生在节点之间传递信息的时候,还发生在节点产生信息的时候,这很容易被攻击者利用。然而,数据认证不同于数据完整性,带消息认证的节点能够检验数据的一致性,但无法检验它的合法性,因为节点产生的源数据可能是恶意的。同时,作为内部攻击节点可以访问到有效的密钥,密码学无法解决这类攻击。

当前比较典型的保证传感器节点通信安全的协议大都是基于密码学的,如 SPINS[1]、TinySec[2]、INSENS[3]、TinyPK[4]、SERP[5]、SEF[6]等,其核心都是密钥的建立和管理,它们都存在无法解决无线传感器网络的数据认证的安全需求。

近年来,基于信任管理的信誉模型在人类社会网络、电子商务、802.11 网络、对等网络等不同领域得到了应用[7~9],本文借鉴了信任管理的思想来建立安全的无线传感器网络,提出了一种无线传感器网络的信誉形式化模型(Reputation Formal Model for Wireless Sensor Network, RFM-WSN)。该方案在对信誉、信任、授权、事件、信誉模型均进行形式化描述基础上,系统地描述了网络节点信誉的表示、更新和整合。根据对信誉分布和β分布的拟合分析与证明,引用贝叶斯定理设计了一个基于β分布的无线传感器网络信誉系统实例,显示了本文所述方法的可行性。实验表明,本方案有较好的稳定性,能够抵抗诽谤攻击和信誉欺骗攻击,很好地解决无线传感器网络对数据认证的需求。

下面将首先给出无线传感器网络信誉模型的形式化定义,然后在第三部分将信誉分布和β分布进行拟合分析,设计一个基于β分布信誉系统实例,并进行仿真实验分析。最后

*)本文研究得到国家自然科学基金"无线传感器网络传输控制协议研究"(项目编号:60573115)和"分布式系统管理中的信任研究"(项目编号:60573043)资助。肖德琴 副教授,硕士生导师,硕士,博士生,主要研究领域为信息安全和无线传感器网络。冯健昭 研究生,主要研究方向为计算机网络与安全。杨 波 教授,博士,主要研究方向为密码与信息安全。张焕国 教授,博士生导师,主要研究方向为可信与信息安全。

在小结部分指出应用本方案的注意事项和下一步要研究的问题。

2 信誉形式化模型描述

在描述信誉、信任、事件、授权行为和信誉模型的形式化定义之前，首先对相关的符号进行如下说明：

i，j，k：表示传感器网络节点；

t：表示时段变量，取值为 0、1、2、…，时段的边界表示时刻，不发生混淆时 t 时段的左边界是 $t-1$ 时刻，右边界是 t 时刻；

$(S)_t$：表示变量在时段 t 的取值，当 $t=0$ 时表示变量 S 的初始化值，用 $(S)_0$ 表示；

S'：表示变量 S 下一时刻的动作或取值，这里采用了时序逻辑描述状态的记法[10]；

X_{ij}：表示节点 i 保存的关于节点 j 的信誉分布，是一随机变量；

T_{ij}：表示节点 i 保存的关于节点 j 的信任，是 X_{ij} 的数学期望；

$\sim$：表示服从，如 $X_{ij}\sim U(0,1)$ 表示 X_{ij} 服从均匀分布；

E_{ij}：表示节点 j 对 i 发起的一次事件；

□：表示证明与推理结束。

根据上面的符号说明，就可以对信誉、事件和信誉模型等概念进行形式化定义了。

定义 1(信誉) 信誉定义为一个实体对另一个实体的评价，被看作一种概率分布。

信誉分为直接信誉和间接信誉两种，直接信誉来自于 i 对 j 的直接评价，间接信誉是 i 得到的所有第三方节点 k 对 j 的间接综合评价信息。如直接信誉和间接信誉分别用 $(X_{ij})_D$ 和 $(X_{ij})_{ID}$ 表示，节点的信誉由两者加权求和计算而得，如式(1)所示：

$$X_{ij}=(X_{ij})_D\oplus(X_{ij})_{ID} \tag{1}$$

其中，用符号⊕来指明这种加权求和运算，具体定义请参考后面第 3 节的实例部分的阐述。它满足交换律和结合律，权值因系统的不同可能有所变化。

定义 2(信任) 信任 T_{ij} 是节点 i 对节点 j 将要发生行为的主观期望，即计算两个节点之间信誉概率分布的统计期望，T_{ij} 表示节点 i 对节点 j 的信任。与信誉不同的是，信任是一个数值，用式(2)来表达：

$$T_{ij}=E[X_{ij}] \tag{2}$$

定义 3(授权) 当一个实体(主动实体)向另一个实体(被动实体)请求通信(授权或资源)时，被动实体对主动实体的请求所采取的通信行为称为授权。节点 i 对 j 的授权行为 B_{ij} 依赖于节点 i 对 j 的信任，B_{ij} 是二值变量{合作，不合作}，采用网络信任阈值 θ_0 来决定 B_{ij} 的值：

$$B_{ij}=\begin{cases}\text{合作} & \forall T_{ij}\geqslant\theta_0\\ \text{不合作} & \forall T_{ij}<\theta_0\end{cases} \tag{3}$$

值得一提的是，即使 $B_{ij}=$“合作”说明节点 i 愿意与节点 j 进行下一次通信，但不一定能够保证通信成功，这是因为节点 j 可能出现系统故障或电源殆尽等异常行为。

定义 4(事件) 一个事件是指发生在实体之间的一次授权行为的触发、应答的完整过程，用 E_{ij} 表示节点 j 对节点 i 发起的一次事件。事件发生后，有可能成功(或可信，用逻辑“1”表示)，也有可能失败(或不可信，用逻辑“0”表示)。

为简便起见，事件发生后的取值仍然用 E_{ij} 表示。事件取值只有“1”和“0”两种情况，是对客观通信事实的描述，符合二项分布，用函数 $B(m+n,x)$，其中 m 表示某时段成功通信事件发生的总次数，n 表示某时段失败通信事件发生的总次数，x 表示成功事件发生的概率。本文中，用 $(E_{ij})_t$ 表示 t 时段发生的一组事件。显然，$B_{ij}=$“合作”是一个事件可以通信的前提，但不能保证事件通信一定能成功，即 $(E_{ij})_t$ 不一定能取 1，当 $(E_{ij})_t=1$ 表示行为正常，当 $(E_{ij})_t\neq1$ 时，说明行为异常，这正表达了事件实际行为与期望行为的差异，正可以作为判定行为异常的标准。

定义 5(信誉模型) 信誉模型是指对整个网络系统各个节点间信誉的建立、更新和整合的一套机制，其目的根据信誉的分布状况计算其信任，为节点下一步行为授权与否提供决策依据。

通常，一个网络信誉模型的建立包括以下几个主要步骤：

(1)系统初始化，设定各项初始参数；

(2)直接信誉更新；间接信誉更新；

(3)信誉整合；

(4)计算信任；

(5)行为决策。根据信誉，判定对下一步授权请求做出合作或不合作响应。

(6)异常行为分析。根据信誉和信任，判定某一行为或某时段行为是否异常。

3 基于 β 分布的 RFM-WSN 应用实例

本节描述一个基于贝叶斯公式的基本系统实例，该系统是在 RFM-WSN 模型下设计的，首先对贝叶斯公式进行简要说明，然后根据信誉系统的建立步骤进行实例应用分析。同时对拟采用的 β 分布与信誉分布进行拟合分析与推理。

贝叶斯公式是用来计算信誉的概率，参考概率论原理[11]，贝叶斯公式表达如下：

$$P(H_j|A)=\frac{P(H_j)P(A|H_j)}{\sum_{i=1}^{n}P(H_i)P(A|H_i)}\quad(j=1,2,\cdots,n) \tag{4}$$

其中 $H_1,H_2,\cdots,H_n$ 为样本空间 Ω 的一个划分，且诸 $P(H_i)>0$，A 为样本空间的任意事件，$P(A)>0$。为了用贝叶斯公式表示信誉系统，在 t 时段信誉 X_{ij} 分布的先验概率用 $(X_{ij})_{t-1}$ 表示，当节点 i 与节点 j 之间在 t 时段发生一组事件 $(E_{ij})_t$ 后，信誉分布的概率用 $(X_{ij})_t$ 表示，代表后验概率，代入公式(4)，得到如(5)所示的后验概率计算公式。

$$(X_{ij})_t=\frac{(X_{ij})_{t-1}*P((E_{ij})_t|(X_{ij})_{t-1})}{\text{归一化全概率}}\quad(l=1,2,\cdots) \tag{5}$$

理论上说来，很多分布如 β 分布、高斯分布、泊松分布、二项分布等都能够表示节点的信誉。下面对信誉分布与 β 分布的拟合分析与推理，发现 β 分布可以非常方便地描述信誉分布，本文采用 β 分布来表示节点的信誉。β 分布函数由两个参数组成，记为 $\beta(a,b)$，为描述简化，引入 γ 函数来表示 β 分布，即：

$$\beta(a,b)=\frac{\gamma(a+b)}{\gamma(a)\gamma(b)}x^{a-1}(1-x)^{b-1}$$

$$\forall\,0<x<1,a>0,b>0 \tag{6}$$

其中，$\gamma(n+1)=n!$，是一个阶乘函数。

3.1 初始化

系统启动时，由于还没有开始进行通信，在没有先验知识情况下，假定信誉在(0,1)中服从均匀分布，记为 $U(0,1)$，其

后验概率分布可由下面的性质1得到保证。

性质1 若信誉$(X_{ij})\sim U(0,1)$，当节点i已经与节点j交互了$m+n$次事件(其中m次成功，n次失败)后，其新的信誉分布用X'_{ij}表示，则有：

$$X'_{ij}\sim\beta(m+1,n+1) \tag{7}$$

证明：(1)将均匀分布和β分布的分布函数定义代入(6)，很容易得到：

$$U(0,1)=\beta(1,1)=1$$

(2)对事件的分布用二项分布表达，对于上述$m+n$次事件(m次成功，n次失败)，记为$B(m+n,x)$，根据二项分布函数的定义[11]有：

$$B(m+n,x)=\frac{(m+n)!}{m!\ n!}x^m(1-x)^n$$

(3)根据假定，初始状态为均为分布，之后交互一次事件，形成一个新的分布，经历$m+n$次事件后，形成$m+n+1$个分布，将已知条件代入公式(5)，有

$$X'_{ij}\sim\frac{U(0,1)*B(m+n,x)}{\text{归一化全概率}}$$

$$\underline{\text{代入公式(1)、(2)步骤结果}}\ \frac{1*C_{m+n}^{m}x^m(1-x)^n}{\frac{C_m^mC_n^n}{C_{m+n+1}^{m+n}}}$$

$$=\frac{\frac{1!}{0!\ 0!}*\frac{(m+n)!}{m!\ n!}x^m(1-x)^n}{\frac{1*1}{\frac{(m+n+1)!}{(m+n)!\ 1!}}}$$

$$=\frac{(m+n)!}{m!\ n!}x^m(1-x)^n*(m+n+1)$$

$$=\frac{\gamma(m+n+2)}{\gamma(m+1)\gamma(n+1)}x^m(1-x)^n$$

$$=\beta(m+1,n+1)$$ □

由定理1可以看出，均匀分布的后验分布服从β分布，符合我们的选择。

3.2 更新信誉

建立信誉系统的初始状态后，接下来经历一组事件后，新的信誉如何分布呢？首先考虑直接信誉计算，对于直接信誉的更新，可以采用下面的性质2执行。

性质2 假设在t时段节点i关于节点j的信誉分布的先验概率为$(X_{ij})_{t-1}$，服从β分布，记为$\beta(a_j+1,b_j+1)$，之后，节点i和节点j又执行了$r+s$次事件，其中r次成功和s次失败。则经历上述事件之后，信誉的分布仍然服从β分布，且新的分布X'_{ij}满足：

$$X'_{ij}\sim\beta(a_j+r+1,b_j+s+1) \tag{8}$$

证明：类同性质1的证明，根据贝叶斯公式，有

$$X'_{ij}\sim\frac{\beta(a_j+1,b_j+1)*B(r+s,x)}{\text{归一化全概率}}$$

$$\underline{\text{代入公式(6)}}$$

$$\frac{\frac{\gamma(a_j+b_j+2)}{\gamma(a_j+1)\gamma(b_j+1)}x^{a_j}(1-x)^{b_j}*C_{r+s}^{r}x^r(1-x)^s}{\frac{C_{a_j+r}^{r}C_{b_j+s}^{s}}{C_{a_j+b_j+r+s+1}^{r+s}}}$$

$$==\frac{\frac{(a_j+b_j+1)!}{a_j!\ b_j!}*\frac{(r+s)!}{r!\ s!}x^{a_j+r}(1-x)^{b_j+s}}{\frac{\frac{(a_j+r)!}{r!\ a_j!}*\frac{(b_j+s)!}{s!\ b_j!}}{\frac{(a_j+b_j+r+s+1)!}{(r+s)!\ (a_j+b_j+1)!}}}$$

$$==\frac{(a_j+b_j+r+s+1)!}{(a_j+r)!\ (b_j+s)!}x^{a_j+r}(1-x)^{b_j+s}$$

$$==\frac{\gamma(a_j+b_j+r+s+2)}{\gamma(a_j+r+1)\gamma(b_j+s+1)}x^{a_j+r}(1-x)^{b_j+s}$$

$$\underline{\text{代入公式(6)}}\ \beta(a_j+r+1,b_j+s+1)$$ □

由上面的证明可以明显看出使用β分布信誉系统的灵活性，信誉更新等效于只更新两个参数a_j和b_j的值：

$$a'_j=a_j+r \tag{9}$$

$$b'_j=b_j+s \tag{10}$$

此外，从直观上，最近获得的信息应赋予更高的权重，因此，可考虑引入遗忘因子w，采用如下推论1的办法进行信誉更新。

推论1 假定节点i保存关于节点j在t时段的信誉分布的先验概率为$\beta(a_j+1,b_j+1)$，遗忘因子为w，则直接信誉更新计算公式表达为公式(8′)：

$$X'_{ij}\sim\beta(w*a_j+r+1,w*b_j+s+1) \tag{8'}$$

证明：由性质2及其证明可知，仅需要验证如下两式成立即可：

$$a'_j=w*a_j+r \tag{9'}$$

$$b'_j=w*b_j+s \tag{10'}$$

假设已知信誉表记录的一系列节点j不同时刻的信誉序列$(\beta(a_j+1,b_j+1))_0,(\beta(a_j+1,b_j+1))_1,\cdots,(\beta(a_j+1,b_j+1))_t$，则整合所有的信誉可以表达为：

$$a'_j=\sum_{t=0}^{t}(a_j)_t\quad b'_j=\sum_{t=0}^{t}(b_j)_t \tag{11}$$

引入遗忘因子w后，得到

$$\left.\begin{aligned}a'_j=\sum_{l=0}^{t}(a_j)_l*w^{(t-l)}\\ b'_j=\sum_{l=0}^{t}(b_j)_l*w^{(t-l)}\end{aligned}\right\}\quad\forall 0\leqslant w\leqslant 1 \tag{12}$$

每次都进行求和运算显得很不方便，一种简单的优化办法是采用递归算法，递归公式表达为：

$$(a_j)'_t=(a_j)_{t-1}*w+(a_j)_t\quad(b_j)'_t=(b_j)_{t-1}*w+(b_j)_t\quad\forall 0\leqslant w\leqslant 1 \tag{13}$$

将$(a_j)_t=r$、$(b_j)_t=s$代入前提即可。 □

遗忘因子w处于0和1之间，它的引入能够保证所有节点始终处于通信状态，恶意节点在开始时会较好地选择通信策略，然后诋毁系统，遗忘因子的引入，将使其不能更新信誉而被系统排除，从而抵御上述攻击。遗忘因子的合理选择能够保证信誉更新的科学性，使节点获得的信誉度更加合理。

下面考虑间接信誉的更新计算方法。

参考Jøsang[12]信任原理的计算方法，节点i接收到的节点k对节点j的间接信誉并不是全部认同的，因为这里还要考虑节点k的信誉，所以对间接信誉有一定程度的打折，即信誉高的节点k给予的间接信誉将获得更高的权重。假设节点i已经拥有节点k的先验信誉分布的两个参数表示为$\beta(a_k,b_k)$，节点k对节点j的信誉分布的两个参数表示为$\beta(a_j^k,b_j^k)$，假定节点i通过节点k得到节点j的间接信誉分布的两个参数表示为$\beta(a_{ij}^k,b_{ij}^k)$，参照文[10]的做法，我们将间接信誉的β分布参数用如下公式(14)和(15)计算：

$$a_{ij}^k=\frac{2*a_k*a_j^k}{(b_k+2)*(a_j^k+b_j^k+2)+2*a_k} \tag{14}$$

$$b_{ij}^k=\frac{2*a_k*b_j^k}{(b_k+2)*(a_j^k+b_j^k+2)+2*a_k} \tag{15}$$

对于不信任节点，$a_k=0$是一特例。由等式(14)，(15)可以看出，在这种情况下，$a_{ij}^k=b_{ij}^k=0$，表示节点i将完全忽略节点k的所有信息，符合常理。通过等式(14)和(15)同样可以验证，当a_k较大或b_k较小时，a_{ij}^k也较大(或b_{ij}^k较小)，说明来

自一个信誉高的节点将获得更高的权重。

3.3 整合信誉

从前面的分析可以得到，节点的信誉需要既考虑直接信誉，又考虑间接信誉。信誉的整合计算，就是把直接信誉和间接信誉综合起来，综合公式(9)、(10)、(14)和(15)，得信誉整合后 β 分布的两参数的计算公式为：

$$a'_j = a_j + a_{ij}^k \tag{16}$$

$$b'_j = b_j + b_{ij}^k \tag{17}$$

将公式(16)和(17)即可求出整合后的信誉分布的两参数。

3.4 信任

节点的信任是信誉分布的统计期望，根据概率统计原理，得：

$$T_{ij} = E(X_{ij}) = E(\beta(a'_j+1, b'_j+1)) = \frac{a'_j+1}{a'_j+b'_j+2} \tag{18}$$

初始时，$a_j = b_j = 0$ 时，可得 $T_{ij} = 0.5$，介于可信与不可信之间，符合常理。

3.5 行为决策

当已知 X_{ij}，对新触发事件 E_{ij} 的行为 B_{ij}，节点 i 是同意还是拒绝跟节点 j 合作呢？B_{ij} 取决于节点 i 保存的关于节点 j 的信誉 X_{ij} 和系统信誉阈值 θ_0，即：

$$B_{ij} = \begin{cases} \text{合作} & \forall T_{ij} \geqslant \theta_0 \\ \text{不合作} & \forall T_{ij} < \theta_0 \end{cases} \tag{19}$$

这样，对于可信节点，系统才接受其通信请求，抵御了恶意节点的非法通信请求，拒绝接入了恶意节点的异常数据，从而在一定程度上保障了节点数据的可靠性。关于系统信誉阈值 θ_0 的设定，需要考虑网络对节点接入的安全性需求，如对于访问控制安全性要求很高的军事网络和电子政务的关键节点可能设定为 0.9，甚至更高；对于普通节点阈值可以设置较小。

3.6 结果分析

根据上述设计，如下仿真结果显示了本模型方案的实用性。

(1)信誉收敛稳定

假定节点 j 向节点 i 发起了一系列通信事件，每次成功合作后的信誉递增，合作失败后的信誉递减，随着通信事件发生次数的递增，其变化趋势如图 1 所示。

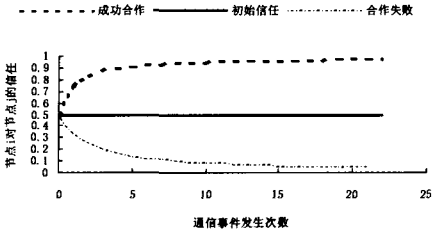

图 1 信誉收敛趋势

由图 1 的信誉收敛趋势曲线可以看出，对于一个完全可信(或不可信节点)的节点经过几次成功(或失败)的通信，很快就可以使其信誉趋于稳定，系统运行发生一段时间后，如果信誉发生急剧抖动，可以推测节点遭受攻击(被具有强大能力的攻击节点假冒，这会导致信誉急剧上升)或节点因电源不足(导致信誉急剧下降)等。从图 1 还可以看出，不可信行为对其信誉和信任的影响是显著的。

(2)遗忘因子对信任的影响

图 2 显示了引入遗忘因子过后，信誉曲线更加稳定平缓。

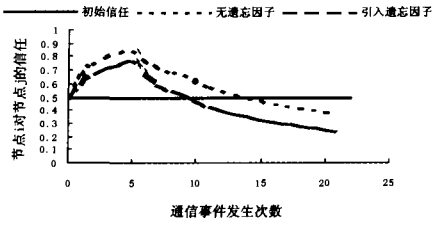

图 2 遗忘因子对信任的影响

(3)诽谤攻击对信任的影响

诽谤攻击是第三方节点 k 抬高或诋毁贬损资源通信请求节点 j 的信誉的一种攻击，本方案具有较好地抵御上述攻击的能力。我们测试了如下两种极端情形：

第一，对于一个完全可信的节点，如图 2 的“无攻击 1”曲线所示，信誉是持续稳定的，假定有一个蓄意攻击的节点 k 欺骗 i 说 j 的信誉一般(例子设为 0.5)，同时由 i 看来 k 的信誉也一般(我们也假定为 0.5，如果比 0.5 更小)，在此诽谤攻击下，其信任变化曲线如图 3“诽谤攻击 1”曲线所示。

第二，如果来自于一个可信节点(对节点 i 来说，k 的信任值为 1)的诋毁攻击(诽谤说 j 的信誉不好，例子为 0.5)，图 3 的“诽谤攻击 2”曲线展示了它对节点 j 的信任值影响并不明显。

上面两种情形下，三条曲线还是非常接近，因此本方案具有较好的抵御恶意节点诽谤攻击的能力。

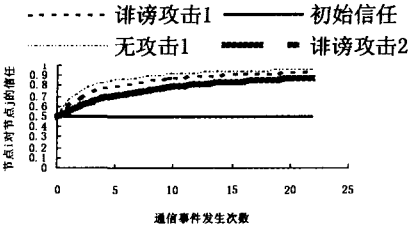

图 3 诽谤攻击对信誉的影响

(4)信誉欺骗攻击

信誉欺骗攻击是第三方节点 k 蓄意抬高资源通信请求节点 j 的信誉的一种攻击，本方案具有较好地抵御此攻击的能力。我们测试了如下两种情形：

第一，对于一个信誉中等(即时好时坏，其信誉为 0.5)的节点 k 的信誉欺骗(谎说 j 的节点信誉为 1)来说，遭受此类攻击的信任曲线如图 4 的“欺骗攻击 1”曲线所示意。与无攻击曲线相比，影响不大。

第二，对于一个本身信誉较好的节点(即其信誉趋近于 1)的信誉欺骗，其带来的影响稍微大一些，但是整个发展趋势基本保持一致，我们可以通过选择较高的网络信任阈值(如 $\theta_0 = 0.9$)来避免这种情况。

结束语 本文针对无线传感器网络中对数据认证性的需求，提出了一个基于无线传感器网络的信誉形式化模型。该模型可操作性强，并引用案例详细阐述了方案的实施措施。对于本方案的应用，还有如下几点值得说明和进一步研究。

(1)密码学为节点认证、数据机密性、数据完整性提供了有效的机制，本文所述方法不是根本脱离密码学，相反，信誉更新、信誉整合都假定系统外部存在节点认证的机制，仍然可采用密码学的原型来实现。

(下转第 100 页)

$Q=dG=11P_1(2)=(1\ 0-1\ 0-1)P_1(2)$

$=-P_1(2)\oplus 2^2(P_1(-2)\oplus 2^2P_1(2))$

$=-P_1(2)\oplus 2^2(P_1(-2)\oplus P_1(3390))$

$=-P_1(2)\oplus 2^2P_1(2491)$

$=P_1(-2)\oplus P_1(970)=P_1(10)$

任取 $k=1887$

公钥为，$n=5809$，$N_n=3002$，$a=2$，$b=1$，$G=P_1(2)$，$Q=P_1(10)$，$k=1887$，私钥为 $d=11$。

签名过程：

(1)由 $kl\equiv 1(\mathrm{mod}\ N_n)\Rightarrow l=35$

(2)计算 $kG=1887P_1(2)$

$=(1\ 0\ 0\ 0-1\ 0-1\ 0\ 0\ 0-1)P_1(2)$

$=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2(P_1(-2)\oplus 2^4P_1(2)))$

$=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2(P_1(-2)\oplus P_1(4594)))$

$=-P_1(2)\oplus 2^5(P_1(-2)\oplus 2^2P_1(5344))$

$=-P_1(2)\oplus 2^5(P_1(-2)\oplus P_1(2695))$

$=-P_1(2)\oplus 2^5P_1(2209)=P_1(-2)\oplus P_1(1472)$

$=P_1(4416)=(3254,4007)$

$r=3254\mathrm{mod}\ 3002=252$

(3)$\delta=(H(m)-d\gamma)l(\mathrm{mod}\ N_n)$

$=(23-11\times 252)\times 35(\mathrm{mod}\ 3002)=2851$

将$(\gamma,\delta)=(252,2851)$作为对消息 m 的签名。

签名验证：

(1)计算 $u_1=\gamma=252$，$u_2=\delta k(\mathrm{mod}\ N_n)$

$=2851\times 1887(\mathrm{mod}\ 3002)=253$

(2)$u_1Q=252P_1(10)$

$=(1\ 0\ 0\ 0\ 0\ 0-1\ 0\ 0)P_1(10)$

$=P_1(4272)$

$u_2G=253P_1(2)$

$=(1\ 0\ 0\ 0\ 0\ 0-1\ 0\ 1)P_1(2)=P_1(3343)$

$U=u_1Q\oplus u_2G=P_1(4272)\oplus P_1(3343)$

$=P_1(5238)$

$V=H(m)G=23P_1(2)$

$=(1\ 0-1\ 0\ 0-1)P_1(2)=P_1(5238)$

$U=V$，接受这个签名。

结论 本文提出了一种基于环 Z_n 上圆锥曲线的 ElGamal 数字签名方案，其安全性是基于大数分解和有限 Abel 群 $C_n(a,b)$ 上计算离散对数问题的困难性。由于在 $C_n(a,b)$ 上，明文嵌入，阶的运算以及点的运算都比较容易，特别是求逆元很容易，因此 ElGamal 在 $C_n(a,b)$ 上的模拟比它在椭圆曲线 $E_n(a,b)$ 上模拟要简单得多。而且通过引进标准二进制计算群元素的整数倍的算法，能节约近 1/4 的计算量，使该方案更具有应用价值。

参 考 文 献

1 Diffe W, Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644～654

2 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems[J]. Comm ACM, 1978, 21: 120～126

3 El-Gamal T. A public key cryptosystem and a signature scheme based on the discrete logarithm[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469～472

4 张明志. 用圆锥曲线分解整数[J]. 四川大学学报(自然科学版), 1996, 33(4): 356～359

5 曹珍富. 基于有限域 F_P 上圆锥曲线的公钥密码系统[A]. 密码学新进展-Chinacrypt'98[C]. 北京：科学出版社, 1998. 45～49

6 曹珍富. RSA 与改进的 RSA 的圆锥曲线模拟[J]. 黑龙江大学自然科学学报, 1999(4): 15～18

7 孙琦，张起帆，彭国华. Dickson 多项式 $g_e(x,1)$ 公钥密码体制的新算法[J]. 四川大学学报(自然科学版), 2002, 1: 18～23

8 孙琦，张起帆，彭国华. 计算群元的整数倍的一种算法及其在公钥密码体制中的应用[A]. 密码学进展-ChinaCrypt'2002. 见：第七届中国密码学学术会议论文集[C]. 北京：电子工业出版社, 2002. 117～124

9 孙琦，朱文余，王标. 环 Z_n 上圆锥曲线和公钥密码协议[J]. 四川大学学报(自然科学版), 2005, 42(3): 471～478

10 王标，朱文余，孙琦. 基于剩余类环 Z_n 上圆锥曲线的公钥密码体制[J]. 四川大学学报(工程科学版), 2005, 37(5): 112～117

(上接第 87 页)

(2)本文中信誉度的最初始状态属于主观信任，假定为均匀分布，介于可信与不可信中间，初步反映了人类社会网络的信誉基本状况，有一定的科学意义。为了进一步提高本方案的精确度，需要对主观信任的科学性问题进行研究，这正是我们下一步要研究的目标。

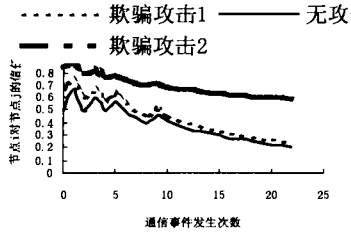

图 4 信誉欺骗攻击对信誉的影响

(3)图 4 显示了来自可信节点的欺骗攻击影响还是比较大的，应考虑在这里再引入遗忘因子减少其欺骗影响。

(4)关于信誉阈值 θ_0 也是一个非常值得研究的问题，因为它与具体的应用网络密切相关，对于异常行为的检测至关重要。可以考虑采用仿真手段去研究一些敏感网络或敏感节点的信誉阈值，为建立行业可信网络提供理论依据。

参 考 文 献

1 Perrig A, Szewczyk R, Wen V, Culler D, Tygar D. SPINS: Security Protocols for Sensor Networks. Wireless Networks Journal, September 2002

2 Karlof C, Sastry N, Wagner D. TinySec: Link Layer Encryption for Tiny Devices. To appear in ACM SenSys, 2004

3 Deng J, Han H, Mishra S. The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks. In: the Proceedings of IPSN, April 2003

4 Watro R, Kong D, Cuti S F, Gardiner C, Lynn C, Kruus P. TinyPK: Securing Sensor Networks with Public Key Technology. In: second workshop on Security in Sensor and Ad-hoc Networks, 2004

5 Eschenauer L, Gligor V D. A key Management Scheme for Distributed Sensor networks. In: Proceedings of ACM CCS, November 2002

6 Chan H, Perrig A, Song D. Random Key Predistribution Schemes for Sensor Networks. In: Proceedings of IEEE Symposium on Security and Privacy, 2003

7 Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management [C]. In: Proceedings of IEEE Conf. Security and Privacy, Oakland, California, USA, 1996

8 Blaze M, Feigenbaum J, Ioannidis J, Keromytis A[S]. RFC2704 - The KeyNote Trust Management System Version 2. 1999

9 Li N, Mitchell J, Winsborough W. Design of a rolebased trust management framework[C]. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland

10 肖德琴，周权，张焕国，等. 基于时序逻辑的加密协议分析，计算机学报，2002. 10

11 刘卫江主编. 概率论与数理统计. 北京：清华大学出版社；北京交通大学出版社, 2005

12 Jsang A, Ismail R. The Beta Reputation System[C]. In: Proc. of the 15th Bled Electronic Commerce Conference, June 2002