doi:10.3969/j.issn.1000-436x.2014.05.002

基于物联网节点行为检测的信任评估方法

刘宴兵，龚雪红，冯艳芬
（重庆邮电大学 计算机科学与技术学院，重庆 400065）

摘 要：针对物联网感知层节点的信任研究未能兼顾信任评估的主客观性且信任传递能耗大的问题，提出一种基于节点行为检测的低能耗信任评估模型。该模型采用事件触发检测与周期性检测相结合的方式，通过直接信任值、统计信任值与推荐信任值 3 种信任因子计算综合信任值，进而判断节点行为是否发生异常。仿真实验结果表明本方法有效兼顾信任评估的主客观性，同时可以快速规避恶意节点并降低信任传递能耗。
关键词：物联网；行为检测；信任评估；能耗
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1000-436X(2014)05-0008-08

Trust system based on node behavior detection in Internet of Things

LIU Yan-bing, GONG Xue-hong, FENG Yan-fen
(School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Establishing a trust system, which considers energy efficiency and a trust metric aware both subjectivity and objectivity in the Internet of Things, is a pow erful technique to defend against malicious attacks and impro ve the performance of network. A trust system based on behavior detection was proposed, which takes direct trust, recommended trust as well as history statistical trust into trust evaluation periodically and in communication. Recommended trust and history statistical trust were calculated by evidence combination and Bayes respectively. Simulation results show that nod es occur abnormal behavior could be quickly detected by the proposed trust system and the energy consumption of transmitting recommended trust was saved greatly.
Key words: Internet of Things; behavior detection; trust evaluation; energy consumption

1 引言

进入大数据时代，云计算与物联网成为当前重要的研究领域[1]。而随着云计算的不断发展，物联网开始逐步涉及多领域多行业，且其中包含的大规模海量数据与个人和群体的隐私及保密问题有关。但物联网是一个开放的环境，定义安全边界困难，不能保证物所附带的数据在传递中不产生变化。其次，传统安全认证方法与常用加密技术的计算方式过于复杂，不适用于节点能力脆弱，资源受限和大规模部署的物联网应用环境[2]。另一方面，物联网感知层节点大都分布在无人监控的场景和区域中，容易成为大多数恶意攻击的源头，特别是有着合法身份的节点却发生拒绝服务、重放攻击、信息截取、注入大量冗余数据分组等异常行为的内部攻击更是加剧了物联网的安全问题。因此，思考如何保障物联网安全已成为国际研究界的共识，特别是围绕物与物之间的信任关系更是一个研究热点。

收稿日期：2013-09-07；修回日期：2013-11-23
基金项目：国家自然科学基金资助项目(61272400, 61309031)；教育部 NCET 基金资助项目；重庆高校创新计划基金资助项目(KJTD201310, KJZH11206)；重庆市教委科学研究基金资助项目(KJ130523&120512)；重庆邮电大学青年科学研究基金资助项目(A2012-79)
Foundation Items: The National Natural Science Foundation of China(61272400, 61309031); NCET; Chongqing Innovative Team Fund for Co llege Development Project(KJTD201310, KJZH11206); Foundation of CEC (KJ130523&120512); CQUPT Research Fund for Young Scholars (A2012-79)

2　相关工作

对网络节点行为的信任研究不仅可以提高网络的安全性，还可以简化不信任带来的监控和防范等额外开销。目前，对节点行为信任评估主要基于过去交往的行为证据之上，建立可信行为模型。Zhu 等人提出一种周期性节点行为的信任认证模型[3]，通过收集路由证据和随机抽查的方法对节点行为进行信任评价。Li 等人提出了基于角色的信任评估模型[4]，将节点在无线传感器网络中的身份作为节点信任的评价依据。Bao 等人提出一种基于入侵检测的信任评估模型[5]，实现了对节点行为的动态检测。He 等人对医疗传感器网的节点行为进行研究，建立一种分布式行为信任评估模型[6]。Bo 等人提出一种基于卡尔曼滤波计算方法的节点异常行为检测模型[7]。肖德琴等人提出一种基于高斯分布与信誉分布拟合的网络信誉模型[8]。Hani 等人则对现有信任模型中存在的漏洞问题进行全面的分析和总结[9]。Zhang 采取信任值取整的方式，通过交互成功率计算直接信任，提出了层次结构的信任评估模型[10]，该信任模型取得了不错的效果，但其未能考虑节点行为信任评估的实时性。林闯等人则从信息安全、可信系统和可信计算等多个角度出发，提出基于滑动窗口的行为信任评估模型[11]。Crosby 等人提出了基于位置检测的信任模型[12]，它可以有效地检测和孤立已经被攻击的节点。胡向东等人在分析数据分组 ID 的基础上，提出一种低成本轻量级的节点选择性转发攻击检测算法[13]。Zhan 等人对节点行为信任评估与路由的关系进行研究，给出兼顾节点行为信任评估与传输能耗的可信路由方案[14]，但该方案过于强调路由的能耗问题，弱化了信任的作用。

现有的信任评估方法都是针对节点过往行为特征及不同应用场景而提出的，并没有考虑主观判断与客观评价相结合的信任评估。此外，信任值用浮点数值而非单字节的整型数值表示，由此导致节点间传递推荐信任的能耗过高，不适用于节点资源受限的物联网环境。因此，本文提出一种基于节点行为检测的信任评估模型以及一种适用于物联网感知层节点的异常行为检测算法，能够在降低信任传递耗能的同时快速判断网络节点是否发生异常行为。

3　基于节点行为检测的信任评估模型

本模型通过收集节点行为特征建立节点的行为信任轮廓，进而将节点实时行为数据与可信行为轮廓通过异常行为检测算法进行比对，然后判断节点是否成为恶意攻击的源头。

3.1　信任评估模型设计

节点行为特征具有多样性，节点在传输速度、分组丢失率或传输时延必然存在差异。仅通过节点行为特征判断或行为统计来区分正常行为与异常行为，并不能很好地实现入侵检测，而且很有可能将节点的正常行为判断为异常行为。因此本文模型将客观评价的推荐信任值、历史统计信任值和主观判断的直接信任值加权求和，得到节点行为综合信任值，然后对节点行为进行异常检测。节点行为正常则更新节点的信任队列，行为异常则执行惩罚响应机制，信任评估流程如图 1 所示。

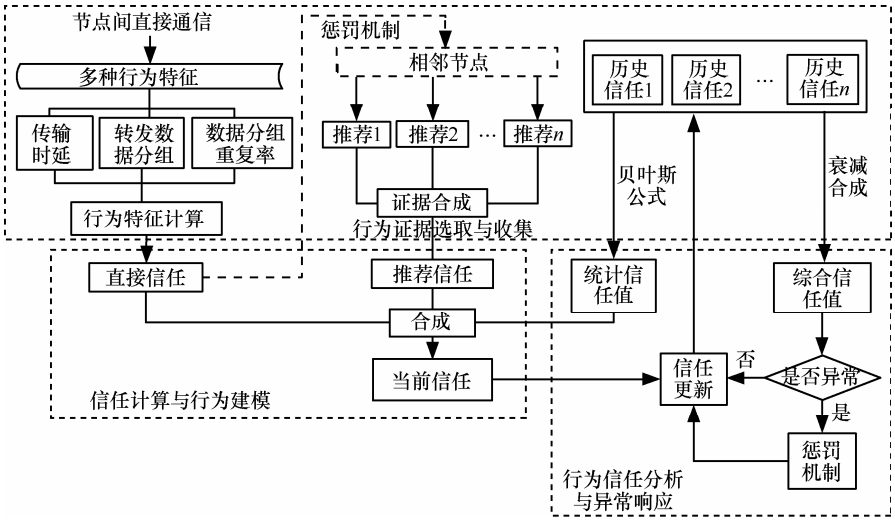

图 1　基于行为检测的信任评估流程

3.2 节点行为特征选取与证据收集模块

3.2.1 节点行为特征选取

随着物联网的发展，越来越多的应用需要部署海量监测节点，而计算与存储能力脆弱、资源受限的监测节点大都分布在无人监控的恶劣环境中，这些都将导致网络节点容易被恶意攻击和非法盗用。轻量级的身份认证协议和加密技术虽能阻止部分来自网络外部的恶意攻击，却无法解决合法身份的网络节点发生拒绝服务、信息截取、注入大量冗余数据分组等异常行为的内部攻击。内部恶意攻击的主要目标是破坏网络设备和篡改数据，这将导致发起攻击的节点产生不同于其他节点的异常行为，如删减、修改、注入、重复传输数据分组[15]。因此，基于节点行为检测的信任评估对网络安全的意义重大。本文选取数据分组转发量、数据分组重复率、传输时延作为节点行为特征进行节点直接信任检测。

3.2.2 节点行为信任证据收集

本文的信任评估模型将物联网的感知层节点分为传感器、中继及基站 3 类节点，在节点行为信任评估过程中，只有中继节点之间相互生成推荐信任值。传感器节点由其通信范围内的中继节点直接评估行为信任值，相邻的传感器节点之间不传递推荐信任值，本文假设基站完全可信。

1) 直接信任值

从节点发起的恶意攻击主要有窃取、篡改感知信息，注入大量错误信息等。因此，数据分组转发量成为直接检测节点异常行为的重要指标之一。当节点 A 向节点 B 请求 N 个数据分组，节点 B 只转发 $k(k \le N)$ 个数据分组，则节点 A 对节点 B 在转发数据分组行为上的直接信任值 T_{AB}^{f} 与 $k/(N+1)$ 成正比关系。所以节点 A 对节点 B 在转发数据分组行为上的直接信任值 T_{AB}^{f} 可以用对数函数表示为

$$T_{\mathrm{AB}}^{f}=\left\lfloor 100\times \mathrm{lb}(1+\frac{k}{N+1})\right\rfloor \tag{1}$$

T_{AB}^{f} 取 0 到 100 之间的整数，当 $k=N$，$T_{\mathrm{AB}}^{f}\approx 100$；当 $k=0$，则 $T_{\mathrm{AB}}^{f}\approx 0$。$T_{\mathrm{AB}}^{f}$ 用整数而非浮点数表示，浮点数值占用 4 byte 的存储空间而整型数值只需要 1 byte，因此有效降低信任记录存储量的同时大幅度减少推荐信任的传输耗能。

节点传输数据分组的重复率能有效判断节点是否发生异常行为。数据分组重复率 R^r 较低时，节点转发数据分组行为的直接信任值将随着 R^r 增大而缓慢变小，随着 R^r 逐渐趋向并大于重复率的临界值 σ，节点是恶意节点的可能性越来越大，这一变化趋势与底数大于 1 的指数函数曲线一致。因此，基于节点转发数据分组重复率的信任值 T_{AB}^{r} 表示为

$$T_{\mathrm{AB}}^{r}=\begin{cases}\left\lfloor 100\times\left(2-\alpha^{R^r}\right)\right\rfloor, & R^r<\sigma\\ 0, & \text{其他}\end{cases} \tag{2}$$

其中，$\alpha>1,\alpha^{\sigma}=2$，$\sigma$ 的取值由网络节点的信任控制强度确定。

在无线通信网络中，由于信号干扰等因素，节点传输数据会产生传输时延，但网络的传输时延必须在用户可容忍的范围内波动。节点 B 向节点 A 转发数据分组，传输时延 d_t 小于临界值 θ，节点 A 完全相信节点 B；随着传输时延 d_t 超出阈值越来越大，节点 B 发起恶意攻击的可能性越来越大，其相应的直接信任值也快速下降。节点在传输时延行为特征上的直接信任值 T_{AB}^{d} 表示为

$$T_{\mathrm{AB}}^{d}=\begin{cases}\left\lfloor 100\times c^{\frac{\mathrm{d_t}-\theta}{\theta}}\right\rfloor, & d_t\ge\theta\\ 100, & \text{其他}\end{cases} \tag{3}$$

其中，$c=0.01$，临界值 θ 与具体应用相关。

定义 1 节点 A 对节点 B 通信行为的直接检测信任值为 $T_{\mathrm{AB}}^{\mathrm{action}}$。行为信任值的合并采用加权系数 ε_f、ε_r 和 ε_d，各个权重系数可取不同的值，具体大小由实际网络对节点行为要求确定。

$$T_{\mathrm{AB}}^{\mathrm{action}}=\left\lfloor \varepsilon_f\times T_{\mathrm{AB}}^{f}+\varepsilon_r\times T_{\mathrm{AB}}^{r}+\varepsilon_d\times T_{\mathrm{AB}}^{d}\right\rfloor \tag{4}$$

其中，$0\le\varepsilon_f,\varepsilon_r,\varepsilon_d\le 1$，且 $\varepsilon_f+\varepsilon_r+\varepsilon_d=1$。

2) 推荐信任

当多个节点同时对单个节点推送信任值时，有可能给恶意节点带来可趁之机。恶意节点通过发送虚假、冲突的推荐信任值有意抬高或贬低某个节点的信任。因此，必须通过信任合并规则解决多个推荐信任问题[16]。本文将各信任值与平均信任值的距离作为权值，与期望值越远的权重越小，其成为恶意诽谤的可能性越大。首先计算全部推荐信任的平均信任值

$$E(m)=\frac{m_1+m_2+\cdots+m_k}{k} \tag{5}$$

然后计算信任值与平均值的距离，进而判断各个推荐信任值的权重，被评价节点 B 的第 i 个推荐信任值 m_i 的权重 ω_i 表示为

$$\omega_i = \frac{100 - \left| m_i - \mathrm{E}(m) \right|}{\sum_{i=1}^{k} (100 - \left| m_i - \mathrm{E}(m) \right|)} \tag{6}$$

对被评估节点B的所有推荐信任值进行加权计算，得到最终的合并推荐值 $T_{\mathrm{B}}^{\mathrm{rec}}$

$$T_{\mathrm{B}}^{\mathrm{rec}} = \left\lfloor \sum_{i=1}^{k} \omega_i \times m_i \right\rfloor \tag{7}$$

3) 历史行为统计信任值

节点行为信任是从社会科学中借鉴过来的概念，主观性过多会影响信任评估的可信度。因此，节点行为的信任评估必须兼顾信任的主客观性。长期大量的节点行为统计可以得到具有稳定性与代表性的客观评价。因此，本文建立被评估节点的信任评估移动队列，其结构如图 2 所示。

信任评估主要通过事件触发和时间周期相结合的方式实现队列滑动，以此更新队列内信任记录。队列内的单个记录将存储本次事件或者当前周期内节点的转发信任值、数据分组重复率信任值、时延信任值、时间、异常标签 5 个属性。

假设节点 A 与节点 B 交互次数为 $\alpha+\beta$ 次，其中，节点 A 评估节点 B 有 α 次是正常行为，β 次应接受惩罚的异常行为。根据贝叶斯公式计算节点 A 对节点 B 的统计信任值 χ 的分布概率为

$$P(\chi|\alpha,\beta) = \frac{P(\chi,\alpha,\beta)}{P(\alpha,\beta)}$$

$$= \frac{\binom{\alpha+\beta}{\alpha}\chi^{\alpha}(1-\chi)^{\beta}}{\int_0^1 \binom{\alpha+\beta}{\alpha}\chi^{\alpha}(1-\chi)^{\beta}\mathrm{d}\chi}$$

$$= \frac{\chi^{\alpha}(1-\chi)^{\beta}}{\int_0^1 \chi^{\alpha}(1-\chi)^{\beta}\mathrm{d}\chi}$$

根据密度函数 $B(\alpha,\beta)=\int_0^1 \chi^{\alpha-1}(1-\chi)^{\beta-1}\mathrm{d}\chi$，有

$$P(\chi|\alpha,\beta) = \frac{\chi^{\alpha}(1-\chi)^{\beta}}{B(\alpha+1,\beta+1)} \tag{8}$$

由此可知节点 A 对节点 B 的行为信任值 χ 服从参数为 α+1 和 β+1 的贝塔分布

$$f(\chi|\alpha+1,\beta+1) = \begin{cases} \dfrac{\chi^{\alpha}(1-\chi)^{\beta}}{B(\alpha+1,\beta+1)}, & 0<\chi<1 \\ 0, & \text{其他} \end{cases} \tag{9}$$

其数学期望为

$$\mathrm{E}(\chi) = \frac{\alpha+1}{\alpha+\beta+2} \tag{10}$$

因此，节点 B 的历史统计值信任值 $T_{\mathrm{B}}^{\mathrm{history}}$ 为

$$T_{\mathrm{B}}^{\mathrm{history}} = \left\lfloor 100 \times \frac{\alpha_{\mathrm{AB}}}{\alpha_{\mathrm{AB}}+\beta_{\mathrm{AB}}+2} \right\rfloor \tag{11}$$

3.3　节点行为建模模块

节点行为建模的主要任务是建立节点行为综合信任轮廓，本文 3.2 节已取得被评估节点 B 的直接观测信任值 $T_{\mathrm{B}}^{\mathrm{action}}$，推荐信任值 $T_{\mathrm{B}}^{\mathrm{rec}}$ 以及历史行为统计信任值 $T_{\mathrm{B}}^{\mathrm{history}}$，综合主观分析和客观统计信

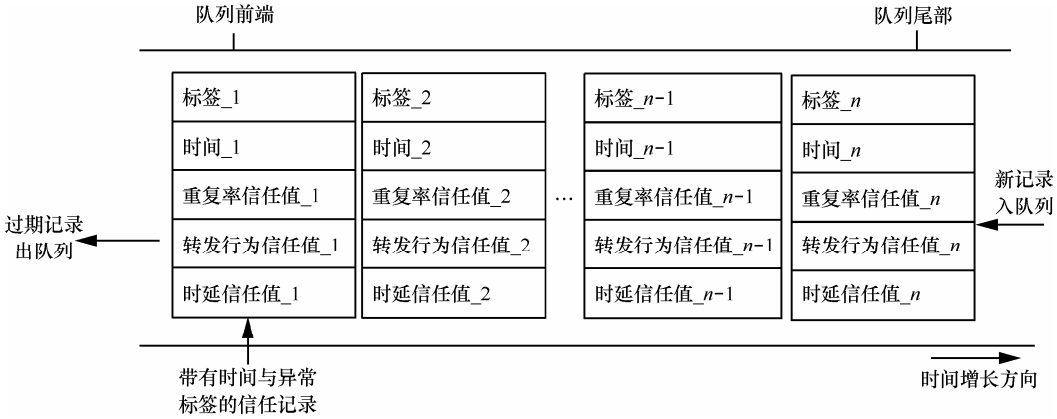

图 2　行为信任评估队列

任值的合并采用加权系数 W_1、W_2 以及 W_3。相对于评价主体节点 A，被评价节点 B 的信任应当以直接信任值为主，推荐信任值与统计信任值为辅助参考，因此节点整体信任值 $T_{\mathrm{AB}}^{\mathrm{total}}$ 为

$$T_{\mathrm{AB}}^{\mathrm{total}} = \left\lfloor W_1 \times T_{\mathrm{AB}}^{\mathrm{action}} + W_2 \times T_{\mathrm{AB}}^{\mathrm{rec}} + W_3 \times T_{\mathrm{AB}}^{\mathrm{history}} \right\rfloor \quad (12)$$

其中，$0 < W_3 \le W_2 < W_1 < 1$，$W_3 + W_2 + W_1 = 1$。在整体信任计算过程中，$W_2$ 与 W_3 可以取相同的数值，而各个权重的具体选择方式依赖于实际网络的应用要求。当节点 A 与节点 B 之间发生数据传输事件，通过历史信任队列左移，把队列前端过期的信任值移出，新生成的整体信任值 $T_{\mathrm{AB}}^{\mathrm{total}}$ 插入队尾，保证信任评估的可扩展性与时间相关性，并体现近期节点行为的重要性与远期行为的衰减性。

3.4 节点行为分析模块

节点行为分析模块首先通过交互事件触发生和周期性相结合的方式生成节点行为数据，然后将节点行为数据作为直接信任值计算的输入，结合历史信任统计信任值与推荐信任值得到节点当前行为整体信任值。最后，根据时间衰减公式计算节点的综合信任值，并与系统预设的最小信任阈值比较，从而评估节点当前行为的真实性并衡量该行为的价值。根据行为信任的社会特性，近期的信任值在综合信任评估中所占的比重越大，因此，综合信任值为

$$T_N^{\mathrm{comp}} = \left\lfloor \sum_{i=1}^{N} \left(c_i \times T_i^{\mathrm{total}} \right) \right\rfloor \quad (13)$$

其中，$c_i = \left(tim_i - tim_0\right) \Big/ \sum_{i=1}^{N} \left(tim_i - tim_0\right)$ 为衰减因子[11]，N 表示队列长度，对于节点行为的信任评估采取保守的长期考察策略，这样既可以使系统对恶意节点为获得高信任值的欺骗行为保持实时警惕，也可以准确有效地评估节点行为的信任值。

3.5 异常行为响应模块

除了评估节点信任值，还要防范恶意节点用少数次、低价值访问来换取高信任的欺骗行为，同时对已经发生的欺骗行为要进行惩罚，通常采用大幅度快降信任值的方式来惩罚欺骗。当被评估节点的某此行为被评估为不信任，则说明节点的行为已经发生异常，该行为可能是由于通信信号弱或信号干扰而发生的异常行为，也有可能是恶意节点试探性地发起的一次攻击行为。因此，该节点的行为有待进一步观察，并将其 ρ 次已标记为信任的行为评估信任值降为不信任值，使得被评估节点信任记录队列内的整体信任值可以快速下降，达到对不信任行为进行惩罚的目的。其中，ρ 的取值与系统的安全等级及节点行为信任控制的强度有关。

4 基于信任分析的异常行为检测算法

4.1 异常行为检测算法

算法通过节点行为特征选取与证据收集模块获取其通信行为特征数据，计算节点行为的直接信任值，进而将直接信任值、推荐信任值及历史统计信任值作为行为异常检测的输入数据。通过加权计算的方式，获得节点行为综合信任值，并与系统设置的信任阈值比较进而判断节点行为是否发生异常。一旦发现节点的行为异常，立即执行惩罚响应操作并隔离该恶意节点。算法步骤如下。

输入：直接信任值 $T_{\mathrm{AB}}^{\mathrm{action}}$，推荐信任值 $T_{\mathrm{B}}^{\mathrm{rec}}$，历史信任值 $T_{\mathrm{B}}^{\mathrm{history}}$，当前节点的信任队列 Q

ρ：欺骗惩罚力度

$T_{\min}$：正常行为信任阈值

$T_{\mathrm{m\_val}}^{\mathrm{system}}$：恶意节点信任值阈值

Array：恶意节点记录数组

输出：节点 Node 行为异常标志 flag

1) 如果 Q 为空，在队尾插入 N 个信任记录，并将 Q 中所有信任值初始化为陌生用户的不确定信任值(用 50 表示)，否则跳到步骤 2)

2) 根据式(11)计算整体信任值 $T_{\mathrm{AB}}^{\mathrm{total}}$

3) 删除 Q 的队头元素并将 $T_{\mathrm{AB}}^{\mathrm{total}}$ 插入队列 Q 中作为新的队尾元素。

4) 根据式(12)计算当前行为综合信任值 T_N^{comp}

5) if ($T_N^{\mathrm{comp}} > T_{\min}$)

6) return false //行为正常

7) if ($T_{\min} > T_N^{\mathrm{comp}} > T_{\mathrm{m\_val}}^{\mathrm{system}}$) //欺骗惩罚

8) wh ile ($\rho < 0$)

9) 从队尾开始，查找第 ρ 个标志为正常行为的信任记录，并将该记录降级为不信任的记录(用小于 50 的整数表示)

10) $\rho = \rho - 1$

11) E nd while
12) Return true // 返回行为异常
13) End if
14) else //信任值过低
15) 将节点 Node 添加到数组 Array 中
16) Return true // 返回行为异常

4.2 算法分析

队列的长度为 m，κ 是信任推荐个数，ρ 为惩罚规则中将信任值降为不信任的惩罚力度。算法第 1）步需要花费 $O(m)$ 的时间初始化当前节点信任队列内的信任值以及计算节点历史统计信任值。第 2）步计算整体信任值时需要先合并当前节点的 κ 个推荐信任值，因此需要 $O(\kappa)$ 的时间。第 3）~4）步更新该节点的信任队列并计算其综合信任值要 $O(1)$的时间。第 5）~16）步对节点行为进行检测，其中，第 8）~11）步是对发生异常行为的节点进行惩罚，惩罚过程中需要将 ρ 次已经是信任的记录降为不信任 min_*tru*，其时间开销为 $O(\rho)$。因此，节点当前行为信任判断过程的时间开销为 $O(\kappa+m+\rho)$。

5 仿真实验分析

仿真实验考虑 4 种恶意节点。第 1 类恶意节点在传输数据过程中丢弃数据分组，第 2 类恶意节点转发大量错误的重复数据分组。第 3 类恶意节点既丢弃数据分组又发送大量重复无用的数据分组。第 4 类节点恶意截取数据分组的并有较大的传输时延，Type 0 为正常节点。仿真实验模拟单个合法节点同时与 20 个节点通信，其中，有 16 个节点发生异常行为，分别有 4 个节点同时发生同一种类型的异常行为，T 为发生通信行为的周期时间。

由图 3 和图 4 可以看出，正常节点在对相邻不同类型节点的数据转发、数据重复率和传输时延的行为信任评估值随着时间的增长而变化。所有节点行为直接信任值初始化为不确定(50)，正常节点的信任值随着交互次数的增加而逐渐升高并趋向右上角，恶意节点的多种异常行为也明显地区分开来。

图 5 是执行惩罚机制与未实行惩罚的信任评估模型中 3 种不同异常行为信任值的变化曲线。由图中可以看出，加入惩罚机制的模型可以更快地降低发生异常行为的节点信任值，从而在更短的时间内发现恶意节点。

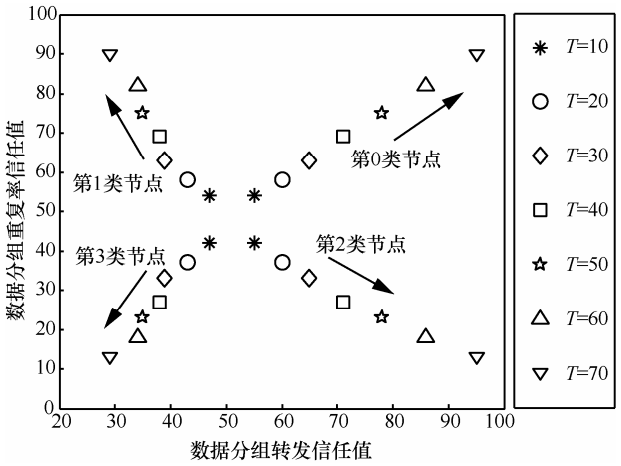

图 3　4 类节点的数据转发与重复率的信任值变化情况

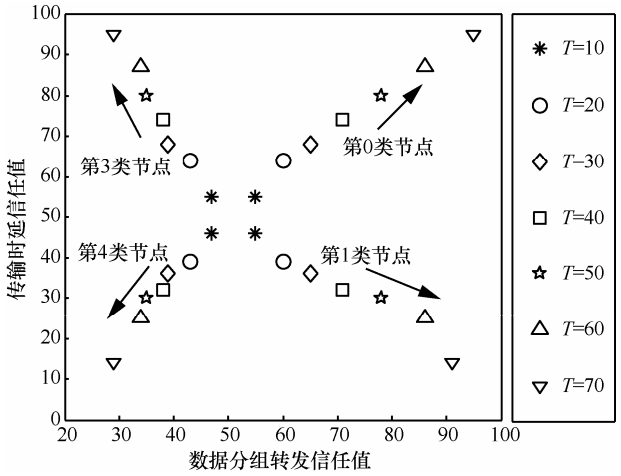

图 4　4 类节点的数据转发与传输时延的信任值变化情况

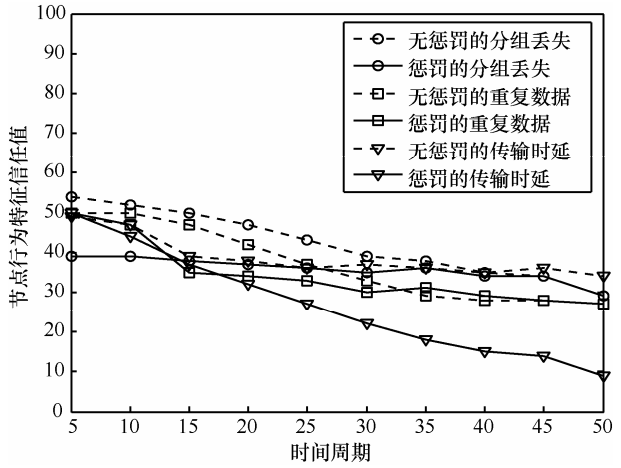

图 5　有惩罚机制的信任模型与无惩罚机制的信任模型中的节点行为信任值变化对比曲线

图 6 是本文信任模型对不同类型节点在多个连续的检测周期内的信任值变化曲线，在 200~260 s 时，发起恶意攻击的节点行为信任值迅速下降，而正常节点的信任值保持稳定。

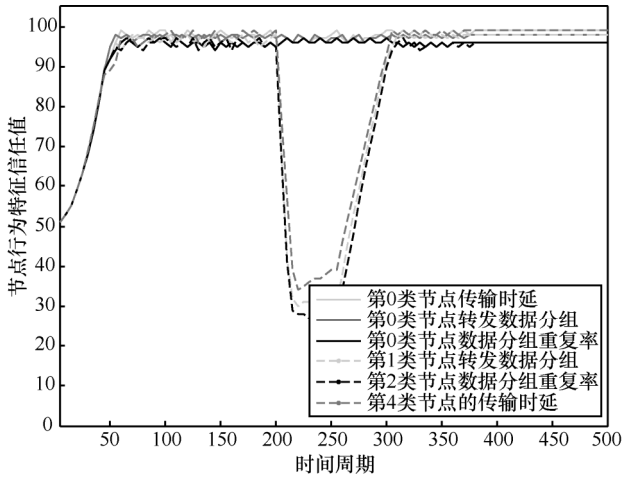

图 6 不同类型节点的行为信任值变化比较

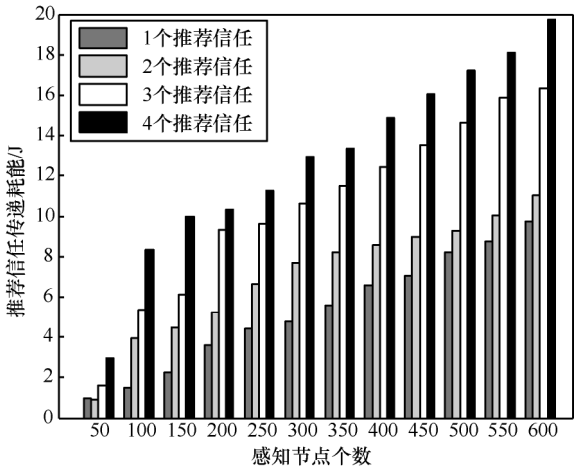

图 8 不同信任推荐个数的耗能比较

图 7 是 3 种不同信任评估模型的传输耗能比较，由图中可看出 TID 模型和 TMA 模型传输耗能明显高于本文的信任模型。原因是已有的信任模型在资源有限的传感器节点之间仍进行推荐信任的传递，且未能有效考虑整型数据表示的信任值比浮点型信任值占用空间量小，传输耗能低的特点。而本文的信任模型仅在中继节点之间传递推荐信任值，信任值取 0~100 之间的整数，有效减少信任存储量与降低传输耗能。当传感器节点个数较少时($n<175$)，由于加入中继节点，本模型耗能略大于 TMA 信任模型。由图 8 可知信任传递耗能与信任个数成正比。因此，在保证信任评估准确性的同时应尽可能降低推荐信任个数。

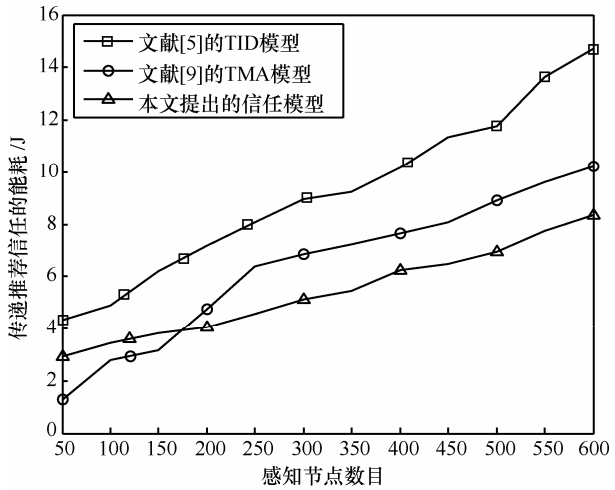

图 7 3 个不同信任模型的耗能比较

6 结束语

本文针对物联网节点行为信任研究未能同时兼顾信任的主客观性，且信任传递能耗大等问题，提出一种基于节点行为检测的信任评估模型及异常行为检测算法。模型采用事件触发检测与周期性检测的方式，将直接信任值、统计信任值与推荐信任值 3 种信任因子作为异常行为检测算法的输入，计算节点行为的综合信任值并判断网络是否存在恶意攻击。本模型采取信任值取整的方式，减少了信任记录的存储量。加入欺骗惩罚机制，缩短了网络发现恶意攻击的时间。仿真实验结果表明本方法可以在较短周期内规避发生异常行为的恶意节点，提高网络安全性的同时有效降低推荐信任的传递能耗。下一步工作将对该模型进行扩展，考虑节点剩余能量、数据分组转发速度等更多的行为特征，进一步提高节点行为信任评估的准确性和可靠性。

参考文献：

[1] ATZORI L, IE RA A, MORABITO G. The Internet of Things: a survey[J]. Computer Networks, 2010, 54(15):2787-2805.

[2] ROMANA R, ZHOUA J, LOPEZB J. On the features and challenges of security & privacy in distri buted Internet of T hings[J]. Computer Networks, 2013, 57 (10):2266-2279.

[3] ZHU H, DU S, GAO Z, *et al*. A probabilistic misbehavior detection scheme towards efficient trust establishment in de lay-tolerant networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, (99):1-6.

[4] LI X Y, ZHOU F, DU J, *et al.* LDTS: a lightw eight and dependable trust system for clustered wireless sensor networks[J]. IEEE on Transactions on Information Forensics and Security, 2012, 8(6):924-935.

[5] BAO F, CHEN R, CHANG M J, *et al*. Trust-based intrusion detection in wireless sensor networks[A]. 2011 IEEE International Conference on Communications (ICC)[C]. Kyoto, Japan, 2011.1-6.

[6] HE D, CHEN C, CHAN S, *et al*. A distributed trust evaluation model and its application scenarios for medical Sensor networks[J]. IEEE Transaction on Information Technology in B iomedicine, 2012, 16

(6):1164-1175.

[7] SUN B, SHAN X M, WU K, *et al*. Anomaly detection based secure in-network aggregation for wireless sensor networks[J]. IEEE Systems Journal, 2013, 7(1): 13-25.

[8] 肖德琴, 冯健昭, 周权等. 基于高斯分布的传感器网络信誉模型[J]. 通信学报, 2008, 29(3): 47-53.
XIAO D Q, FENG J Z, ZHOU Q, *et al*. Gauss reputation framework for sensor networks[J]. Journal on Communications, 2008, 29(3): 47-53.

[9] CROSBY G.V, HESTERL, PISSION N. Location-aware, trust-based detection and isolation of c ompromised nodes in w ireless sensor networks[J]. International Journal Network Security, 2011, 12(2): 107-117.

[10] ZHANG J, SHANKARAN R, ORGUN M A, *et al*. A dynamic trust establishment and management framework for wireless sensor networks[A]. 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)[C]. Hong Kong, China, 2010. 484-491.

[11] 林闯, 田立勤, 王元卓. 可信网络中用户行为可信的研究[J]. 计算机研究与发展, 2008, 45(12): 2033-2043.
LIN C, TIAN L Q, WANG Y Z. Research on use r behavior trust in trustworthy network[J]. Journal of Computer Research and Development, 2008, 45(12): 2033-2043.

[12] ALZAID H, ALFARAJ M, RIES S, *et al*. Trust Management VII[M]. Berlin Heidelberg: Springer, 2013.66-82.

[13] 胡向东, 余朋琴, 魏琴芳. 物联网中选择性转发攻击的发现[J]. 重庆邮电大学学报, 2012, 24(2):148-152.
HU X D, YU P Q, WEI Q F. Detection of selective forwarding attacks in the Internet of Things[J]. Journal of Chongqing University of Posts and Telecommunications, 2012, 24(2):148-152.

[14] ZHAN G , SHI W, DENG J. Design and implementation of TARF: a trust-aware routing framework for WSNs[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(2):184-197.

[15] SHANKARAN R, VARADHARAJAN V, ORGUN M A, *et al*. Context-aware trust management for peer-to-peer mobile ad-hoc networks[A]. 33rd Annual IEEE International Computer Software and Applications Conference[C]. Seattle, Washington, USA, 2009. 188-193.

[16] JOSANG A, ISMAIL R, BOYD C. A survey of trust and reputation systems for on line service provision[J]. Decision support systems, 2007, 43(2):618-644.

作者简介：

刘宴兵（1971-），男，四川遂宁人，博士，重庆邮电大学教授、博士生导师，主要研究方向为无线网络管控和网络信息安全。

龚雪红（1987-），女，广西来宾人，重庆邮电大学硕士生，主要研究方向为可信物联网。

冯艳芬（1989-），女，河南安阳人，重庆邮电大学硕士生，主要研究方向为网络与信息安全。