一种分布式网络环境下基于挑战-响应模型的可信评估方法

梁 靓* 张镨丹 武彦飞 贾云健
(重庆大学微电子与通信工程学院 重庆 400044)

摘 要：运用信任模型进行可信评估是解决分布式网络安全问题的重要手段。然而，目前大部分研究工作把研究重点放在如何收集更完整的信任证据，以及如何利用一些新手段如机器学习、区块链等评估节点信任值，很少对如何获取节点可靠的初始信任值进行研究。实际上，针对分布式网络提出的很多信任模型都依赖于历史信任证据，而初次对网络进行可信评估时并不具备相关历史信息。基于此，该文面向分布式网络环境的安全问题，提出了基于挑战-响应模型的可信评估方法。首先利用挑战-响应模型获取节点可靠的初始信任值，并利用此初始信任值对网络中的节点进行分簇，在簇内进行信任值计算和信任值更新，完成分布式网络环境下完整的可信评估流程。仿真结果表明，相较于统一设置初始信任值的方式，该文所提方法能对恶意节点、自私节点的信任值有较准确的预测，同时对恶意节点的检测率也更高。

关键词：可信评估；分布式网络；挑战-响应模型；初始信任值
中图分类号：TN915.08; TP393 **文献标识码**：A **文章编号**：1009-5896(2023)02-0600-08
DOI: 10.11999/JEIT211331

A Trusted Evaluation Method Based on Challenge-Response Model in Distributed Network Environment

LIANG Liang ZHANG Pudan WU Yanfei JIA Yunjian
(*School of Microelectronics and Communication Engineering, Chongqing University, Chongqing* 400044, *China*)

Abstract: Using trust models to conduct trust evaluation is an efficient way to solve the security problem in distributed networks. However, most of the researches focus on collecting trust evidence completely or using new methods such as machine learning, blockchain to conduct trust evaluation. Few of the researches focus on how to obtain reliable initial trust of network nodes. In fact, many trust models for the distributed network rely on historical trust evidence, but the historical information is unavailable for the first trust evaluation. To address this problem, a trust evaluation method based on challenge-response model is proposed. First, the challenge-response model is leveraged to obtain a reliable initial trust. Then, the trust is used for trust evaluation process, including clustering, trust calculation and trust update. Simulation results show that the proposed method has better performance than the unified initialization trust based method, in terms of the prediction accuracy for malicious nodes and selfish nodes, as well as the detection rate for malicious nodes.

Key words: Trust evaluation; Distributed network; Challenge-response model; Initial trust

1 引言

近年来，分布式网络应用前景越来越广泛，与集中式网络相比，分布式网络能有效避免因单个重要节点失效而影响整个网络运行的问题。但也因为传统网络安全措施如身份认证、访问控制等技术过于依赖中心节点的特点，分布式网络安全问题需另找一条解决途径——信任模型。

文献[1]针对p2p网络中典型的信任模型Eigentrust进行改进，保留每个节点与交互节点利用迭代得出全局信任值的优点，还解决了Eigentrust模型对新加入节点估计不准确的问题。文献[2]基于熵的信任模型和基于概率的信任模型提出了信任值建立和信任值更新方法并将所提出的信任模型和评估方法应用于adhoc网络。文献[3]基于adhoc网络的特

收稿日期：2021-11-25；改回日期：2021-06-18；网络出版：2022-06-28
*通信作者： 梁靓 liangliang@cqu.edu.cn
基金项目：国家自然科学基金 (62071075, 61971077)，中央高校基金 (2020CDJ-LHZZ-022)，庆市自然科学基金 (cstc2020jcyj-msxmX0704)
Foundation Items: The National Natural Science Foundation of China (62071075, 61971077), The Fundamental Research Funds for the Central Universities of China (2020CDJ-LHZZ-022), The Natural Science Foundation of Chongqing (cstc2020jcyj-msxmX0704)

点提出了分布式自适应信任模型DATEA，分为单跳模块与多跳模块。单跳模块可自适应地设置权重来计算直接信任值与推荐信任值，多跳模块负责间接信任值的计算。文献[4]针对无线传感器网络提出了一种分布式高效信任模型EDTM，考虑了直接信任值和推荐信任值。该模型在直接信任值中提出基于数据、能量和通信的3维信任证据，在推荐信任值中引入可靠性和熟悉度两个指标以提高推荐信任值的准确性。文献[5]针对水下无线传感器网络提出了一种基于C4.5决策树的可信评估方法，该方法采用模糊逻辑信任模型收集各类信任证据并进行分析，再采用训练好的C4.5决策树完成信任值分类。文献[6]基于水下传感网络易遭到混合攻击的特点提出了一种分布式容错信任模型，该模型分为3个阶段。首先利用量化的环境模型反映水下环境对信任评估的影响；然后构建一个基于强化学习的信任更新模型来对抗混合攻击；最后采用一种信任恢复模型来恢复低信任值的节点以提高网络的资源利用率。

运用信任模型进行可信评估虽然是解决分布式网络安全问题的重要手段，但很多针对分布式网络提出的信任模型依赖于节点过去行为的历史信任证据，可是初次对分布式网络进行可信评估时是没有这些信任证据的。一种解决方式是对网络中所有节点统一设置信任值，这是许多现有信任模型采用的方式，其优点是设置简单且节省能量，缺点是统一设置的信任值并不代表节点的真实行为。另一种方式是对节点进行评估来获取可靠的初始信任值，这种做法的优点是可以在可信评估初始阶段获取节点的真实行为，从而对恶意节点和自私节点有更准确的预测。与统一设置初始信任值相比，该方式的缺点是相对复杂而且会消耗更多能量。在文献[7]中，作者提出了一种在个人空间物联网中创建设备初始信任值的方法。

本文基于挑战-响应模型，提出了一种面向分布式网络的可信评估方法。网络节点通过该方法对挑战进行响应，形成关于节点的先验知识，用于度量其初始信任值。然后利用节点的初始信任值进行分簇，在簇内进行信任值计算和信任值更新，完成分布式网络中整个可信评估的流程。

2　系统模型

2.1　网络模型

本文所研究的分布式网络结构如图1所示，由一个超级节点和大量普通节点组成。

其中，超级节点是拥有足够能量的可靠节点，主要负责与普通节点实行挑战-响应模型以获取各节点的初始信任值。部署在一定区域范围内的各个节点$n_i \in \boldsymbol{N}$, $i=1, 2,\cdots, M$都由超级节点分配给它们一个唯一的标识符ID_i。

2.2　攻击模型

攻击者对分布式网络发起的内部恶意攻击一般分为3个阶段[8]，其各个阶段的攻击过程和攻击可能带来的后果如表1所示。分布式网络中的节点通常都配备有编程接口或测试接口以便对其进行编程或者调试。其中，当攻击者对节点发起物理捕获攻击时，一般手段是采用一块编程板连接到节点的编程接口或测试接口来获取节点中的关键信息[9]。所以在对分布式网络进行可信评估前，必须假设当攻击者发起物理节点物理捕获攻击时，每个节点都可以检测到被编程板连接。

3　基于挑战-响应模型的初始信任值获取

3.1　挑战-响应模型

在网络开始运行前，超级节点中需引入伪随机数生成算法为每个节点生成独一无二的挑战数，该挑战数在网络中是公开的。然后，每个节点需生成密钥对来实施挑战-响应模型，运用RSA公钥密码算法原理[10–12]，对节点集合$\boldsymbol{N}=\{n_1, n_2, \cdots, n_M\}$进行预置密钥操作。

节点完成预置密钥后，超级节点和普通节点间

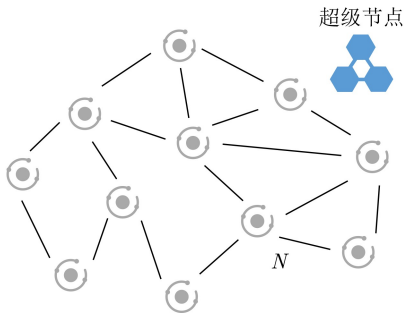


图 1 分布式网络结构图

表 1　内部攻击过程及后果

攻击阶段	攻击过程	攻击带来的后果
1	捕获某些物理节点	破解并获得被捕获节点存储的关键机密数据
2	将被捕获的节点或者克隆节点重新部署到原网络	扰乱网络正常通信
3	控制被捕获节点发起各种内部攻击	发起数据包篡改、重放攻击、黑洞攻击等内部攻击，威胁整个网络运行

实行挑战-响应模型，以获取每个普通节点的初始信任值。挑战-响应模型的运作机制如图2所示，不同颜色的线条代表不同的挑战-响应轮次。据图2可知超级节点与普通节点n_i之间实施挑战-响应模型的步骤如下：

(1)节点n_i发送[ID_i, (E_i, R_i)]给超级节点，超级节点把这个对应关系记录在表中；

(2)超级节点生成一个挑战数Nonce_i并把挑战数发送给节点n_i；

$$\mathrm{result}=\begin{cases} a^i_{\mathrm{num}}=a^i_{\mathrm{num}}+2, & \\ a^i_{\mathrm{num}}=a^i_{\mathrm{num}}+1, & b^i_{\mathrm{num}}=b^i_{\mathrm{num}}+c_{\mathrm{num}}/3, \\ b^i_{\mathrm{num}}=b^i_{\mathrm{num}}+1, & \end{cases} \begin{array}{ll} & \mathrm{Is}_i=\mathrm{Nonce}_i\|\mathrm{ID}_i\|1 \\ & \mathrm{Is}_i=\mathrm{Nonce}_i\|\mathrm{ID}_i\|0 \\ & \text{其他} \end{array} \tag{1}$$

第1种情况下，超级节点相信该节点未被捕获；第2种情况下节点n_i有很大可能被攻击者的编程板连接，挑战失败且累计挑战失败次数为$c_{\mathrm{num}}/3$次(c_{num}为挑战的总轮数)；第3种情况表明这些节点可能是合作意愿较低的自私节点，挑战失败且累计挑战失败次数1次。利用上述挑战-响应模型，可以获得节点的响应结果。

3.2 初始信任值获取

获取节点初始信任值前，网络中任一节点行为均具有不确定性。引入贝叶斯准则来度量节点行为的不确定性概率x。首先给x分配一个先验分布$p(x)$，$p(x)$取自Beta函数族[7]，即

$$\begin{aligned} p(x)&=\frac{1}{\int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\mathrm{d}x}x^{\alpha-1}(1-x)^{\beta-1} \\ &=\frac{1}{B(\alpha,\beta)}x^{\alpha-1}(1-x)^{\beta-1} \end{aligned} \tag{2}$$

Beta(1,1)是均匀分布[13]。初次对网络进行可信

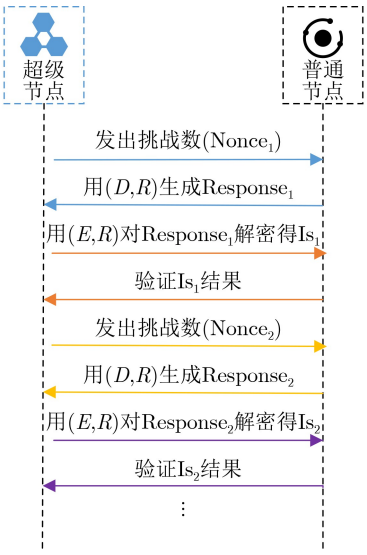


图 2 挑战-响应模型运作机制

(3)节点n_i收到挑战后，结合标识符ID_i、挑战数Nonce_i以及自己是否感应到被编程板连接的状态h(0表示连接状态，1表示未连接状态)，采用密钥对$(D_i,\ R_i)$生成响应$\mathrm{Response}_i=\mathrm{Nonce}_i\|\mathrm{ID}_i\|h$并将$(\mathrm{ID}_i,\ \mathrm{Response}_i)$发给超级节点；

(4)当超级节点收到响应后采用预存的密钥$(E_i,\ R_i)$对$\mathrm{Response}_i$进行解密得到消息序列Is_i，根据消息序列Is_i的不同，对应的响应结果由式(1)给出

评估时，节点的任何一个信任值都可能对应任意概率，因此参数选择$\alpha=\beta=1$。在挑战-响应模型中，响应被定义为二元事件，用r表示一轮挑战结束后的响应结果。当r=1时，代表节点给超级节点的响应是预期中的响应，反之亦然。每一轮挑战-响应回合后r发生的概率结合给定未知概率x如式(3)所示

$$p(r|x)=x^r(1-x)^{1-r} \tag{3}$$

当一轮挑战-响应完成后，结合全概率式和条件概率式，利用贝叶斯准则更新x的后验分布$p(x|r)$如式(4)所示

$$\begin{aligned} p(x|r)&=\frac{p(r\cap x)}{p(r)} \\ &=\frac{p(r|x)p(x)}{p(r|x_1)p(x_1)+\cdots+p(r|x_n)p(x_n)} \\ &=\frac{p(r|x)p(x)}{\int_0^1 p(r|x)p(x)\mathrm{d}x} \end{aligned} \tag{4}$$

对式(4)进行整理得

$$\begin{aligned} p(x|r)&=\frac{x^{(\alpha+r-1)}(1-x)^{\beta+1-r-1}}{\int_0^1 x^{(\alpha+r-1)}(1-x)^{\beta+1-r-1}\mathrm{d}x} \\ &=\frac{x^{(\alpha+r-1)}(1-x)^{\beta+1-r-1}}{B(\alpha+r,\beta+1-r)} \end{aligned} \tag{5}$$

此时x的后验分布也为Beta分布，且参数为$(\alpha+r)$和$(\beta+1-r)$。

在随后几轮的挑战-响应中，x的估计将采用上一轮挑战-响应结束后的后验分布作为其先验分布，在c_{num}轮挑战-响应之后x的后验分布为$p(x|r_1r_2\cdots r_{c_{\mathrm{num}}})$，其参数为$(1+c_{\mathrm{num}}\bar{r})$和$(1+c_{\mathrm{num}}-c_{\mathrm{num}}\bar{r})$。因此$c_{\mathrm{num}}$轮挑战-响应结束后$x$的后验分布期望值如式(6)所示

$$E(x|\bar{r})=\frac{1+c_{\text{num}}\bar{r}}{1+c_{\text{num}}\bar{r}+1+c_{\text{num}}-c_{\text{num}}\bar{r}}=\frac{1+c_{\text{num}}\bar{r}}{2+c_{\text{num}}} \tag{6}$$

其中，$\bar{r}=\dfrac{1}{c_{\text{num}}}\sum_{i=1}^{c_{\text{num}}}r_i$。采用Beta分布获取节点信任值时，$x$的后验分布期望值$E(x|\bar{r})$代表其信任值。应用式(7)将挑战-响应模型得出的结果映射到初始信任值T_{ini}计算中可得

$$T_{\text{ini}}=\frac{a_{\text{num}}^{i}+1}{a_{\text{num}}^{i}+b_{\text{num}}^{i}+2} \tag{7}$$

4　信任值计算与信任值更新

获取节点的初始信任值后，对节点进行分簇：(1)将初始信任值最高的几个节点选为簇头节点，负责簇内管理；(2)剩下的节点被随机均匀地分配到每一个簇中，形成如图3所示的分层管理结构。

4.1　信任值计算

评估节点A获取被评估节点B信任值的步骤如下：(1)根据两节点间的通信行为和节点B的剩余能量来计算直接信任值；(2)若节点A与节点B之间通信行为较少，则需挑选一组与节点A、B均有过交互的推荐节点$\{C_1,C_2,\cdots,C_Z\}$给出推荐信任值；(3)若有推荐信任值，则需对直接信任值和推荐信任值进行加权得到整合信任值。信任值计算过程如图4所示。

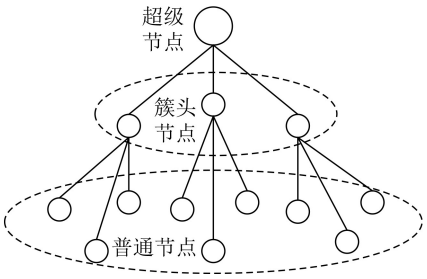


图 3 分布式网络分层管理结构

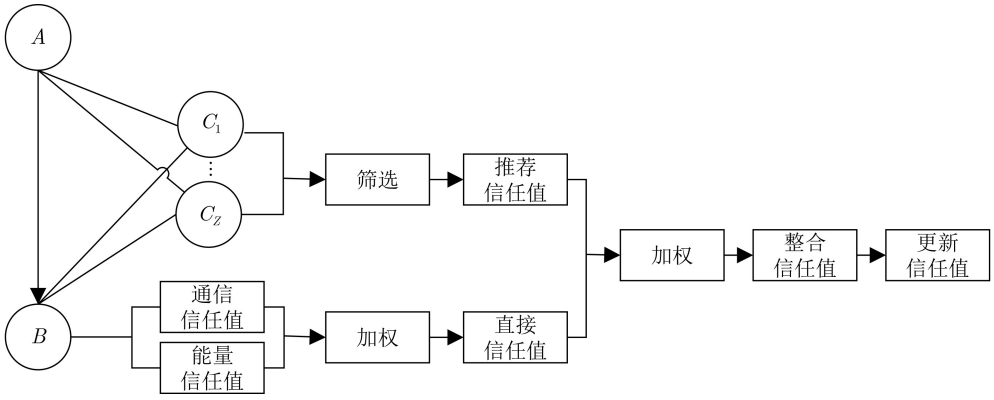


图 4 信任值计算过程

4.1.1　直接信任证据

(1) **基于通信行为的信任证据**

基于主观逻辑的信任模型引入了不确定度，比用单一数值表示节点间信任关系的方法更准确[14]，所以采用此信任模型来量化基于通信行为的信任证据。引入信任3元组$\{b,d,u\}$，其中b, d和u分别对应于信任、不信任和不确定度，$\{b,d,u\}$的计算方法由式(8)给出

$$\left.\begin{aligned}b&=\frac{s}{s+\lambda f+u}\\ d&=\frac{\lambda f}{s+\lambda f+u}\\ u&=\frac{u}{s+\lambda f+u}\end{aligned}\right\} \tag{8}$$

其中，$b,d,u\in[0,1]$且$b+d+u=1$。s和f是指通信成功和不成功的次数，$\lambda(\lambda>1)$表示对不成功通信的惩罚因子。u是分布式网络中的不确定因素，本文将其定义为动态变量$u=\delta_c(s+f)$，其中$\delta_c\in(0,1)$为不确定因素的调控因子。基于通信行为的信任证据可表示为

$$T_{\text{com}}=\frac{2b+u}{2} \tag{9}$$

(2) **基于能量的信任证据**

分布式网络中的节点依赖于它们所拥有的能量[5]，能量信任值的计算由式(10)给出

$$T_{\text{ene}}=\begin{cases}\dfrac{E_{\text{res}}}{E_{\text{ini}}}, & E_{\text{res}}\geq\theta\\ 0, & E_{\text{res}}<\theta\end{cases} \tag{10}$$

其中，θ为能量阈值，E_{res}和E_{ini}分别代表节点当前剩余能量与未开始评估前的初始能量。若节点当前剩余能量较低，可能是参与了内部攻击而消耗了节点自身过多能量，且剩余能量较低的节点可能无法与其他节点进行交互。因此可将剩余能量作为衡量能量信任值的指标。

基于通信信任值T_{com}、能量信任值T_{ene}，根据式(11)可获得两节点之间的直接信任值T_{dir}

$$T_{\text{dir}} = \omega_{\text{com}} T_{\text{com}} + \omega_{\text{ene}} T_{\text{ene}} \tag{11}$$

其中，ω_{com}和ω_{ene}分别是通信行为信任证据和能量信任证据的权重，且$\omega_{\text{com}} + \omega_{\text{ene}} = 1$。

4.1.2 推荐信任证据

若评估节点A与被评估节点B间通信数据包过少，还须加入推荐信任值以保证信任值计算的准确性[15,16]。节点A想获取节点B的推荐信任值时，将挑选节点A和B的一组公共邻居节点中初始信任值较高的节点作为推荐节点$C_i(i = 1, 2, \cdots, Z)$。节点A收到多个推荐值时通过检测每个推荐值的一致性来计算其权重，计算方法如式(12)所示

$$\omega_{C_i}^{B} = 1 - \left| T_{C_i}^{B} - T_{\text{ave}}^{B} \right| \tag{12}$$

其中，$T_{C_i}^{B}$是推荐节点C_i对节点B的推荐值，T_{ave}^{B}是所有推荐节点对节点B推荐值的平均值。基于推荐值$T_{C_i}^{B}$、推荐权重$\omega_{C_i}^{B}$，以及推荐节点个数Z，计算推荐信任值为

$$T_{\text{recom}}^{B} = \frac{\sum_{i=1}^{Z} \omega_{C_i}^{B} \times T_{C_i}^{B}}{Z} \tag{13}$$

综上所述，节点的信任值计算方法如式(14)所示

$$T = \begin{cases} T_{\text{dir}}, & \text{cp}_{AB} \geq \text{Th}_{\text{num}} \\ \omega_{\text{dir}} T_{\text{dir}} + \omega_{\text{recom}} T_{\text{recom}}, & \text{cp}_{AB} < \text{Th}_{\text{num}} \end{cases} \tag{14}$$

其中，cp_{AB}是评估节点A与被评估节点B之间的通信数据包数量，Th_{num}是定义的通信数据包阈值；ω_{dir}和ω_{recom}分别是直接信任值和推荐信任值的权重，$\omega_{\text{dir}} + \omega_{\text{recom}} = 1$。

4.2 信任值更新

本文采用基于新记录滑动窗口的信任值更新机制。基于新记录触发的信任值更新原理是当有新的信任记录产生时，滑动窗口移动，旧的信任记录被移除窗口。如图5所示窗口存储节点的信任记录，信任值更新开始后窗口随新记录的产生从左向右移动，定期清除历史记录。

信任值更新应保持快降慢升的准则[17]，引入调节因子$\gamma(0 < \gamma < 1)$来控制信任值更新的快慢，T_{new}是最新记录中的信任值，T_{old}是历史信任值。信任值更新方式由式(15)给出

$$T'_{\text{new}} = T_{\text{old}} + (T_{\text{new}} - T_{\text{old}}) \times \gamma^{T_{\text{new}} - T_{\text{old}}} \tag{15}$$

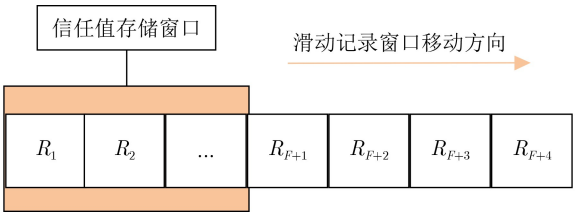


图 5 滑动窗口示意图

5 仿真验证与结果分析

本文采用MATLAB进行仿真验证。在100 m×100 m的区域内随机部署100个节点，设置挑战-响应的轮数为10轮，经过挑战-响应后获取每个节点相应的初始信任值，选择初始信任值不小于0.95的节点作为簇头节点，随机均匀地把剩下的节点分配到每一个簇中，簇头节点拥有较多能量，簇内节点与簇头节点之间的通信数据包cp_{AB}随机分配。参照文献[4]的仿真参数设置，将通信数据包阈值Th_{num}的初始值设为60，信任值更新的轮数设为3轮。

现对基于挑战-响应模型获取节点信任值算法的复杂度进行分析。在挑战-响应阶段中，挑战-响应总轮次数为c_{num}，所以获取节点初始信任值的循环最多执行$c_{\text{num}}N$次。设信任值更新的轮次为T_{num}轮，则获取节点直接信任值和间接信任值最多循环执行$2N + N^2$次，信任值更新的循环执行$T_{\text{num}}N$次。因此基于挑战-响应模型获取节点信任值算法的计算复杂度为$O(c_{\text{num}}N + 2N + N^2 + T_{\text{num}}N)$，可在二次时间内求解。

5.1 挑战-响应模型性能验证

在此环节中设置恶意节点率为25%，自私节点率为10%(序号76-100为恶意节点，66-75为自私节点)，得到经挑战-响应后获取的节点初始信任值如图6所示。从图中可以看到恶意节点的初始信任值都很低，自私节点的初始信任值也不高，为信任值计算提供了可靠前提。

图7为经过3轮信任值更新后每一簇节点的信任值变化情况。从图7(a)—图7(c)中可以看到大部分节点信任值变化的幅度不大，反映出了挑战-响应模型的误判率较低，用初始信任值就可以较为准确地预测节点在信任值计算阶段与信任值更新阶段的表现。

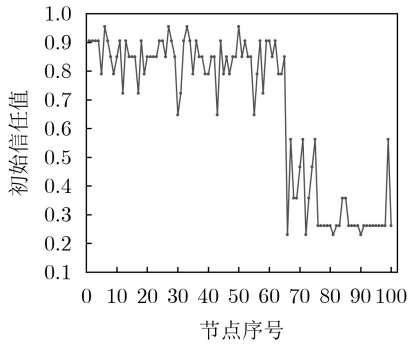


图 6 挑战-响应后的初始信任值

5.2 可信评估性能验证

为验证本文可信评估方法的性能，将基于挑战-响应模型的可信评估方法与基于统一初始信任值的方法进行对比仿真实验。在统一初始信任值的评估方法中，把所有节点的初始信任值设为0.5，信任值计算与信任值更新方式均与本文所设计的方法一致。

在图8(a)中，恶意节点率由5%增加到40%，步进为5%。比较了两种不同设置初始信任值方法下的恶意节点检测率，基于挑战-响应模型的可信评估方法中随着恶意节点数量的增加，其检测率依旧较高，而统一信任值方法的检测率一直在30%至50%徘徊。

在可信评估中常用信任计算误差(TCE)来评价模型的好坏[18]，TCE越小说明模型效果越好。设M是网络中节点的数量，$\tau_t(i)$是时间t内第i个节点的信任值，在一定时间t内

$$\mathrm{TCE}=\sqrt{\frac{\sum_{i\in M}\left[\tau_t(i)-p_t(i)\right]^2}{|M|}} \tag{16}$$

其中，$p_t(i)$表示时间t内第i个节点为诚实节点的可能性，$p_t(i)=1$表示节点为正常节点，$p_t(i)=0$表示节点为恶意节点，$p_t(i)=0.5$表示节点为自私节点。在图8(b)中，恶意节点率由5%增加到40%，步进为5%。比较了两种不同设置初始信任值方法下TCE的变化，可以看出基于挑战-响应模型的可信评估方法的信任计算误差较小，模型性能更好。

文献[4]针对无线传感器网络提出了一种分布式信任模型EDTM，该模型采用统一设置初始信任值并首次根据多维信任证据评估节点信任值。相关文献[3,19]也将该经典模型作为基准进行了对比。本文所设计的模型与EDTM模型的对比结果如图9所示。其中，图9(a)为恶意节点检测率的变化图，可以看出基于挑战-响应模型的评估算法的恶意节点检测率始终高于基于EDTM模型的算法。图9(b)为信任计算误差的变化图，由该图可知基于挑战-响应模型算法的信任计算误差始终小于基于EDTM模型的算法。由此可以说明本文提出的算法性能更优于基于EDTM模型的算法。

6 结束语

为了解决在分布式网络中运用信任模型进行可信评估时缺乏历史信任证据的问题，本文提出了基于挑战-响应模型的可信评估方法。整个可信评估过程分为两步：第1步是在超级节点和普通节点间

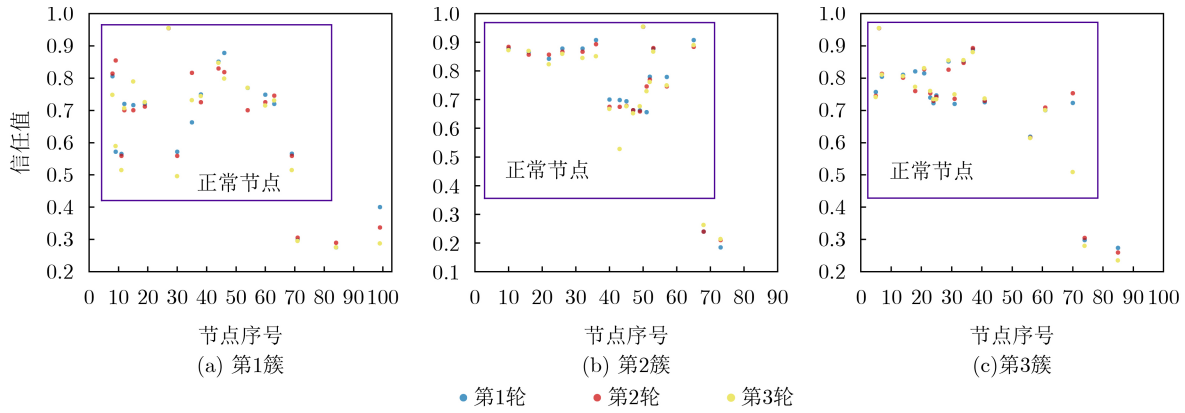


图 7 各簇更新后的信任值

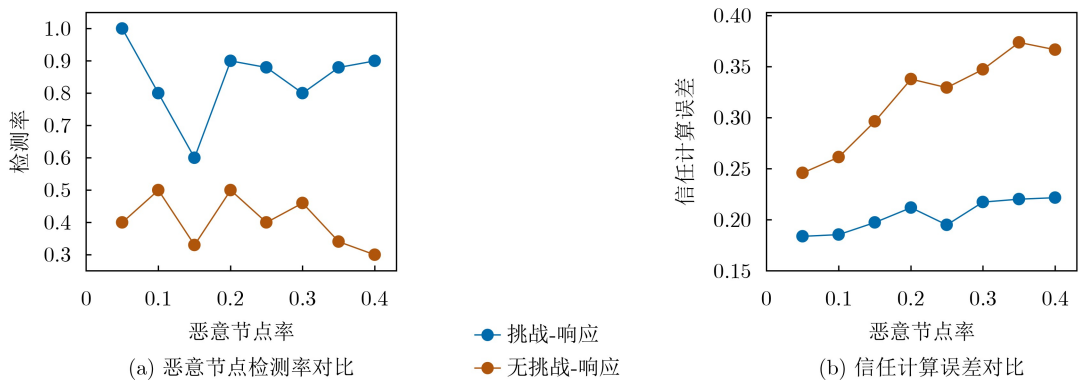
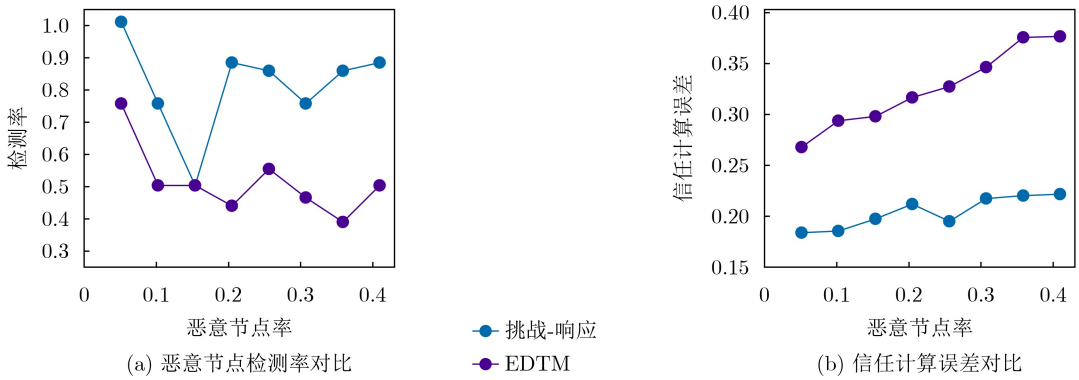


图 8 基于挑战-响应与无挑战-响应方法的性能对比



(a) 恶意节点检测率对比 (b) 信任计算误差对比

图 9 本文算法与EDTM模型算法的性能对比

实施挑战-响应模型来获取普通节点可靠的初始信任值。第2步是利用获得的初始信任值进行分簇并在簇内实现信任值计算和信任值更新，以达到提早检测恶意节点并降低自私节点信任值的目的。仿真实验结果表明，采用挑战-响应后获取的初始信任值可以较为准确地检测出恶意节点并降低自私节点的信任值，使用此初始信任值完成整个可信评估流程后的恶意节点检测率较高且信任计算误差较小，所以在分布式网络中运用挑战-响应模型获取节点的初始信任值并实施完整的可信评估流程是一种解决缺乏历史信任证据问题的可靠手段。由于挑战-响应模型涉及密钥的生成与配送问题，耗时较长，如何做到高效且可靠地获取节点初始信任值来完成可信评估是未来的研究方向。

参 考 文 献

[1] KURDI H A. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems[J]. *Journal of King Saud University - Computer and Information Sciences*, 2015, 27(3): 315–322. doi: 10.1016/j.jksuci.2014.10.002.

[2] SUN Y L, YU Wei, HAN Zhu, *et al*. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): 305–317. doi: 10.1109/JSAC.2005.861389.

[3] ZHANG Degao, GAO Jinxin, LIU Xiaohuan, *et al*. Novel approach of distributed & adaptive trust metrics for MANET[J]. *Wireless Networks*, 2019, 25(6): 3587–3603. doi: 10.1007/s11276-019-01955-2.

[4] JIANG Jinfang, HAN Guangjie, WANG Feng, *et al*. An efficient distributed trust model for wireless sensor networks[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2015, 26(5): 1228–1237. doi: 10.1109/TPDS.2014.2320505.

[5] JIANG Jinfang, ZHU Xinyu, HAN Guangjie, *et al*. A dynamic trust evaluation and update mechanism based on C4.5 decision tree in underwater wireless sensor networks[J]. *IEEE Transactions on Vehicular Technology*, 2020, 69(8): 9031–9040. doi: 10.1109/TVT.2020.2999566.

[6] HAN Guangjie, HE Yu, JIANG Jinfang, *et al*. Fault-tolerant trust model for hybrid attack mode in underwater acoustic sensor networks[J]. *IEEE Network*, 2020, 34(5): 330–336. doi: 10.1109/MNET.001.2000006.

[7] NGUYEN T, HOANG D, NGUYEN D, *et al*. Initial trust establishment for personal space IoT systems[C]. 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, USA, 2017: 784–789. doi: 10.1109/INFCOMW.2017.8116476.

[8] 张志华, 罗守山, 朱洪亮, 等. WSN异步休眠模式下节点捕获早期检测方法[J]. 北京邮电大学学报, 2018, 41(3): 32–38. doi: 10.13190/j.jbupt.2017-228.
ZHANG Zhihua, LUO Shoushan, ZHU Hongliang, *et al*. A node capture early detection scheme for WSN in asynchronous sleep mode[J]. *Journal of Beijing University of Posts and Telecommunications*, 2018, 41(3): 32–38. doi: 10.13190/j.jbupt.2017-228.

[9] LIN Xiaodong. CAT: Building couples to early detect node compromise attack in wireless sensor networks[C]. 2009 IEEE Global Telecommunications Conference, Honolulu, USA, 2009: 1–6. doi: 10.1109/GLOCOM.2009.5425922.

[10] VERGNAUD D. Comment on “efficient and secure outsourcing scheme for RSA decryption in internet of things” [J]. *IEEE Internet of Things Journal*, 2020, 7(11): 11327–11329. doi: 10.1109/JIOT.2020.3004346.

[11] DESAI S S and NENE M J. Node-level trust evaluation in wireless sensor networks[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(8): 2139–2152. doi: 10.1109/TIFS.2019.2894027.

[12] DESAI S S and NENE M J. Multihop trust evaluation using memory integrity in wireless sensor networks[J]. *IEEE Transactions on Information Forensics and Security*, 2021, 16: 4092–4100. doi: 10.1109/TIFS.2021.3101051.

[13] FANG Weidong, ZHANG Chuanlei, SHI Zhidong, *et al*.

BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks[J]. *Journal of Network and Computer Applications*, 2016, 59: 88–94. doi: 10.1016/j.jnca.2015.06.013.

[14] UZUNOĞLU B. An adaptive Bayesian approach with subjective logic reliability networks for preventive maintenance[J]. *IEEE Transactions on Reliability*, 2020, 69(3): 916–924. doi: 10.1109/TR.2019.2916722.

[15] DING Zhuai, YUE Zijie, YANG Shanlin, *et al*. A novel trust model based overlapping community detection algorithm for social networks[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2020, 32(11): 2101–2114. doi: 10.1109/TKDE.2019.2914201.

[16] BOUDAGDIGUE C, BENSLIMANE A, KOBBANE A, *et al*. Trust management in industrial internet of things[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 3667–3682. doi: 10.1109/TIFS.2020.2997179.

[17] ZHANG Juanjuan, SUN Qibo, ZHOU Ao, *et al*. A novel trust update mechanism based on sliding window for trust management system[C]. The 16th International Conference on Computational Science and its Applications, Beijing, China, 2016: 521–528. doi: 10.1007/978-3-319-42085-1_41.

[18] XIONG Li and LIU Ling. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2004, 16(7): 843–857. doi: 10.1109/TKDE.2004.1318566.

[19] WANG Tian, LI Yang, FANG Weiwei, *et al*. A comprehensive trustworthy data collection approach in sensor-cloud systems[J]. *IEEE Transactions on Big Data*, 2022, 8(1): 140–151. doi: 10.1109/TBDATA.2018.2811501.

梁　靓：女，博士，副教授，研究方向为新一代移动通信、可信物联网等.

张镨丹：女，硕士生，研究方向为可信评估、隐私保护.

武彦飞：女，博士生，研究方向为无线网络资源管理、网络切片.

贾云健：男，博士，教授，研究方向为通信与计算融合、新一代移动通信等.

责任编辑：马秀强