doi:10.3969/j.issn.1000-436x.2014.03.011

模拟人群信任和决策机制的协作频谱感知方法

王小毛，黄传河，吕怡龙，王斌，范茜莹，周浩
(武汉大学 计算机学院，湖北 武汉 430072)

摘 要：通过模拟人群内部的信任和决策机制，针对多用户的频谱协作感知一致性问题，提出了一种分布式算法。该算法首先通过网络的历次协作过程预测出各感知用户的动态可信值，据此产生用户的相对可信值，并结合决策机制使得用户之间进行数据交互，随着数据的可信、迭代交互，所有用户状态将趋于一致，最后通过判定算法得出最终结果。算法充分考虑了实际环境中各用户频带感知能力的不平衡性，而且各次级用户只需要进行少量局部数据交换即可实现协作感知，与传统的 OR-rule、1-out-of-N rule 以及普通迭代法有较大区别。对 3 种数据篡改攻击进行了分析，并在预测算法的基础上提出了相应的安全策略。理论分析与仿真结果表明，新算法在准确性和安全性上均优于传统合作频谱感知算法，能显著提高频谱感知准确率，同时兼具较强的防攻击能力。
关键词：认知无线电；一致性；协作频谱感知；数据篡改攻击；可信值；感知能力不平衡性
中图分类号：TP393.0 **文献标识码**：A **文章编号**：1000-436X(2014)03-0094-15

Cooperative spectrum sensing scheme based on crowd trust and decision-making mechanism

WANG Xiao-mao, HUANG Chuan-he, LV Yi-long, WANG Bin, FAN Xi-ying, ZHOU Hao
(School of Computer, Wuhan University, Wuhan 430072, China)

Abstract: A distributed consensus-based scheme by simulating the crowd trust and decision-making mechanism was proposed. This scheme firstly predicts the dynamic trust value among sensing users by the previous cooperative process, and then generates the user's relative trust value, and makes the data interaction among the users by using the combination of relative trust value and decision-making mechanism. All users' state can reach a consensus as the credible and iterative data interaction. All users get the final results by the determinant algorithm. This new spectrum sensing scheme utilizes the imbalance of each users' sensing ability in the real environment. Each secondary user can maintain cooperation with others only through the local information exchange with the neighbors. It is quite different from traditional spectrum sensing scheme, such as OR-rule, 1-out-of-N rule and ordinary iterative method. Three SSDF attacks were analysed, on the basis of the corresponding anti-attack policy was proposed. Theoretical analysis and simulation results show that the new scheme is better than the existing cooperative spectrum sensing algorithm in accuracy and security. New scheme not only can improve the accuracy of spectrum sensing but also has the strong anti-attack capability.
Key words: cognitive radio; consensus; cooperative spectrum sensing; SSDF attack; trust value; imbalance of sensing ability

1 引言

随着无线通信技术的不断发展、通信量的不断增长，频谱作为一种有限的资源，它的利用率越来越受人们的关注。在资源一定的情况下，如何提高资源的有效利用率则成了解决问题的关键。认知无线电(CR, cognitive radio)是一种具有学习能力、能与周围环境进行信息交互、以感知和利用空间中的

收稿日期：2012-12-05；**修回日期**：2013-10-22
基金项目：国家自然科学基金资助项目(61173137)；湖北省自然科学基金资助项目(2010CDA004)；教育部博士点基金资助项目(20120141110002)
Foundation Items: The National Natural Science Foundation of China (61173137); The Natural Science Foundation of Hubei Province (2010CDA004); The Ph.D. Programs Foundation of Ministry of Education of China(20120141110002)

各种频谱的技术[1]。它不仅能提高频谱的利用率，还能探测各种频带的存在性，其具有环境感知和传输参数自我修改的功能。CR 是无线电的一种新的应用方式，它能够在宽频带上可靠地感知频谱环境，探测合法的授权用户(主用户)的出现，能自适应地占用即时可用的本地频谱，同时在整个通信过程中不给主用户带来有害干扰。CR 主要作用是提高频谱资源的利用率，克服因频谱资源有限而带来的不足[2]。目前，认知无线电技术正被应用在新一代的移动自组织网络（MANET, mobile ad hoc network）中[3]。MANET 是一种动态变化、自组织、分布式的网络环境，它的应用越来越广泛，例如军事战场通信、灾难援助、自主车辆通信等，在这种环境下的认知无线电应用简称为 CR-MANET，近几年来越来越多地受到专家、学者的关注。

在现有授权网络的基础上，构建基于主—次分层接入模型的 CR-MANET，不仅能够与现有静态频谱分配体制兼容，又能以低成本的代价获得频谱利用率的大幅提高[4]。因此，频谱感知是 CR-MANET 中需要解决的首要问题，其主要目的是快速可靠地获取周围环境中的动态频谱信息，使各次用户（SU）在不干扰现有主用户（PU）的前提下，实现基于伺机接入方式的频谱共享[4]。为了减少多径及阴影等因素带来的不利影响，让频谱监测结果更为准确，通常采取多个次级用户进行频谱协作[5]感知的方式。现有的协作频谱感知（CSS）方案大部分都需要特定的基站或者融合中心收集所有协作用户的本地感知数据或决策，然后以某种规则进行融合并做出统一判决[6]。但在这种分布式的 MANET 环境中，这些基于融合的 CSS 方案并不实用，因为在这种动态的独立性高的网络中很难找到与所有协作用户都能进行信息交互的节点充当融合中心。针对此问题，文献[7]首次将一致性算法引入到 CSS 中，仅通过邻接点之间进行多次局部信息交互后就能使所有次级用户状态趋于统一，然后通过判决得出最终监测结果。

与大多数信息融合式 CSS 一样，分布式 CSS 也面临着多种潜在的安全威胁。在物理层，伪装主用户攻击[8]是将要面临的主要干扰形式。而在链路层，CSS 的局部信息交互过程更容易受到敌方的攻击[9]，而这些攻击通常都是通过恶意篡改本地感知结果来实现的，故统称为篡改感知数据（SSDF）攻击[8]。

现有的 CSS 文献中一些是针对算法预测结果的准确性进行讨论，由此产生了多种 CSS 策略，如 OR-rule[10]、1-out-of-N rule 以及迭代循环取平均值[11]；一些则是在某算法的基础上对其安全性进行分析，抵抗多种 SSDF 攻击，然后加以改进。其中，对信息融合式 CSS 方案进行讨论的有文献[10,12,13]；对分布式 CSS 研究的有文献[11,14,15]；专门针对 CSS 安全问题进行讨论的有文献[9]。事实上，现有提出的一些策略和算法并没有充分考虑到环境因素带来的影响，特别是在 MANET 这样一种动态的分布式网络结构中，各频谱感应节点由于在实际环境中对噪声、辐射等外界因素的敏感程度不同以及因地理位置的微小差异造成的信号接收强度不同，导致了各节点感知能力的不平衡性、感知结果的不确定性。因此，在必要的安全机制的保障下如何动态挑选出其中优势节点并加以最大化利用从而使得频谱预测结果变得更为准确成了本文的最终目标。

本文通过模拟人群内部的信任和决策机制旨在对一致性 CSS 方案进行完善，提供一种具有较高安全性和准确率的 CSS 方案。在该方案中，人群内部信任机制的引入有助于提高 CSS 抵抗 3 种潜在 SSDF 攻击的能力，而决策机制的引入则用来提高 CSS 在分布式环境下预测结果的准确性，2 种机制相辅相成。由于人群内部的信任和决策机制是生物体经过几千年进化的结果，它不仅具有高合理性，而且具有高安全性，将此 2 种机制结合应用到 CSS 的一致性方案中，能明显提高 CSS 的安全性和结果预测的准确性。通过理论分析和实验结果，证明了所给方案优于传统方案。

2　系统模型

2.1　能量检测

在多用户合作频谱感知模型中，次用户每个 CR 进行能量检测，能量检测器通过检测频带上的能量高低来区别 PU 的存在与否。能量检测可以描述为一种二元假设检验问题，本文采用文献[16]所述的模型以及相应概率分布。

2.2　CSS 的一致性数据融合方案

在 CR-MANET 环境中，N 个次级用户按照上层协议分布在特定范围内，分布式 CSS 可以看作一个典型的多主体协作问题。

为了便于说明，将网络等效为一个连通图 $G=(V,E)$，其中 $V=\{1,2,\cdots,N\}$ 为顶点集合，表示所有次级用户；E 表示边集合，即所有次级用户链路。若以 $\boldsymbol{A}=\{a_{ij}\}$ 表示图的邻接矩阵，且 $a_{ij}\in\{0,1\}$，那么 $E=\{(i,j)\in V\times V, a_{ij}=1\}$，且次用户 i ($i\in[1,N]$) 的邻接点集合为 $Ne_i=\{j\in V\mid a_{ij}=1\}$，其度数为 $d_i=|Ne_i|$，而整个网络的度定义为图 G 的度 $G_{\text{degree}}=\max\{d_i\mid d_i=|Ne_i|, i\in[1,N]\}$。图 1 为在 MANET 环境中具有 9 个节点的网络分布图示例。整个 CSS 过程分成三步，各次级用户首先分别以能量检测算法进行本地感知，然后将检测结果作为该节点初始值 $X_i(0)$，并在局部范围（即与所有邻接用户）进行多次信息交互，信息交换完成后产生新的能量感应值 $X_i(n)$，最后根据 $X_i(n)$ 做出最终决策 D_i，整体流程如图 2 所示。

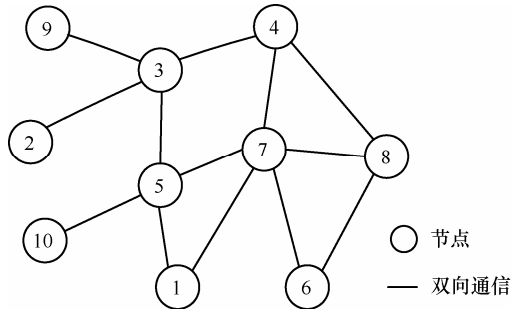


图 1 含 10 个正常节点的分布式认知无线电网络

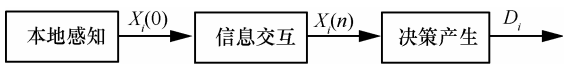


图 2 一致性协作感知方案流程

其中，$n=\{1,2,3,\cdots\}$ 表示信息交互的次数。信息交互规则按照式(1)进行[7]。

$$X_i(n+1)=X_i(n)+k\sum_{j\in Ne_i(n)}(X_j(n)-X_i(n)) \quad (1)$$

其中，$0<k<\Delta^{-1}$，k 称为影响因子，它表示节点 i 在信息交互过程中受周围邻接节点影响的难易程度；Δ 为 MANET 网络的规模大小，一般用节点数目来表示。

当所有节点经过交信息交互后趋于统一的稳定值或者当 $n\geqslant m$（m 为设定的信息交互次数上限）时，终止各节点信息交互，并根据最终交互状态做出决策 D_i，即

$$D_i=\begin{cases}1, X_i(n)>\lambda\\ 0, \text{其他}\end{cases} \quad (2)$$

其中，λ 表示统一设置的判决门限，D_i 为 1 表示 PU 存在，为 0 表示 PU 不存在。

2.3 CSS 面临的安全威胁

在上述的 CSS 方案中，某些节点可能被敌方控制而成为恶意用户，它们通过篡改感知数据而发动 SSDF 攻击，其主要的攻击形式有 3 种[14]：1) 自私型攻击(SFA, selfish attack)，主要是指恶意用户在信息交互过程中始终向邻接用户发送较高的感知状态（相对于检测判决门限），使得邻接用户误以为当前信道被占用，从而使大量空闲频谱被浪费或被敌方侵占；2) 干扰型攻击(IFA, interference attack)，即恶意用户始终发送相对较低的状态值，向其他用户盲目发射，造成对主用户的干扰；3) 混乱型攻击(CFA, confusing attack)，是指恶意用户向外随机发送正常和恶意状态，使相邻用户的迭代过程发生紊乱，从而导致网络的状态始终无法趋于一致。

3 基于人群信任和决策机制的 CSS 方法

3.1 人群内部决策机制及其与 CSS 的映射关系

由于分布式 CSS 可以看作一个典型的多主体协作问题，如果把每个 CR 节点当作一个人，那么 CSS 问题将非常类似于在一群人中（这群人对某问题具有各自的观点）得出一个更合理更能反应客观事物的观点。通常，一般会采取 3 种办法：少数服从多数，以投票的方式产生最后结果；只要其中选“是”的人数大于等于 n（n 为预先设定值），最终结果即为是，否则结果为否；让大家经过多次讨论直到所有人形成统一的观点，然后将这个观点作为最后结论。

以上所说的 3 种方式，如果将第一种方式应用在 CSS 中并不太合理，因为要确定一个频带上的 PU 存在与否并不需要其中大部分节点感应到，某些时候只需要少数节点甚至一个节点能感应到。对于第二种方法，将其应用在 CSS 模型中则显得更为合理些，并且实现起来较简单。但是，在实际环境中，如果回答“是”的节点为恶意节点，那么它将很轻松地就改变整个网络的最后决策，安全性极差；如果这些节点为误判节点，一旦误判节点大于等于 n 则会直接导致最后决策错误，准确性得不到保障。为此，将试着采用第三种方式，但这种方式相对复杂一些。人与人之间讨论和交流本身就是一个复杂的过程，因为每个人在交流过程中被周围人影响的难易以及每个人

影响其他人的能力也不同。综上所述，要将第三种方式应用在 CSS 中，必须量化所有的这些细节。本文则是通过最大程度模拟人群内部决策过程（以上第三种方式）和信任机制(第 3 节重点描述)而提出的一种分布式算法。以下为模拟过程描述。

1) 人们进行讨论的过程中，每个人只会与自己周围的人交流，这种机制类似于网络中的所有节点只与自己邻接节点通信。

2) 讨论开始后，首先会在人群中形成一个讨论圈，确定参与讨论的人群范围，这个过程应用在网络中则是：网络中节点在每一次收到邻接节点信息时会根据最大可容忍的偏差值来确定其是否为正常节点，用以剔除一些恶意节点，在每一轮的信息交互中会在整个网络形成一个通信子集。

3) 人与人交流的结果会受到许多因素的影响，例如，相互之间是否曾经认识，是否了解对方，各自的身份如何，以往交谈的情况如何等。而这些因素在交谈中处于核心位置，因为交谈双方之间的相互信任程度会影响到最终交流结果。为了最大程度摸拟人类这种决策过程，同样在分布式的 MANET 网络中引入了一种可信机制，下一节将会对此进行详细描述，并对其进行数学分析和推导。

4) 人们在围绕某个问题进行讨论是一个多次循环重复的过程，理想情况下，当参与讨论的所有人达到统一观点后结束。在网络中则是通过迭代通信来实现，让所有通信节点在迭代公式的作用下最终趋于一个共同值。

5) 人们在经过多次讨论后达到的统一观点即作为最终结论。在网络中则是将产生的共同值经过某种变型作为最后结果。

3.2　一致性 CSS 方案

既然是模拟人群内部机制，所以在新的 CSS 方案的演化形成过程中，它与所模拟机制拟合度越高，那么它的安全性和准确性则越高。因此，接下来所做的全部分析和推导要么是为了提高网络和模拟机制 2 种方案之间的拟合度，要么是为了从内容上直接提高算法准确性或网络机制的安全性。

3.2.1　信息交互方案

对于任意节点 $i\in\{1,N\}$，定义 $X_i(0)=Y_i$ 为 i 节点初始能量感应值，$X_i(n)$ 为其第 n 次数据信息交互后的能量值，或称为节点状态值，并且此时其邻接用户集合记作 $Ne_i(n)$。若在某时刻节点 i 的状态值为 $X_i(n)$，邻接用户集合为 $Ne_i(n)$，在时间段 T 内，节点 i 与其邻接用户 $Ne_i(n)$ 中的所有合法次用户进行一次数据交互，使得其状态值由 $X_i(n)$ 变为 $X_i(n+1)$，这个过程称之为节点 i 的一次信息交互过程，或节点 i 的第 $n+1$ 次信息交互，时间 T 称之为单步信息交互时长。

若不考虑任何潜在的 SSDF 攻击，并且所有节点按照式(1)进行信息交互，当 n 值足够大时，所有节点状态值都将趋于一个共同的值 X^*，然后通过比较 X^* 与给定阈值 λ 大小，产生最终决策 D_i。由于每一次的信息交互后，所有参与数据交换的节点的状态值总和并没发生改变，即

$$\sum_{i\in\{1,N\}} X_i(n)=\sum_{i\in\{1,N\}} X_i(n+1) \tag{3}$$

进一步推导可得

$$\sum_{i\in\{1,N\}} X_i(0)=\sum_{i\in\{1,N\}} X_i(n) \tag{4}$$

因此，所有节点的数据在经过 n 次更新后其总和并没有发生变化，X^* 最后为所有节点的平均值，即有

$$X^*=\frac{1}{N}\sum_{i\in\{1,N\}} X_i(0) \tag{5}$$

根据式(5)不难看出式(1)即上面提到的 3 种方法（见 3.1 节）中的第二种，其中提到的人数大于等于 n 即相当于这里的 $X^*\geqslant\lambda$ 变型。目前，现有文献中关于 CSS 的分布式算法大部分是基于此种思想。在此，将使得它向第三种方法转换。

首先，由于每一个节点受周围邻接节点影响的程度并不是一个定值，其次，不同节点之间的影响关系并不同。因此，可以将 k 替换成 k_{ij}（k_{ij} 的产生，从其根源上讲，则是由于设备所处的环境及机器之间的微小差异造成的），其表示节点 i 与其邻接节点 j 之间的影响因子，这点与现实社会中每个人易受其他人影响的程度不同是一致的。对于网络中任意节点 i，需要确定其与各邻接节点之间的影响关系，以便在迭代过程中计算下一次的迭代值。将式(1)变为

$$X_i(n+1)=X_i(n)+\sum_{j\in Ne_i(n)}(k_{ij}(X_j(n)-X_i(n))) \tag{6}$$

其中，$0<k_{ij}<\Delta^{-1}$。然而，整个网络通过变型的式(6)进行多次迭代后，所有节点状态值最终能否趋于统一？答案是肯定的。给出定理 1 并予以证明。

定理 1 对于连通网络 $G=(V,E)$，其中 $V=\{1,2,\cdots,N\}$ 为顶点集合；E 表示边集合。若以 $\boldsymbol{A}=\{a_{ij}\}$ 表示图的邻接矩阵，且 $a_{ij}\in\{0,1\}$，那么 $E=\{(i,j)\in V\times V,a_{ij}=1\}$。任意节点 i ($i\in[1,N]$)的邻接点集合为 $Ne_i=\{j\in V\mid a_{ij}=1\}$，其度数为 $d_i=|Ne_i|$，并定义 $X_i(0)$ 为节点 i 初始值，$X_i(n)$ 为其第 n 次数据信息交互后的结果，$Ne_i(n)$ 为其第 n 次信息交互后的邻接用户集合，并且其数据交互规则按式(6)进行（其中，$0<k_{ij}<\Delta^{-1}$，Δ 为网络节点数），则在整个网络数据持续交互中，最终必然会使得网络中所有节点的值相同，此时，称所有节点趋于一致，或网络收敛。

证明 在任意时刻，设网络当前迭代计数为 n，整个网络节点状态值中最大和最小值分别为 $M(n)$ 和 $S(n)$，则有

$$M(n)=\max\{X_i(n)\mid i\in[1,N]\}$$

$$S(n)=\min\{X_i(n)\mid i\in[1,N]\}$$

那么，当整个网络的第 n 次迭代计算完成，迭代计数增为 $n+1$ 后，此时，网络中的最大值和最小值则分别为 $M(n+1)$ 和 $S(n+1)$。显然，在所有节点状态值还未趋于统一之前，必然有 $S(n+1)<M(n+1)$，如果不等式

$$S(n)\leqslant S(n+1)<M(n+1)\leqslant M(n) \tag{7}$$

成立，并且存在正整数 l 使得

$$S(n)<S(n+l)<M(n+l)<M(n) \tag{8}$$

同时成立，则随着迭代次数的不断增多，必然存在正整数 $l'(l'>l)$，使得

$$S(n+l')<S(n+l'+1)=M(n+l'+1)<M(n+l') \tag{9}$$

成立。此时，网络最小值等于最大值，整个网络收敛于 $S(n+l'+1)$。因此，问题转化为证明式(7)和式(8)的正确性。

设当前网络最大值为 $M(n)$，对于网络中任意节点 i，有

$$\sum_{j\in Ne_i(n)}(k_{ij}(X_j(n)-X_i(n)))\leqslant\sum_{j\in Ne_i(n)^+}(k_{ij}(X_j(n)-X_i(n))) \tag{10}$$

其中，$Ne_i(n)^+=\{j\mid j\in Ne_i(n)\text{且}X_j(n)\geqslant X_i(n)\}$，$|Ne_i(n)^+|$ 表示 $Ne_i(n)^+$ 所包含元素个数。因为 $\Delta\geqslant(G_{\text{degree}}+1)\geqslant(d_i+1)$，所以，在 $j\in Ne_i(n)^+$ 时有

$$0\leqslant k_{ij}(X_j(n)-X_i(n))\leqslant\frac{1}{\Delta}(X_j(n)-X_i(n))\leqslant\frac{1}{d_i}(X_j(n)-X_i(n))$$

从而

$$\sum_{j\in Ne_i(n)^+}(k_{ij}(X_j(n)-X_i(n)))\leqslant\frac{1}{d_i}\sum_{j\in Ne_i(n)^+}((X_j(n)-X_i(n)))\leqslant\frac{1}{d_i}\sum_{j\in Ne_i(n)^+}X_j(n)-\frac{|Ne_i(n)^+|}{d_i}X_i(n)\leqslant\frac{|Ne_i(n)^+|}{d_i}(\max\{X_j(n)\mid j\in Ne_i(n)^+\}-X_i(n))\leqslant\max\{X_j(n)\mid j\in Ne_i(n)^+\}-X_i(n)\leqslant M(n)-X_i(n) \tag{11}$$

由式(6)、式(10)、式(11)可知

$$X_i(n+1)=X_i(n)+\sum_{j\in Ne_i(n)}(k_{ij}(X_j(n)-X_i(n)))\leqslant X_i(n)+M(n)-X_i(n)=M(n)$$

即 $X_i(n+1)\leqslant M(n)$。

上式中，由于 i 为任意节点，因此 $M(n+1)\leqslant M(n)$，同理可证 $S(n+1)\leqslant S(n)$，由此可得式(7)成立。

对网络中任意非最大值节点 i，其必然满足 $X_i(n)<M(n)$，若 $\sum_{j\in Ne_i(n)^+}(k_{ij}(X_j(n)-X_i(n)))=0$，则由式(6)和式(10)可得 $X_i(n+1)=X_i(n)<M(n)$。

若 $\sum_{j\in Ne_i(n)^+}(k_{ij}(X_j(n)-X_i(n)))>0$，则

$$\sum_{j\in Ne_i(n)^+}(k_{ij}(X_j(n)-X_i(n)))<\sum_{j\in Ne_i(n)^+}(\Delta^{-1}(X_j(n)-X_i(n)))<\frac{1}{d_i}\sum_{j\in Ne_i(n)^+}(X_j(n)-X_i(n))$$

结合式(11)可得 $\sum_{j\in Ne_i(n)^+}(k_{ij}(X_j(n)-X_i(n)))<M(n)-X_i(n)$，进一步结合式(6)和式(10)可得 $X_i(n+1)<M(n)$。由此得出以下结论。

结论 网络中任意节点 i，若 $X_i(n)<M(n)$，则必有 $X_i(n+1)<M(n)$。

设 $R_{M(n)}=\{i\,|\,i\in[1,N]且X_i(n)=M(n)\}$，其表示最大值节点集合，包含元素个数为 $|R_{M(n)}|$。显然，在网络未收敛前，$R_{M(n)}$ 中至少存在一个节点 i，且 i 具有一个非最大值邻接节点 j，即网络必然存在满足如下条件的 i 和 j

$$i\in R_{M(n)}, j\in Ne_i(n), X_j(n)<X_i(n)$$

则 i 在与其邻接用户进行信息交互时有

$$X_i(n+1)=X_i(n)+\sum_{j\in Ne_i(n)}(k_{ij}(X_j(n)-X_i(n))) < X_i(n)=M(n) \tag{12}$$

从而，可以得到以下结论。

① 若 $M(n+1)=M(n)$，根据式(7)和结论可知 $R_{M(n+1)}\subseteq R_{M(n)}$，而由式(12)知至少存在一个节点 i ($i\in R_{M(n)}, i\notin R_{M(n+1)}$)，使得 $1\leqslant|R_{M(n+1)}|\lessdot|R_{M(n)}|$。因此得出：当 $M(n+1)=M(n)$ 时，$R_{M(n+1)}\subset R_{M(n)}$ 且 $|R_{M(n+1)}|\geqslant 1$。由此可知，若网络最大值保持不变，则最多经过 $l=|R_{M(n)}|$ 次迭代后，$R_{M(n+l)}$ 为空集，此时，$M(n+l)<M(n)$。

② 若 $M(n+1)<M(n)$，即 $l=1$ 时，$M(n+l)<M(n)$。

由①和②可知，存在正整数 $l=|R_{M(n)}|$，使得 $M(n+l)<M(n)$。同理可证，存在正整数 $l=|R_{S(n)}|$，使得 $S(n+l)>S(n)$。因此，存在正整数 $l=Max(|R_{M(n)}|,|R_{S(n)}|)$ 使得

$$S(n)<S(n+l)<M(n+l)<M(n)$$

即式(8)成立。证明完毕！

若不考虑任何潜在的 SSDF 攻击，从以上证明中可以看出，只要给定的 n 足够大，则所有次用户的最终状态都将趋于一致，收敛值记作 X^*。

为了让整个系统能够有效地运行，从式(6)可以看出，需要寻找一种合理的机制来计算 k_{ij} 的值。

首先，给每一个节点 i 赋予一个威望值 V_i（V_i 规定为整数，其含意类似于单个人在其生活群体中具有的威望），V_i 值越高，在信息交互中节点 i 则能更大程度影响其周围邻接节点。由此可知，节点 j 对 i 的影响因子 k_{ij} 与 (V_j-V_i) 成正比。因此，令

$$k_{ij}=\xi(V_j-V_i) \tag{13}$$

其中，$\xi>0$，为比例系数。

从数学的角度分析，(V_j-V_i) 的值有可能为负数而使得 k_{ij} 也为负数，为了避免此种情况的出现，另规定当 $V_j<V_i$ 时，$k_{ij}=\xi$，所以将式(13)变为

$$k_{ij}=\max(\xi(V_j-V_i),\xi) \tag{14}$$

又因为 $k_{ij}<\Delta^{-1}$，所以需将式(14)进一步改为

$$k_{ij}=\min(\max(\xi(V_j-V_i),\xi),\Delta^{-1}) \tag{15}$$

从安全性的角度考虑，V_i 的值既不能由节点 i 自身来确定，又不能保存在本地。因此，V_i 的值应是由其邻接节点 j 来确定，并存储在 j 中。为此，定义

$$T_{(j,i)}=V_i \tag{16}$$

其中，$T_{(j,i)}$ 表示为邻接节点 j 中存储的 i 相对于 j 的威望值。

为了获得一种更通俗的说法，称 $T_{(j,i)}$ 为节点 j 对于节点 i 的信任值，或可信值，其值越高，表示 j 越信任 i，i 的值能更大程度影响 j，并且其值是存储在节点 j 中。根据式(15)和式(16)得 k_{ij} 的值为

$$k_{ij}=\min(\max(\xi(T_{(i,j)}-T_{(j,i)}),\xi),\Delta^{-1}) \tag{17}$$

从式(17)可以看出，节点 i 要计算邻接节点 j 的影响因子 k_{ij} 必须知道 $T_{(i,j)}$ 和 $T_{(j,i)}$ 的值，其中 $T_{(i,j)}$ 为存储在节点 i 内部，为已知，而 $T_{(j,i)}$ 为未知数。因此，节点 j 在每一次将感应值传递给 i 进行数据更新时需同时附带对方可信值 $T_{(j,i)}$。如图 3 所示，i 和 j 通信时，数据发送分组中附带有能量值 X_i，可信值 T_j，迭代计数 n。

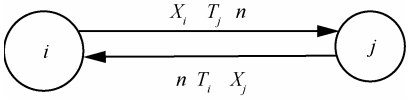


图 3　网络节点通信

根据式(17)可将式(6)变为

$$X_i(n+1)=X_i(n)+\sum_{j\in Ne_i(n)}(\min(\max(\xi(T_{(i,j)}-T_{(j,i)}),\xi),\Delta^{-1})(X_j(n)-X_i(n))) \tag{18}$$

式(18)即为节点之间进行信息交互所用的迭代公式。由于在网络系统运行过程中 $T_{(i,j)}$ 是一个动态变化的值，因此，如何产生和维护 $T_{(i,j)}$ 的值将变得非常重要，成为整个系统的核心问题之一，它直接

关系到算法的好坏和系统的性能。接下来，进一步分析和推导，确定出可信值 $T_{(i,j)}$的计算方法。

3.2.2 可信值计算、使用与更新

既然可信值 $T_{(i,j)}$ 反应的是节点 i 对 j 的信任程度，根据上面的分析，它是一个动态变化的值，它反应的是历史感应情况，其值应该是由节点 j 频谱感应的历史好坏情况来决定。因此，在网络系统建立之初，所有节点对每一个邻接节点的可信值记录皆为 0，随着系统的一次次运行，节点之间的相互通信，每个节点对周围邻接节点都会产生一个相应可信值，并且这个可信值是随着系统的运行而动态变化的。所以，在每个节点内部建立一张表，用于存储邻接节点的可信值，这种存储邻接节点可信值的表称之为可信值表。整个系统在运行过程中，每一次迭代完成后都会产生一个最终结果值 X^*，可信值表的每次数据更新发生在迭代结束之后，为了方便可信值的更新，可信值表内部需额外存储邻接节点的初始能量感应值。由于最终结果是多个节点合作产生的，所以可以假定结果值 X^* 是准确的，或者说是相对准确的。那么，通过比较邻接节点的初始能量感应值和最终结果值 X^*，则可以判断邻接节点初始感应值的准确性，从而来更新该邻接节点的可信值，并更改可信值表记录。可信值表的初始化采用第三方推荐策略，更新则采用慢增长和快恢复策略。

例如图 4 中，标明了图 1 中部分节点（节点 8、节点 4、节点 9）的可信值表，节点 8 的可信值表记录了它的 3 个邻接节点（节点 4、节点 7、节点 6）的可信值。可信值表中包括 3 列数据，分别为节点唯一标识符 ID、邻接节点可信值 Trust、邻接节点初始感应值 X_0。除了标识符 ID 外，其他两项皆为动态变化值。序号为 9 的节点为新加入节点，其可信值表尚未初始化。而序号为 4 的节点和序号为 8 的节点有一个共同邻接节点 7，因此它们的可信值表中的关于节点 7 的初始感应值 X_0 在任意时刻都相同，而可信值 Trust 则不一定相同，因可信值反应的是 2 个节点之间的相互关系，不同节点对同一节点的可信值并不一定相同。

图 4 所示的各节点关系及其内部存储的可信值表，非常类似现实社会网络中各个体（人）之间的相互关系，在每一个人的大脑内部都存储了周围熟悉人的可信值，这种可信值直接影响人与人之间的交流，并且随着不断的信息交换，可信值不断发生变化，从而进一步影响他们之间的交流。

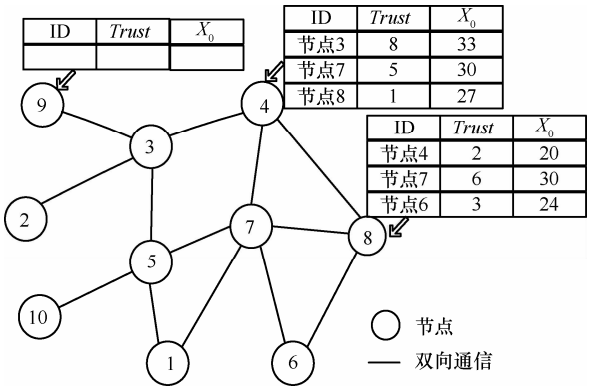


图 4 附带可信值表说明的 10 节点分布式认知无线电网络

在网络运行过程中，每次网络迭代结束后都会出现最终收敛值 X^*，并通过其与邻接节点的初始能量感应值 X_0 之间的关系来更新该邻接节点的可信值。下面将设计一种合理的可信值更新方案。

方案 1 在判决结果为 H_1 ($X^* > \lambda$)时，若 $X^* < X_0$，则采用慢增长（$Trust = Trust + 1$）策略更新可信值，若 $X^* > X_0$，则采用快恢复（$Trust = \left\lfloor \frac{Trust}{2} \right\rfloor$）策略更新可信值；在判决结果为 H_0 ($X^* < \lambda$)时，若 $X^* > X_0$，则采用慢增长策略更新可信值，若 $X^* < X_0$，则采用快恢复策略更新可信值。

不难看出，方案 1 中，在判决结果 H 已经产生的情况下，凡是对 H 的产生起到正面作用的节点均采用了慢增长策略，而凡是对 H 的产生起到负面作用的节点均采用了快恢复策略。因此，网络中的节点其可信值要么慢增长要么快恢复。此种策略下，节点可信值更新过于频繁，整个网络可信值有可能出现动荡不稳定的现象。

方案 2 定义 2 个用于可信值更新的能量判定阈值 $\underline{\lambda}$ 和 $\overline{\lambda}$，且满足 $\underline{\lambda} < \lambda < \overline{\lambda}$。在判决结果为 H_1 ($X^* > \lambda$) 时，若 $\overline{\lambda} < X_0$，则采用慢增长 ($Trust = Trust + 1$)策略更新可信值，若 $\underline{\lambda} > X_0$，则采用快恢复($Trust = \left\lfloor Trust / 2 \right\rfloor$)策略更新可信值，否则，可信值保持不变；在判决结果为 H_0 ($X^* < \lambda$) 时，若 $\underline{\lambda} > X_0$，则采用慢增长策略更新可信值，若 $\overline{\lambda} < X_0$，则采用快恢复策略更新可信值，否则，可信值保持不变。

方案 2 中，若判定为存在，则只有当节点初始能量值高到一定程度，即 $\overline{\lambda} < X_0$ 时，才采用慢增长，

而快恢复则是节点初始值低到一定程度（$\underline{\lambda} > X_0$）时才使用；若判定不存在，则采用相反操作。此种策略下，容易出现所有节点可信值全为慢增长或快恢复的极端情况。

综上所述，结合方案 1 和方案 2 的优缺点，得出第三种方案，并用于可信值更新。

方案 3　定义 2 个用于可信值更新的能量判定阈值 $\underline{\lambda}$ 和 $\overline{\lambda}$，且满足 $\underline{\lambda} < \lambda < \overline{\lambda}$。在判决结果为 H_1 ($X^* > \lambda$)时，若 $X_0 > \max(X^*, \overline{\lambda})$，则采用慢增长($Trust = Trust + 1$)策略，若 $X_0 < Min(X^*, \underline{\lambda})$，则采用快恢复($Trust = \left\lfloor \frac{Trust}{2} \right\rfloor$)策略，否则，可信值保持不变；在判决结果为 H_0 ($X^* < \lambda$)时，若 $X_0 < \min(X^*, \underline{\lambda})$，则采用慢增长策略，若 $X_0 > \max(X^*, \overline{\lambda})$，则采用快恢复策略，否则，可信值保持不变。

方案 3 能保证采用慢增长策略均是对判决结果具有明显正面促进作用的节点，而采用快恢复策略则是对判决结果起到较大负面作用的节点。对于那些中间部分的节点（对结果的产生不具有明显正负面作用）保持可信值不变。

接下来，将给出网络在实际运行过程中各节点内部对可信值表的操作算法，包括可信值表的初始化、更新和使用。

1) 可信值表初始化

在 CR-MANET 建立之初，网络中的节点将其所有邻接用户可信值初始化为 0。

在 CR-MANET 运行过程中，有新节点加入时，该节点采用第三方推荐策略初始化其可信值表。假设新加入节点为 i，Ne_i 为 i 的邻接节点集合，对于任意邻节点 j ($j \in Ne_i$)，设 j 的邻接节点集合为 Ne_j，则 $Ne_i \cap Ne_j$ 为 i 和 j 的公有邻接节点集合，且有 $T_{(j,i)} = 0$，那么节点 i 对于节点 j 的可信值 $T_{(i,j)}$，则计算如下(其余节点类似)。

节点 i 首先向其邻接用户集合 Ne_i 广播 j 的可信值询问数据分组，对于收到数据分组的任意节点 z ($z \in Ne_i$)，查找本地可信值表中 $T_{(z,j)}$ (若不存在，则令 $T_{(z,j)} = -2$)，并返回给 i。i 在收到 Ne_i 中所有节点关于 j 的可信值回复后，形成可信值集合，并剔除其中可信值为-2 的元素，剩余集合记作 T_{Ne_i}，其中 $|T_{Ne_i}|$ 表示可信值记录个数。显然，$|T_{Ne_i}| \leqslant (d_i - 1)$ ($d_i = |Ne_i|$，为节点 i 的度数)，接下来，根据 $|T_{Ne_i}|$ 大小分 3 种情况计算 $T_{(i,j)}$。

(a) 若 $|T_{Ne_i}| \geqslant 3$，则

$$T_{(i,j)} = \frac{Sum(T_{Ne_i}) - Max(T_{Ne_i}) - Min(T_{Ne_i})}{|T_{Ne_i}| - 2} \tag{19}$$

式(19)中，通过减去最大值和最小值来去掉偏离 $T_{(Ne_i \cap Ne_j)}$ 中心最远的二邻接点，用于降低恶意节点篡改可信值使得其过高或过低对网络造成影响的可能性。

(b) 若 $0 < |T_{Ne_i}| < 3$，直接令

$$T_{(i,j)} = \frac{Sum(T_{Ne_i})}{|T_{Ne_i}|} \tag{20}$$

(c) 若 $|T_{Ne_i}| = 0$，则 i 和 j 无共同邻接用户，无法找到第三方来推荐 j 的可信值，由于 j 的可信值不能由 j 决定，此时，令 $T_{(i,j)} = 0$。

从以上过程中可以看出，新加入节点对其他节点可信值的获取是通过第三方推荐来确定的。在新用户收到多个邻接用户上报的可信值后，除了能从中提取出相对可靠的可信值外，同时还能通过判断上报可信值是否处于正常区间 $[0, T_{\max}]$ ($T_{\max}$ 为可信值上限)，以此识别部分恶意用户。由于可信值表初始化仅仅发生在节点新加入到网络或整个网络建立之初时才运行，在无法找到第三方推荐节点时，本着可信值宜小不宜大的原则，直接将其置为 0。

可信值表的使用和更新涉及到数据发送方和数据接收方，下面将对其进行算法描述。

算法 1　（数据发送方）

输入：T（本地可信值表）、Ne（邻接节点集合）

输出：向量组 (X, T_S, n, S)（S 代表任意邻接节点 ID、T_S 为节点 S 可信值、n 为本地迭代计数、X 为本地能量值）

```
begin
    if(T 未初始化)
        初始化 T;
    else
    {
    foreach(S in Ne)
    {
      T_S = find(S,T); //从 T 中查找 S 的记录,
                       返回 S 可信值 T_S，若不
```

存在，则返回 $T_S = 0$

if($T_S != -1$)

{

send(X, T_S, n, S);//将能量值 X 、可信值 T_S 、迭代计数 n 发往目标节点 S

}

}

}

end

算法 2 （数据接收方）

输入：P（从邻接点传来的数据分组）、S（代表 P 中节点 ID）、X_S（表示 S 的能量值）、n_S（表示 S 的迭代计数）、T_S（S 的可信值）、Ne（表示邻接节点集合）、T（本节点可信值表）

输出：X（本节点能量状态值）、n（本节点迭代计数）、T（本节点可信值表）、D（判决结果）

begin

while(true)

{

wait(接收数据分组);

P = receive(数据分组);

从数据分组 P 内提取 S 、X_S 、n_S 值;

if($n_S == n$)

{

if($n == 0$) //存储初始能量值

{

if(T 中关于 S 记录存在)

{

将 X_S 写入 S 对应记录的 X_0 列值;

}

else

在 T 中添加新记录 $(S, 0, X_S)$;

}

将 (S, n_S, X_S) 存入 E; // E 为邻时链表，记录接收到的数据信息

if(E 中记录条数== T 中 Trust 列不为−1 的记录条数) //本次迭代数据接收完毕

{

$n++$;

计算新的 X 值; //将 E 中数据代入式(20)

清空 E;

if($n \geqslant n_{\max}$) //迭代次数超过迭代上限

{

$n = 0$;

D =判决(X);//将 X 和 λ 代入式(3)

foreach(记录 R in T)

{

if($R \to Trust != -1$)// 非恶意用户

{

if($D == 1$) // PU 存在

{

if($R \to X_0 > \max(X^*, \overline{\lambda})$)

$R \to Trust++$;//慢增长

else if($R \to X_0 < \min(X^*, \underline{\lambda})$)

$R \to Trust = \lfloor R \to Trust / 2 \rfloor$;

//快恢复

}

else // PU 不存在

{

if($R \to X_0 < \min(X^*, \underline{\lambda})$)

$R \to Trust++$; //慢增长

else if($R \to X_0 > \max(X^*, \overline{\lambda})$)

$R \to Trust = \lfloor R \to Trust / 2 \rfloor$;

//快恢复

}

}

}

}

}

}

}

end

在算法 2 中，通过慢增长策略保证了能量感应准确性高的节点可信值逐渐增大($T = T + 1$)，随着网络系统的运行，它们能更大程度影响周围邻接节点，增大了其影响最终结果的比重；快恢复策略将可信值进行折半处理($T = \left\lfloor \frac{T}{2} \right\rfloor$)，它能保证中途毁坏节点可信值的快速减小，避免那些高可信值的非正常节点长时间影响周围邻接节点，能迅速减小

其影响最终结果的能力，另外，快恢复算法还能保证恶意节点的可信值始终处于较低状态，减小其影响周围节点的能力，而且，通过折半处理可以保证合法邻接用户可信值始终处于非负状态，处理更方便。

通过可信值表存储邻接节点的可信值，使每个节点能够有效识别出周围邻接节点中那些能量感应准确性高的节点，然后与这些节点进行数据融合，从概率上来讲，它能产生出更接近实际能量值，从而提高最后结果的准确率。从系统的安全性来讲，可信值表机制能有效防止类似 SSDF 攻击，表中记录的可信值既能反应各邻接节点的可信度，又能反应各邻接节点的历史能量感应和通信情况，对于那些新加入的恶意节点由于其可信值在各邻接节点中并无记录，即为 0。因此，恶意节点影响周围邻接节点的能力较小，其能量感应值的大小对最终结果的产生影响并不大。通过可信值表机制能有效削弱恶意节点的攻击性。例如图 5 中，用户 M_1 和 M_2 为新加入的恶意节点，在这种分布式的 MANET 环境中，它们通过发送伪造数据与周边节点进行通信。为了达到攻击目的，它们伪造出来的数据一般要么过高，要么过低，或者随机产生。由于节点在每次通信中都会判断所收到数据是否在有效范围内，一旦超出正常范围则会中止与该节点的通信。因此，M_1 和 M_2 要想达到攻击目的，伪造的数据必须处于有效范围内，但由于恶意节点 M_1 和 M_2 的可信值为 0，它们影响周边节点的能力较小，其发送出去的伪造数据对周边节点数据影响也将非常小。

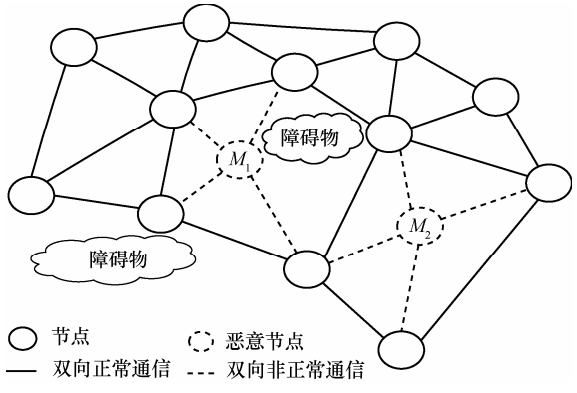


图 5　含 2 个恶意节点的分布式认知无线电网络

因此，其攻击性并不强。随着系统的持续运行，可信值表的不断更新，快恢复策略能有效保证 M_1 和 M_2 的可信值始终处于较低状态，它们的攻击性并不会随着系统的不断运行而有所增长。综上所述可以看出，可信值表机制不仅有助于产生更为准确的最终能量值，而且对系统的安全性提供了保障。

3.3　一致性 CSS 方案的安全策略

在上面分析中，首先推导出了决策算法，即各节点用于信息交互的内部机制和迭代计算公式，然后在此基础上进一步推导出了可信表机制，它们二者是相互合作的关系。那么，后者的产生能否对前者起到反促进作用，即能否通过可信值表机制反推回决策层，对其进行进一步完善？接下来将沿着以上思路继续分析。

网络中的节点 i，在每一次的信息交互中，会收到 Ne_i 中所有邻接用户的状态值，而这些状态值并不一定全是经合法用户法发送，部分节点有可能受敌方控制而发动 SSDF 攻击。也就是说，节点 i 收到的部分信息可能是敌方为了达到某种目的而发送的伪造数据。这些数据要么是过高（SFA），要么是过低(IFA)，要么是随机伪造(CFA)。为了防止 3 种 SSDF 攻击，可以从数据的 3 种伪造形式着手。

3.3.1　SFA 和 IFA 攻击防御

任意次用户在收到邻接用户发送的状态值后，首先检查该值是否处于正常能量感应值正常范围内。不妨设某节点为 i，收到其一邻接用户 j 状态值 $X_j(n)$，i 节点首先检查 $X_j(n)$ 是否处于能量正常数值区间 $[\lambda_{\min},\lambda_{\max}]$ 内。若 $X_j(n)\in[\lambda_{\min},\lambda_{\max}]$ 成立，则认为是合法用户，继续运行；否则，认为 j 为恶意用户，立即修改可信值表，将 j 可信值标识为-1，并将 j 从 i 邻接用户集合中剔除掉，即执行 $T(i,j)=-1, Ne_i(n)=Ne_i(n)-j$。如果网络在迭代过程中，有邻接用户始终发送不变的偏高或偏低的状态值（属于正常区间 $[\lambda_{\min},\lambda_{\max}]$ 内），则其检测方法按下面的 CFA 攻击防御策略处理。

3.3.2　CFA 攻击防御

CFA 攻击的特点是恶意用户所发送的数据是随机的，在正常范围内忽大忽小，目的是使迭代过程发生紊乱。而合法次用户随着迭代次数的增多，其感知状态值将逐步向最终收敛值 X^* 靠拢，其整体波动性将会有下降的趋势，相邻数据段之间的波动差值应逐渐减小。相比之下，恶意用户由于其上报给邻接节点的状态值并无规律性（或始终不变），其波动性呈现无规律状态。根据这一特点，利用如

下方法，可以将恶意用户剔除掉。

定义函数

$$S_i(n_s,n_d)=\sum_{n=n_s}^{n_d}(X_i(n)-\bar{X}_i(n_s,n_d))^2 \tag{21}$$

其中，

$$\bar{X}_i(n_s,n_d)=\frac{1}{n_d-n_s}\sum_{n=n_s}^{n_d}X_i(n) \tag{22}$$

$S_i(n_s,n_d)$ 表示 i 节点在迭代过程中状态序列值从 $X(n_s)$ 到 $X(n_d)$ 的方差，方差计算所包含的序列长度为 (n_d-n_s+1)，称之为检验步长，$X(n_s)$ 为序列段起始值，$X(n_d)$ 为序列段终止值，$\bar{X}_i(n_s,n_d)$ 表示该序列段均值。

显然，函数 $S_i(n_s,n_d)$ 反应的是次用户 i 从 n_s 到 n_d 序列段的波动水平，其值越小，表示该段序列值越集中，波动越小；反之，则越分散，波动越大。

因此，对于邻接用户 j，$j\in Ne_i$，设定其检验步长为 l。若不等式

$$S_j(0,l-1)>S_j(l,2l-1)>S_j(2l,3l-1)\cdots \tag{23}$$

不成立（此时若将其判定为恶意节点，少数情况下会出现误判现象），则进一步验证，判断不等式

$$\begin{aligned}&|S_j(0,l-1)-S_j(l,2l-1)|>|S_j(l,2l-1)-S_j(2l,3l-1)|>\\&|S_j(2l,3l-1)-S_j(3l,4l-1)|>|S_j(4l,5l-1)-S_j(5l,6l-1)|\\&>\cdots\end{aligned} \tag{24}$$

是否成立，若也不成立，则将 j 判定为恶意用户，立即修改可信值表，并将 j 从 i 邻接用户集合中剔除掉，即执行 $T(i,j)=-1,Ne_i=Ne_i-j$。在式(23)和式(24)的联合检验下，不仅能将误判概率减到最小，而且能将恶意节点剔除。

为了防止恶意用户上报针对检验步长 l 的具有一定规律的状态序列值，在每一次检验完毕后，可以使 l 值在设定区间 $[l_{\min},l_{\max}]$ 内随机跳动，进一步增强其安全性。

从以上 CFA 防御策略可知，网络中的每个用户需存储其所有邻接用户最近 $3l_{\max}$ 次上报数据，用于计算各数据段之间的波动关系，通过其数据相关性判断该节点是否为恶意用户。

至此为止，假设了网络中的所有节点都能知道自己的邻接节点，并在任意时刻都能和其邻接节点进行可靠稳定的通信，而且网络拓扑结构在每一次的频谱感知过程中不会发生变化。

4 CSS 方法特性分析

4.1 网络的连通性和收敛性

在上面迭代规则(式(18))中，各次用户无需网络的任何先验知识，只需根据其自身状态值、可信值表以及邻接点状态进行数据更新，因此该规则适用于大型的分布式网络中。在不考虑任何攻击的条件下，整个网络可等效为非时变图，由式(6)的证明可知，该规则能保证所有次用户的状态最终趋于一致。然而，在攻击条件下，为了抵御 SSDF 攻击而引入安全策略后，各次用户的邻接点集合在信息交互过程中将不断变化，网络应等效为一个动态的有向图。将所有合法次用户构成的动态子图记为 $G_a(n)=(V_a,E_a(n))$，其中 V_a 和 $E_a(n)$ 分别表示合法次用户顶点集合以及边集合。根据文献[17]的结论可知，只要在足够多次迭代过程中所形成的一系列子图的集合

$$\bigcup_{i=n}^{n+T}G_a(i)=\{G_a(n),G_a(n+1),\cdots,G_a(n+T)\} \tag{25}$$

能够保证强连通，即具有生成树，则所有合法次用户的一致收敛特性仍可以得到保证。显然，迭代规则(式(1))将使整个网络最终收敛于平均值，即

$$X_i(n)\to X_1^*=\frac{1}{m}\sum_{i=1}^{m}Y_i,n\to\infty \tag{26}$$

而通过改进后的数据交互规则(式(18))以及可信值表的引入，网络的最终收敛状态值则会在初始平均值上下波动

$$X_i(n)\to X^*=\frac{1}{m}\sum_{i=1}^{m}Y_i+\theta,n\to\infty \tag{27}$$

其中，θ 表示以平均值为中心的偏离值。显然，θ 值的产生正是可信值表产生的结果，它能让 X^* 更接近实际能量值。

4.2 收敛过程分析

从迭代式(6)可以看出，在网络初始运行阶段，$|X_j(n)-X_i(n)|$ 将会相对较大，而随着迭代记数 n 的变大，$|X_j(n)-X_i(n)|$ 将会有逐渐减小的趋势（偶尔会出现个别增大的情况），最后直到整个网络收敛，$|X_j(n)-X_i(n)|$ 变为 0。所以，整个网络在运行过程中，各用户前期状态值波动较大，而中后期则波动较小，进入收敛阶段。因此，可以将网络运行过程分成 2 个时间段：网络同化期和网络收敛期。在同化期，$|X_j(n)-X_i(n)|$ 相对较大，此时

$k_{ij}(X_j(n)-X_i(n))$中的可信因子k_{ij}能发挥更大的作用；而在收敛期，$|X_j(n)-X_i(n)|$较小，k_{ij}作用将会降低。为了加大网络的同化作用以及加快网络的收敛速度，可以做出如下处理。

同化作用：在网络同化期，由于$0<k_{ij}<\Delta^{-1}$，结合式(17)可知，要加大同化作用，就需让可信值有更大的增长空间（即降低Δ值）。从定理 1 的证明可知，Δ只需满足$\Delta \geqslant (G_{\text{degree}}+1)$即可。为此，令$\Delta = G_{\text{degree}}+1$，此时各节点可信值会有更大的增长空间，$k_{ij}$将会有更大的取值区间，网络同化作用将得到加强。

收敛加速：在网络收敛期，由于k_{ij}作用的降低以及同化作用已基本完成，此时，网络的主要任务就是尽快收敛。因此，为了加快收敛速度，网络一旦进入收敛阶段，就让k_{ij}始终取最大值，即令$k_{ij} \equiv G_{\text{degree}}+1$。

至于网络同化期和网络收敛期的区分，则可通过迭代次数的区间划分。设置迭代记数阈值n_c，$n<n_c$时，属于网络同化期；$n \geqslant n_c$时，属于网络收敛期。n_c一般取在收敛所需总迭代次数的1/3左右，或根据经验值来设定。

4.3　时效性分析

从 CSS 的整体框架来看，本文采用的方法和该领域已有的部分文献类似，如文献[7,9,11]，都是采用图 2 所示的操作流程，区别在于已有文献以式(1)为计算基础，而本文采用的是式(18)。因此，从时效性的角度来分析，本文与文献[7,9,11]的对比可以归结为式(1)与式(18)之间的对比，它们都需要经历通信、本地计算、通信 3 个步聚，并且一直循环下去，直到网络收敛。3 个步聚中，通信过程几乎无差别（仅数据分组中多了一个图 3 所示的 T 变量），真正差别在于本地计算。在本地计算中，式(18)引入了可信值的概念，而可信值的 3 个阶段（初始化、更新、使用）中的前 2 个阶段都是在网络收敛之后或能量感知之前才会运行，对 CSS 的时效性无影响。因此，式(18)的本地计算与式(1)相比，仅多了一次 IO 操作（即从本地取 T 值）。

从以上分析可知，本文的方法与已有文献[7,9,11]相比，在通信上，数据分组中增加了一个变量；在计算上，多了一次 IO 操作，而此两点在整个流程（如图 2 所示）中占据的时间开销几乎可以忽略不计。

而本文在引入加速收敛方法（见 4.2 节中）后，随着收敛速度的提高，整体时效性将会比同类文献（如文献[7,9,11]）要高。

4.4　检测结果准确性分析

为了便于对检测结果准确性进行分析，首先对虚警概率Q_{f}和漏检概率Q_{m}予以简要说明，Q_{f}反应的是频谱的利用率，其值越高说明频谱利用率越低，而Q_{m}反应的是主用户在使用频带过程中被干扰的概率，其值越高，被干扰机率越大。

随着网络的多次运行，各节点可信值记录生成并且相对稳定后，在正常情况下，若 PU 不存在，即H_0，则由于部分高可信值节点能量检测能力相对较强，初始能量感应值会较低，这些节点的共同作用将会拉低整个网络最终收敛值，使得$\theta<0$；若 PU 存在(H_1)，同理有$\theta>0$。因此，Q_{f}和Q_{m}满足

$$\begin{aligned} Q_{\text{f}} &= P\{X^* > \lambda \mid H_0\} \\ &= P\{X_1^* + \theta > \lambda \mid H_0\} < P\{X_1^* > \lambda \mid H_0\}, \theta < 0 \end{aligned} \tag{28}$$

$$\begin{aligned} Q_{\text{m}} &= P\{X^* < \lambda \mid H_1\} \\ &= P\{X_1^* + \theta < \lambda \mid H_1\} < P\{X_1^* < \lambda \mid H_1\}, \theta > 0 \end{aligned} \tag{29}$$

由文献[9]知

$$P\{X_1^* > \lambda \mid H_0\} = 1-\Gamma(\frac{m\lambda}{2}, mTW) \tag{30}$$

$$p\{X_1^* < \lambda \mid H_1\} = 1-\int_{\gamma_0} Q(\sqrt{2TW\gamma_0}, \sqrt{m\lambda}, mTW) f_{\gamma_0}(x) \tag{31}$$

因此，

$$Q_f < 1-\Gamma(\frac{m\lambda}{2}, mTW) \tag{32}$$

$$Q_m < 1-\int_{\gamma_0} Q(\sqrt{2TW\gamma_0}, \sqrt{m\lambda}, mTW) f_{\gamma_0}(x) \tag{33}$$

其中，γ_0是所有合法用户的平均信噪比之和，$f_{\gamma_0}(x)$是γ_0的概率密度函数，$Q(\cdot,\cdot,\cdot)$和$\Gamma(\cdot,\cdot)$分别是 Marcum Q 函数和非完全 gamma 函数。

显然，随着网络的不断运行，可信值表会越来越成熟，在其他条件不变的情况下，式(28)和式(29)中的$|\theta|$会越来越大，Q_{f}和Q_{m}则会越来越小，从而，整个网络性能会随着时间推移越来越高，式(32)和式(33)可作为虚警概率和漏检概率理论上限。

在网络规模上，若节点分布大致均匀，节点数

多，则能获得更多关于该区域能量值，通过迭代计算，并选取好合适的能量判定阈值，以此得到的检测结果更能接近实际频谱使用情况。但网络节点总数也有一定限制，节点的个数不能大到影响该区域内部的正常、稳定通信。

5　仿真结果

本节通过仿真实验对提出方案的有效性进行验证和讨论，并与文献[11]给出的基本方案进行对比。为了兼顾算法的准确性和安全性，实验以图 1 和图 5 的拓扑结构为例，分别对 2 种情况进行仿真。图 1 用以分析算法准确性，图 5 则用来考虑其安全性。

图 1 所示分布式 CRN 由 10 个正常次用户、13 条链路组成。假设各次用户的感知信道为独立同分布的 Suzuki 衰落信道[18]，功率发散因子为 $\sigma = 8$ dB，各用户本地能量检测的时间带宽积 $m = 20$，平均 SNR 分别在 0 ~ 5 dB 范围内均匀分布，信息交互的最大迭代次数为 120，本地感知的初始值根据文献[16]中的能量感知模型随机产生，由于现实中每个节点所处环境以及节点内部器件的微小差异导致其感知能力的不平衡性。因此，在网络运行过程中，为了让仿真更加逼近实际，初始值还需进一步结合每个节点的感知能力值，能力值的确定这里采用随机模式生成。为了得到所提出算法在 CRN 中的性能，通过观察 Q_f 和 Q_m 在不同参数下的变化值，并在同等条件下与 OR-rule[9]（它比 AND-rule、MAJORITY-rule 好）以及普通迭代法[11]进行对比，最终得出结论。在 OR-rule 合作频谱感知算法中，每个次用户通过本地感知系统与既定阈值比较判断 PU 是否存在，若存在，则为 1；否则为 0，最终所有次用户将二进制数发往集中控制器节点，由集中控制器进行数据累加，若最终总和大于等于 1，则 PU 存在，否则不存在。普通迭代法，即迭代取平均值法，将整个网络中次用户感知的能量值进行迭代融合，待网络收敛后，通过收敛值与既定阈值进行比较从而来判断 PU 的存在性，其核心思想为式(1)。针对图 1 的网络场景，对本文提出的方案进行了 10 000 次仿真，然后取平均值，图 6 为 Q_f 和 Q_m 的变化趋势曲线。在图 6 中，曲线旁的数字标注为对应阈值 λ（单位：dB）。从第三条曲线（本文提出方法）中可以看出，当 λ 取值在 47 dB 附近时，Q_f 和 Q_m 可同时达到 10^{-3} 左右，相比之下，其他 2 条曲线 λ 最佳取值分别在 47 dB 和 52 dB，而对应 Q_f 和 Q_m 值则分别处于 10^{-2}~10^{-3} 和 10^{-2}，通过 3 条曲线可以看出，本文提出的方法在性能上要比 OR-rule 和普通迭代法好。

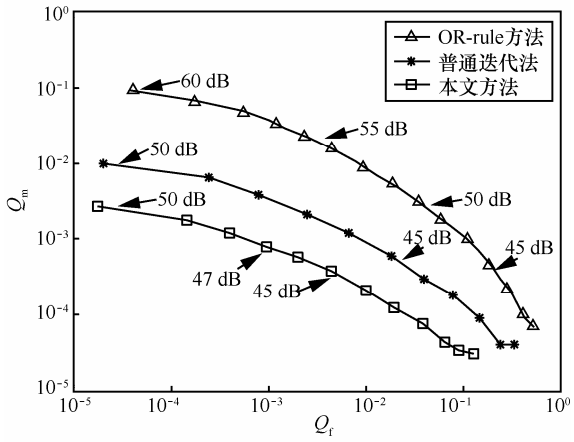


图 6　无攻击时的 CROC 特性曲线

图 6 中除了 OR-rule 属于集中控制方式，其余 2 种则属于分布式控制方式。由于 OR-rule 性能与另外 2 种相差较远，而且其安全性也不高。因此，在考察本文提出算法的安全性时，主要通过其与迭代平均值法进行比较。仿真过程中由于网络迭代次数有限，而且个别用户不可避免地会受到攻击的影响。因此，网络收敛定义适当放宽，当网络节点最大值与最小值的差值小于 0.1 dB 时，网络即认为收敛。接下来在对图 5 所示的网络场景进行仿真模拟中，检验步长 l 的随机取值区间设置为 [8,12] 。

表 1　不同攻击形式下网络节点状态收敛率

攻击形式	迭代平均值法	本文方法
无攻击	100%	98.6%
SFA 攻击	0%	93.4%
IFA 攻击	0%	92.2%
CFA 攻击	0%	93.8%

若图 5 网络场景中全为合法用户，即无攻击情况下，网络节点收敛率比普通迭代平均值法略低，如表 1 所示，达到 98.6%左右；若 M_1 和 M_2 为恶意节点，在其 3 种 SSDF 攻击形式下，由于安全策略的引入，少数情况下会将部分合法用户误当成恶意节点，因此收敛率要更稍低些。另外，针对图 5 网络场景，分别进行了以下 3 种情况下的仿真。

(a) M_1 和 M_2 皆为恶意节点，随机选择 3 种 SSDF 攻击方式。

(b) M_1 为恶意节点，攻击方式随机选择，M_2 为

正常节点。

(c) M_1 和 M_2 皆为正常节点。

在 SFA 攻击方式中，节点持续向周围用户发送偏高感知状态值“120”，而 IFA 方式则是节点持续向周围用户发送偏低感知状态值“1”，对于 CFA，节点持续向周围用户发送[0,100]区间内随机状态值。通过 10 000 次仿真模拟取平均值，得出如图 7 和图 8 所示概率对比图。

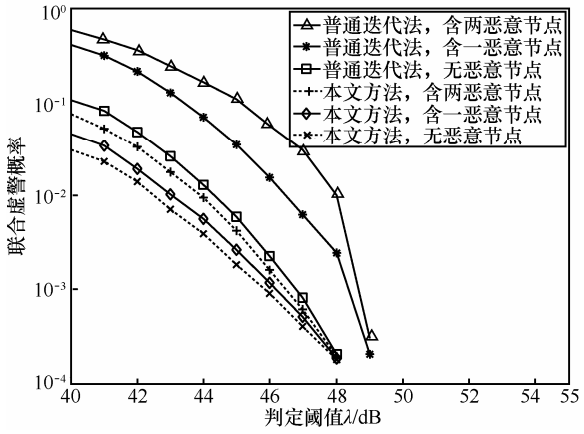


图 7　不同算法中联合虚警概率对比

在图 7 中，上面 3 条曲线为普通迭代法在(a)、(b)、(c) 3 种情况下的模拟结果，从中可以看出，由于普通迭法并没引入很强硬的安全措施，3 条曲线相隔较远；而下面 3 条则是本文所提供方法对应曲线图，其 Q_f 值比对应普通迭法中的要小，而且，对于(a)、(b)、(c) 3 种情况，3 条曲线相差并不远，证实安全策略的引入对算法起到了显著作用。同样，图 8 中包含了同等情况下 6 条 Q_m 值的对比曲线，从各曲线以及曲线之间的对比程度说明了本文算法的优越性以及安全策略的有效性。

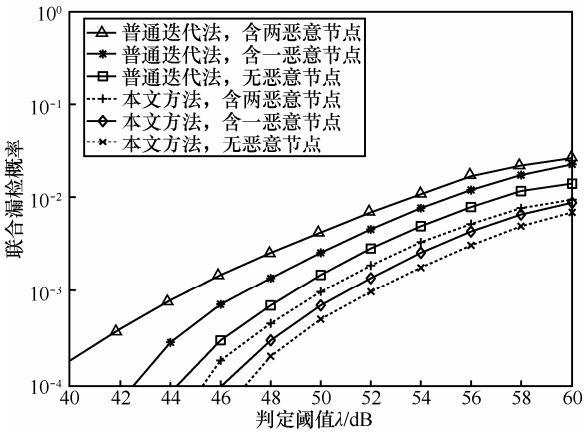


图 8　不同算法中联合漏检概率对比

6　结束语

本文重点研究了 MANET 环境中认知无线电频谱感知的问题。通过将人类之间的信任和决策机制很好地投射到此类问题中，除了能实现算法的分布式外，还解决了分布式算法中一种类似于动态权值的问题（包括这种“权值”的初始化、自动更新以及应用），并且在这种复杂机制中引入了安全算法，算法的准确性也得到了保障。仿真结果表明，利用本文算法不仅能增强 PU 探测的准确性，并且对各种恶意攻击具有较强抵抗能力。在未来的工作中，作者将进一步优化本文提出的 CSS 方法，并将该方法应用到认知无线电各领域中。

参考文献：

[1] UYANIK G S, OKTUG S. A QoS based cooperative spectrum utilization in cognitive radio networks[A]. Sarnoff Symposium (SARNOFF), 2012 35th IEEE[C]. 2012.1-5.

[2] HAYKIN S. Cognitive radio: brain-empowered wireless communications[J]. IEEE JSAC, 2005,23:201-221.

[3] AKYILDIZ I F, LEE W Y, CHOWDHURY K R. CRAHN: cognitive radio ad hoc networks[J]. Ad Hoc Net, 2009,7(5): 810-836.

[4] TO B L, OTMANI M, NGUYEN T M T. Decentralized cooperative spectrum sensing for cognitive radio ad-hoc network: hidden terminal awareness approach[A]. Information Science, Signal Processing and their Applications(ISSPA), 2012 11th International Conference on[C]. 2012. 146-151.

[5] 朱佳, 郑宝玉, 邹玉龙. 基于最佳中继选择的协作频谱感知方案研究[J]. 电子学报，2010,38(1):92-98.
ZHU J, ZHENG B Y, ZOU Y L. Cooperative spectrum sensing in multiuser cognitive radio networks with best relay selection[J]. Acta Electronica Sinica, 2010,38(1):92-98.

[6] SHEN B, ULLAH S, KWAK K. Deflection coefficient maximization criterion based optimal cooperative spectrum sensing[J]. AEU-International Journal of Electronics and Communications, 2010, 64(9): 819-827.

[7] LI Z, YU F R, HUANG M A. Cooperative spectrum sensing consensus scheme in cognitive radios[A]. INFOCOM[C]. Leblon, 2009. 2546-2550.

[8] CHEN R L,PARK J M, BIAN K G. Robust distributed spectrum sensing in cognitive radio networks [A]. INFOCOM [C]. Phoenix, 2008. 31-35.

[9] 刘全, 高俊, 郭云玮等. 抗 SSDF 攻击的一致性协作频谱感知方案[J]. 电子学报, 2011, 39(11):2643-2647.
LIU Q, GAO J,GUO Y W, *et al*. Securing consensus-based cooperative spectrum sensing against spectrum sensing data falsification at-

tacks[J]. Acta Electronica Sinica, 2011, 39(1):2643-2647.

[10] LETAIEF K, ZHANG W. Cooperative communications for cognitive radio networks[J]. Proc IEEE, 2009,97(5):878-893.

[11] YU F R, HUANG M Y, TANG H. Biologically inspired consensus-based spectrum sensing in mobile ad hoc networks with cognitive radios[J]. IEEE Network, 2010, 24(3):26-30.

[12] NALLAGONDA S, ROY S D, KUNDU S. Cooperative spectrum sensing with censoring of cognitive radios in Rayleigh fading channel[A]. National Conference on Communications (NCC)[C]. 2012. 1-5.

[13] LI H S, HAN Z. Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: an abnormality detection approach[A]. DySPAN[C]. Singapore, 2010. 1-12.

[14] YU F R, TANG H, HUANG M. Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios[A]. MILCOM[C]. Boston, 2009.1-7.

[15] RIBEIRO F C, CAMPOS M L R, WERNER S. Distributed cooperative spectrum sensing with adaptive combining[A]. 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)[C]. 2012. 3557-3560.

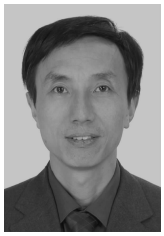
[16] URKOWITZ H. Energy detection of unknown deterministic signals[J]. Proceedings of the IEEE, 1967, 55(4):523-531.

[17] REN W, BEARD R W. Consensus seeking in multiagent systems under dynanically changing interaction topologies[J]. IEEE Trans on Automatic Control, 2005, 50(5):655-661.

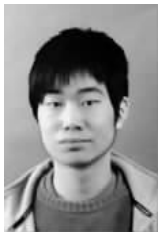
[18] KYPEROUNTAS S, CORREAL N, SHI Q. Performance analysis of cooperative spectrum sensing in suzuki fading channels[A]. The 2nd CrownCom[C]. Orlando, 2007.428-432.

作者简介：

王小毛（1984-），男，湖北天门人，武汉大学博士生，主要研究方向为移动 ad hoc 网络、计算机图形学等。

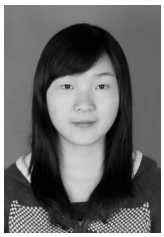


黄传河（1963-），男，湖北随州人，博士，武汉大学教授、博士生导师，主要研究方向为移动互联网、移动 ad hoc 网络、无线传感器网络、无线 mesh 网络、WDM 网络、物联网、网络安全、分布并行处理。



吕怡龙（1989-），男，河南平顶山人，武汉大学硕士生，主要研究方向为移动 ad hoc 网络。

王斌（1989-），男，河南郑州人，武汉大学硕士生，主要研究方向为移动 ad hoc 网络。



范茜莹（1990-），女，河南驻马店人，武汉大学硕士生，主要研究方向为移动 ad hoc 网络。

周浩（1979-），男，湖北武汉人，博士，武汉大学讲师，主要研究方向为无线网络、物联网、云计算。