计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191100124

基于能量分类器的抗 SSDF 攻击协作频谱感知算法

丁诗铭[1,2]　王天荆[1]　沈　航[1,2]　白光伟[1]
1 南京工业大学计算机科学与技术学院　南京 211816
2 南京大学计算机软件新技术国家重点实验室　南京 210093
(dwaxer@163.com)

摘　要　频谱感知是认知无线电通信的重要环节,SSDF(Spectrum Sensing Data Falsification)是协作频谱感知面临的严重安全威胁。SSDF 攻击方式逐渐呈现动态化的趋势,传统防御算法因假定攻击强度保持不变而难以识别动态的篡改数据。针对动态化的 SSDF 攻击,提出一种基于能量分类器的抗 SSDF 攻击协作频谱感知算法。该算法首先通过分析动态 SSDF 攻击的特性,结合距离判别法将邻居节点能量分类,通过将分类结果与本地结果进行对比来识别恶意邻居节点;然后本地节点在滑动时间窗内根据历史频谱判决信息和当前频谱判决信息建立信誉模型,并由此更新各邻居节点的信誉值;最后,本地节点实施加权协作频谱感知。仿真结果表明:相比 LDCSS(Largest Deviation-based distributed Cooperative Spectrum Sensing)算法和 RBCSS(Reputation-based Cooperative Spectrum Sensing)算法,所提算法在动态 SSDF 攻击的攻击强度接近阈值时频谱检测概率分别提高了 15%和 16%,显著增加了认知网络的协作频谱感知性能,提升了频谱共享的效率。

关键词:分布式频谱感知;数据篡改;能量检测法;距离判别;信誉值
中图法分类号　TP393

Energy Classifier Based Cooperative Spectrum Sensing Algorithm for Anti-SSDF Attack

DING Shi-ming[1,2],WANG Tian-jing[1],SHEN Hang[1,2] and BAI Guang-wei[1]
1 College of Computer Science and Technology,Nanjing Tech University,Nanjing 211816,China
2 State Key Laboratory for Novel Software Technology,Nanjing University,Nanjing 210093,China

Abstract　Spectrum sensing is an important part of cognitive radio communication and is under the serious threats of spectrum sensing data falsification (SSDF) in terms of security,which trends dynamically in the attacking methods nowadays. It is difficult to identify dynamic tampered data using traditional defense algorithms because the traditional ways always assume that the attacking strength remains unchanged. Aiming at the dynamic SSDF attack,an energy classifier enabled cooperative spectrum sensing algorithm for anti-SSDF attack is proposed. This algorithm firstly analyzes the characteristics of dynamic SSDF attacks,combines with the distance discriminant method to classify the neighbor users. Then it identifies the malicious neighbor users by comparing the classification results with the local results. Afterward the local user establishes a reputation model under the sliding time window based on the information of historical results,thereby updates the reputation values of neighbor users and will eventually implement weighted cooperative spectrum sensing. The simulation results show that compared with the largest deviation-based distributed cooperative spectrum sensing (LDCSS) algorithm and the reputation-based cooperative spectrum sensing (RBCSS) algorithm,this algorithm provides an increased spectrum detection probability by 15% and 16% respectively when the attacking strength is close to the threshold,which not only significantly increases the cooperative spectrum sensing performance of the cognitive network,but also improves the efficiency of spectrum sharing.

Keywords　Distributed spectrum sensing,Data falsification,Energy detection algorithm,Distance discrimination,Trust value

到稿日期:2019-11-18　返修日期:2020-04-25　本文已加入开放科学计划(OSID),请扫描上方二维码来获取补充信息。
基金项目:国家自然科学基金项目(61502230,61501224);江苏省自然科学基金项目(BK20150960);江苏省普通高校自然科学研究项目(15KJB520015);江苏省六大高峰人才基金资助项目(RJFW-020);南京市科技计划项目(201608009);南京大学计算机软件新技术国家重点实验室资助项目(KFKT2017B21)
This work was supported by the National Natural Science Foundation of China(61502230,51501224),Natural Science Foundation of Jiangsu province,China(BK20150960),Natural Science Foundation of the Higher Education Institutions of Jiangsu Province,China(15KJB520015),Six Peak Talents Foundation of Jiangsu Province,China(RJFW-020),Nanjing Science and Technology Plan Project,China(201608009) and State Key Laboratory for Novel Software Technology,Nanjing University(KFKT2017B21).
通信作者:沈航(hshen@njtech.edu.cn)

1 引言

认知无线电网络(Cognitive Radio Networks，CRN)[1]中的频谱感知是认知无线电(Cognitive Radio，CR)用户伺机使用主用户(Primary User，PU)[2]授权频谱传输数据的关键技术。由于设备故障、信道阴影衰落和噪声等影响，常导致单个 CR 用户误判 PU 占用信道状态。CR 用户间的协作频谱感知(Cooperative Spectrum Sensing，CSS)[3]能够解决上述问题，有效提高频谱感知的效率与可靠性[4]。然而，当 CR 用户间存在恶意用户时，这些恶意用户会向邻居用户传输虚假的感知信息，误导邻居用户做出错误的判决，从而导致网络资源浪费或者信息拥塞，极大地降低整个 CRN 的频谱感知性能[5]。因此，对 CRN 中恶意用户的检测与防御尤为重要。

CRN 中常见的攻击有模拟主用户攻击(Primary User Emulation Attack，PUEA)[6]和频谱感知数据伪造攻击(Spectrum Sensing Data Falsification，SSDF)[7]。前者根据 PU 位置与信号的强弱发动攻击，后者通过篡改感知数据发动攻击。前一种攻击所需的 PU 情况很难获得，因此恶意用户更易发动 SSDF 攻击。常见的 SSDF 攻击有 3 种：1)利用攻击，即恶意用户向邻居用户发送较高的感知能量值，使邻居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恶意用户侵占；2)破坏攻击，即恶意用户始终发送相对较低的状态值，使其他用户盲目发送数据，从而降低 PU 的判决准确度；3)混乱型攻击，即恶意用户向外随机发送正常和恶意的感知信息，使相邻用户的频谱判决产生紊乱，导致协作感知结果与频谱真实状况不一致[8]。利用攻击和破坏攻击篡改能量值的方式相对单一，通过能量检测法[9]很容易被识别出来。但是混乱型攻击篡改能量值的方式灵活且攻击力强，传统检测方法[10]无法识别这种攻击。因此，分析混乱型攻击的特征以有效地抗御 SSDF 攻击是亟待解决的问题之一[11-13]。

针对 SSDF 攻击，文献[14]要求 CR 用户对其本地感知结果进行预判决，只有满足可靠判决的 CR 用户才能将感知结果发送到融合中心，再由融合中心进行融合操作获得最终频谱判决结果[15]。这种防御方法不仅会丢失受到环境或信道影响的正常 CR 用户，造成本地感知结果不可靠，而且集中式的处理方法使得 CR 用户与融合中心之间需要传输大量的数据，增加通信网络的负担。为了减少数据传输量、节省网络资源，防御 SSDF 攻击的分布式协作频谱感知受到越来越多研究者的关注。文献[16]提出了基于最大差值的协作频谱感知(Largest Deviation-based distributed Cooperative Spectrum Sensing，LDCSS)算法，该算法通过比较 CR 用户与其邻居用户的感知值，利用最大差值原则来排除恶意用户。但是，该算法需要大量的网络先验知识，具有较大的不稳定性和局限性。文献[17]提出了基于中位数的分布式协作频谱感知算法，CR 用户收集邻居用户的感知数据后，选取与其邻居间感知数据差值的中位数作为迭代依据，降低了恶意用户的感知数据对本地判决的影响。上述识别恶意用户的方法过于简单，当恶意用户数量较多时，不准确的中位数会导致错误的频谱感知结果。

依靠一次频谱感知信息来识别恶意用户常常会导致误判。文献[18]提出了基于信誉模型[19]和可靠用户的协作频谱感知方法(Reputation-based Cooperative Spectrum Sensing，RBCSS)，当邻居用户的感知结果和 CR 用户的最终本地结果一致时，其信誉值增加，结果不一致时其信誉值减少，若邻居用户的信誉值低于预设的阈值，则将其判别为恶意用户。混乱型攻击下，上述简单的信誉模型无法反映出 CR 用户可靠性的变化，因此根据混乱型攻击的特点建立新的信誉模型是分布式协作频谱感知进行本地融合判决的重要研究问题之一。文献[20]提出了基于机器学习的协作感知信誉机制，鼓励用户发送可靠信息，使发送诚实信息的用户信誉值增加，但该方法没有对恶意用户以信誉值加以惩罚，导致恶意用户可以先伪装成诚实用户以增加信誉值，当信誉值高于阈值时再发动攻击，从而给网络带来极大的损害。

传统 SSDF 攻击模式下攻击强度为常数，本文提出了攻击强度动态变化的动态 SSDF 攻击模式，针对这种攻击模式设计基于能量分类器的抗 SSDF 攻击协作频谱感知算法(Energy Classifier-enabled Cooperative Spectrum Sensing，ECCSS)。在初始阶段，通过能量分类器将邻居节点发送的能量值结合距离判别的方式进行分类，以初步识别出恶意用户的攻击；在融合阶段，CR 用户在时间窗内根据能量分类结果更新邻居节点的信誉值，以当前信誉值作为权重因子结合历史信誉值实施加权协作频谱感知，获得最终的判决结果。仿真结果表明，相比 LDCSS 算法与 RBCSS 算法，本文方案能够有效抗御恶意用户的动态 SSDF 攻击，大大提高了频谱检测性能。

本文第 2 节深入分析动态 SSDF 攻击发动的过程与特征；第 3 节针对动态 SSDF 攻击模型提出基于能量分类器的抗 SSDF 攻击协作频谱感知算法，包括基于距离判别的能量分类器和时间窗下的信誉机制；第 4 节通过仿真实验对该算法进行性能分析与评价；最后总结全文。

2 动态 SSDF 攻击模型

假设 CR 网络中存在着一个 PU，I 个 CR 用户和 U 个恶意用户，其中 CR 用户和恶意用户随机分布在 PU 周围，分布式网络结构如图 1 所示。假设在一个感知周期内网络拓扑结构保持不变，当 CR 用户之间的距离大于有效通信距离时，则互不为邻居用户。首先每一个次用户(Secondary User，SU)进行本地频谱感知，获得本地感知能量值；然后 SU 与其一跳可达的邻居用户进行数据交互以获得最终判决结果。

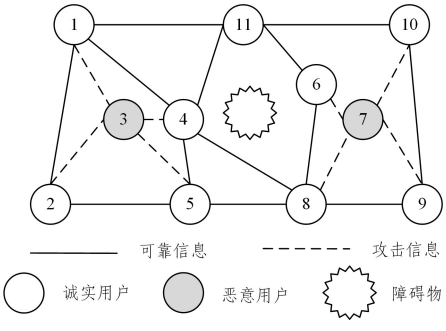


图 1 分布式 CRN 拓扑结构

Fig. 1 Distributed CRN topology

2.1 能量检测法

传统的能量检测法中，CR 用户通过对 PU 信号进行频谱检测来判断 PU 是否存在。这一过程可以描述为：

$$y(t)=\begin{cases}n(t), & H_0\\ h(t)\cdot s(t)+n(t), & H_1\end{cases} \tag{1}$$

其中，$y(t)$代表 CR 用户的接收信号，$s(t)$表示 PU 信号，$n(t)$表示均值为 0、方差为 σ^2 的加性高斯白噪声。$s(t)$与 $n(t)$是实信号且相互独立。$h(t)$为 PU 与 SU 之间进行信号传输的信道增益。H_0 代表 PU 不存在即频段空闲，H_1 代表 PU 信号存在并占用频段。

假设 CR 用户的采样样本总数为 N，则第 n 时刻其能量值 $Y(n)$为：

$$Y(n)=\frac{1}{N}\cdot\sum_{i=1}^{N}|y(i)|^2 \tag{2}$$

由中心极限定理，当 N 足够大($N\geqslant 50$)时，$Y(n)$近似服从高斯分布：

$$\begin{cases}H_0: Y(n)\sim N(\sigma^2, 2\sigma^2/N)\\ H_1: Y(n)\sim N((1+\gamma)\cdot\sigma^2, 2\sigma^4\cdot(2\gamma+1)/N)\end{cases} \tag{3}$$

其中，γ 代表接收信噪比。根据式(3)，CR 用户的本地检测概率 p_d 和本地虚警概率 p_f 为：

$$p_d=\Pr(Y\geqslant\lambda/H_1)=Q\left(\left(\frac{\lambda}{\sigma^2}-\gamma-1\right)\cdot\sqrt{\frac{N}{4\gamma+2}}\right) \tag{4}$$

$$p_f=\Pr(Y\geqslant\lambda/H_0)=Q\left(\left(\frac{\lambda}{\sigma^2}-1\right)\cdot\sqrt{\frac{N}{2}}\right) \tag{5}$$

其中，λ 是本地判决门限，$Q(x)=\frac{1}{\sqrt{2\pi}}\cdot\int_x^{\infty}e^{-t^2/2}dt$ 为互补误差函数。采用纽曼皮尔逊准则，由式(5)可以求解如下的判决门限：

$$\lambda=(Q^{-1}(p_f)\cdot\sqrt{N/2}+1)\cdot\sigma^2 \tag{6}$$

如果 CR 用户检测到的能量值大于系统阈值 λ，则表示信道被 PU 占用；反之，能量值小于阈值 λ，则表示信道处于空闲状态。

2.2 攻击过程

恶意用户通过篡改本地能量值来扰乱诚实用户的频谱判决，以实施恶意攻击。为了更好地躲避探测，恶意用户发起动态随机攻击。假设恶意用户的攻击强度为 Δ（偏离本地感知能量值），则恶意用户以概率 P_{SD} 发起攻击强度为 $\pm\Delta$ 的 SSDF 攻击。传统的随机攻击中 Δ 为常数值，诚实用户通过学习历史能量值能够很容易识别出此攻击强度；而新型的动态 SSDF 攻击由于 Δ 动态变化而不易被诚实用户识别，攻击能力得到增强。

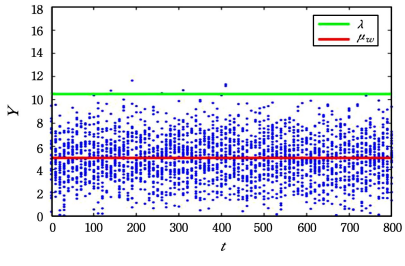
恶意用户在发动 SSDF 攻击前，需要分析 CR 用户接收信号能量值的一般分布特性，以模仿诚实用户行为，躲避识别。本文通过 30 个 CR 用户对同一个 PU 状态在 80 个时隙下分别进行 80 轮频谱感知，以获取接收信号能量值的分布情况，如图 2 所示。由图 2(a)可知：信道噪声能量值分布在阈值 λ 下方且近似高斯分布，主要集中在均值 μ_w 附近。假设恶意用户的实际能量值为 $Y(<\lambda)$，它将能量值篡改为：

$$Y+\Delta=Y+(\lambda-Y+\alpha\lambda) \tag{7}$$

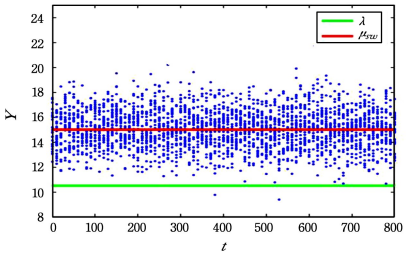
其中，攻击强度 $\Delta=\lambda-Y+\alpha\lambda$，$\alpha\in(0,1)$为比例系数。当攻击强度 Δ 较大或较小时，传统的均值或中位数方法能够非常容易地分辨出异常值，剔除恶意用户的能量值；但若攻击强度 Δ 使得篡改的能量值接近判别阈值，则诚实用户很难用传统方法排除恶意用户攻击。类似地，图 2(b)显示了 PU 占用信道时接收信号的能量值分布在阈值 λ 上方且近似高斯分布，主要集中在均值 μ_{sw} 的附近。恶意用户通过将能量值篡改为

$$Y-\Delta=Y-(Y-\lambda+\alpha\lambda) \tag{8}$$

来发起 SSDF 攻击，其中 $Y>\lambda$。针对这种新型攻击，需要设计恶意节点探测机制，以保证分布式协作频谱感知的可靠性。



(a) H_0 状态



(b) H_1 状态

图 2 CR 用户接收信号的能量值分布

Fig. 2 Energy distribution of CR users received signal

3 抗 SSDF 攻击协作频谱感知算法

本节将 $c_{i,j}$ 定义为与 c_i 相邻的第 j 个节点，$y_{i,j}$ 为 $c_{i,j}$ 的能量值，$r_{i,j}$ 为 $c_{i,j}$ 的信誉值。

图 3 给出了 ECCSS 算法执行框架。$c_{i,j}$ 将能量值 $y_{i,j}$ 传送至能量分类器，将分类结果与本地分类结果比较，并在时间窗内迭代更新，以此计算分类后各邻居节点的信誉值 $r_{i,j}$。最后，本文算法以信誉值作为权重因子进行加权协作频谱感知，获得最终的判决结果 z。

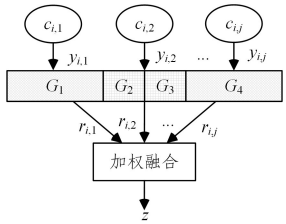


图 3 ECCSS 算法框架

Fig. 3 ECCSS algorithm framework

3.1 基于距离判别的能量分类器

根据图 2 中动态 SSDF 攻击的特点，本文设计了基于距离判别的能量分类器，并将之嵌入抗 SSDF 攻击的协作频谱感知框架。具体地，能量分类器有 4 个子类$\{G_1, G_2, G_3, G_4\}$，其对应的能量值区间分别为：

$$\begin{cases} G_1 \in (0,(1-\lambda)\cdot\alpha) \\ G_2 \in ((1-\lambda)\cdot\alpha,\lambda) \\ G_3 \in (\lambda,(1+\lambda)\cdot\alpha) \\ G_4 \in ((1+\lambda)\cdot\alpha,+\infty) \end{cases} \tag{9}$$

其中，G_1，G_2 子类的状态为 H_0；G_3，G_4 子类的状态为 H_1。G_1 子类的节点经过恶意篡改被误判为 G_3 子类的节点，从而判断该节点状态为 H_1；反之，G_3 子类的节点经过恶意篡改被误判为 G_1 子类的节点，从而判断该节点状态为 H_0；同理 G_2，G_4 子类的节点状态也因恶意篡改而混乱，如图 4 所示。

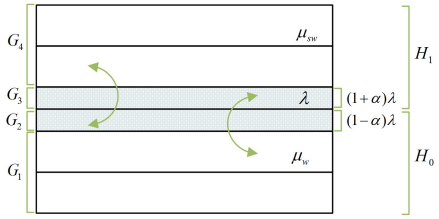


图 4 能量分类器

Fig. 4 Energy classifier

针对图 1 分布式协作频谱感知的网络拓扑，假设第 i 个节点 c_i 接收到 J 个邻居节点传送的感知能量值。为了更好地利用这些感知信息进行协作频谱判决，c_i 不仅需要识别恶意用户偏差较小的攻击能量值，而且需要去除受到阴影衰落等外部环境因素影响而偏差较大的能量值，因此首先对接收信息进行预处理。根据误差理论，c_i 由筛选准则将能量值

$$Y_{i,j} \in \left(0,\frac{1}{2\,\overline{Y}_i}\right) \cup \left(\frac{3}{2\,\overline{Y}_i},+\infty\right), j \in \{1,\cdots,J\} \tag{10}$$

删除，以减少极端感知信息的影响。其中，$\overline{Y}_i$ 为各节点感知值的均值。接着，c_i 将预处理后的邻居节点的能量值输入能量分类器（见图 4），以识别恶意用户的攻击能量值。例如：第 j 个邻居节点 $c_{i,j}$ 的能量值 $Y_{i,j} \in G_3 \in (\lambda,(1+\lambda)\cdot\alpha)$，而大部分邻居节点的能量值属于 $G_1 \in (-\infty,\lambda)$，则可以认为 $c_{i,j}$ 大概率是恶意用户。

上述恶意用户识别方法简单易行，但是频谱检测效率低。通常，PU 占用或不占用信道的状态会持续一段时间，同时恶意用户常在一段时间内持续发动攻击，因此根据时间相关性可以进行长周期的协作频谱感知，即 c_i 将邻居节点的多个感知能量值合并成向量，并将其输入能量分类器测量其与 4 个子类的马氏距离，然后由分类后的感知信息进行一次频谱判决，给出长周期内的信道状态。为此，需要给出能量分类器中各子类的统计特性。假设在感知时间 (T_l,T_{l+1}) 内各节点进行了 S 次频谱感知，则邻居节点 $c_{i,j}$ 的多个能量值形成的向量为 $\hat{Y}_{i,j}=(Y_{i,j,1},\cdots,Y_{i,j,S})$，其中 $Y_{i,j,s}(s\in\{1,\cdots,S\})$ 服从正态分布。于是，$\hat{Y}_{i,j}$ 可作为 S 维高斯随机变量。据此，图 4 中能量分类器的 4 个子类的统计特性均可看作 S 维高斯随机变量，其分布分别满足：

$$\begin{cases} H_0: G_r^0 \sim N(\mu_r^0,\Sigma_r^0), & r=1,2 \\ H_1: G_r^1 \sim N(\mu_r^1,\Sigma_r^1), & r=3,4 \end{cases} \tag{11}$$

其中，$\mu_1^0=(\sigma^2,\cdots,\sigma^2)$，$\Sigma_1^0=\mathrm{diag}(2\sigma^4/N,\cdots,2\sigma^4/N)$，$\mu_2^0=(\lambda+(1+\alpha)\cdot\lambda/2,\cdots,\lambda+(1+\alpha)\cdot\lambda/2)$，$\Sigma_2^0=\mathrm{diag}((1+\alpha)\cdot\lambda/2,\cdots,(1+\alpha)\cdot\lambda/2)$，$\mu_3^1=(\lambda-(1-\alpha)\cdot\lambda/2,\cdots,\lambda-(1-\alpha)\cdot\lambda/2)$，$\Sigma_3^1=\mathrm{diag}((1-\alpha)\cdot\lambda/2,\cdots,(1-\alpha)\cdot\lambda/2)$，$\mu_4^1=((1+\gamma)\cdot\sigma^2,\cdots,(1+\gamma)\cdot\sigma^2)$，$\Sigma_4^1=\mathrm{diag}(2\sigma^4\cdot(2\gamma+1)/N,\cdots,2\sigma^4\cdot(2\gamma+1)/N)$。

当 c_i 接收到邻居节点 $c_{i,j}$ 的能量向量 $\overset{\wedge}{\boldsymbol{Y}}_{i,j}$ 后，根据式(12)分别计算它与 4 个子类之间的马氏平方距离：

$$d_r^2(\overset{\wedge}{\boldsymbol{Y}}_{i,j},G_r)=(\overset{\wedge}{\boldsymbol{Y}}_{i,j}-\mu_r^v)\cdot\sum_r^{-1}(\overset{\wedge}{\boldsymbol{Y}}_{i,j}-\mu_r^v)^{\mathrm{T}} \tag{12}$$

其中，$v\in\{0,1\}$。比较 4 个马氏平方距离得到能量分组为：

$$r^*=\arg\min_{1\leqslant r\leqslant 4} d_r^2(\overset{\wedge}{\boldsymbol{Y}}_{i,j},G_r) \tag{13}$$

则 $\overset{\wedge}{\boldsymbol{Y}}_{i,j}\in G_{r^*}$。在 H_0 下，若 $\overset{\wedge}{\boldsymbol{Y}}_{i,j}\in G_2$，则邻居节点 $c_{i,j}$ 大概率发动了 SSDF 攻击；反之，在 H_1 下，若 $\boldsymbol{Y}_{i,j}\in G_3$，则邻居节点 $c_{i,j}$ 大概率发动了 SSDF 攻击。

3.2 时间窗下的信誉机制

传统的信誉模型利用当前的判决结果来更新节点的信誉值，没有考虑历史判决结果对当前信誉值的影响，因此难以快速地对动态 SSDF 攻击做出反应。为此，本文在滑动时间窗内建立新的信誉机制来确定 CR 用户的可靠性。

假设滑动时间窗被分成 K 个时隙，每个时隙 I_k 对应一次频谱判决，其状态定义为：

$$I_k=\begin{cases} 0, & \text{本地分类结果一致} \\ 1, & \text{与本地分类结果不一致} \end{cases} \tag{14}$$

各节点通过图 4 的能量分类器将分类结果与本地分类结果进行对比。根据滑动时间窗下的信誉机制（见图 5），将动态 SSDF 攻击的特点归纳如下：

(1)恶意节点两次判决为 1 之间的时隙数小于诚实用户；

(2)当前时隙判决为 1，且与上一次判决为 1 之间的时隙数越小，则该 CR 用户是恶意用户的可能性就越大，因此其信誉值应大幅减少；

(3)滑动窗口内判决为 1 的时隙数越多，则该 CR 用户是恶意用户的可能性就越大，因此其信誉值应大幅减少。

针对上述特性，定义 $d_j(j\in\{1,\cdots,k\})$ 是当前时隙判决为 1 与前面判决为 1 的第 j 个时隙之间的时隙个数（例如，d_5 是 I_1 与 I_6 之间的时隙个数）。显然，d_j 反映了历史判决错误与当前判决错误之间的距离，此距离越小，说明 CR 用户错误判决的频率越高，此节点是恶意用户的可能性越大，其信誉值应按比例减少；反之，CR 用户应为诚实节点，其信誉值应增加。本文设计了式(15)的信誉值更新强度，这种更新强度是通过在时间窗内累加 d_j 对信誉值的影响获得的。

$$\delta=\begin{cases} 1, & \sum_{k=1}^{T} I_k=0 \\ \sum_{j=1}^{k}\beta\times\{1-\sin(\frac{\pi}{2T_0}d_j)\}, & \sum_{k=1}^{T} I_k\geqslant 1 \end{cases} \tag{15}$$

其中，β 为惩罚因子，令 $\beta=-1$。从 $\sin(\frac{\pi}{2T_0}d_j)$ 可知，d_j 越小，则信誉值变化越大，即历史判决对当前判决产生的影响越大。

信誉值更新的具体步骤如下：对于 c_i 的本地判决结果 u_i，若邻居节点 $c_{i,j}$ 上报的判决结果 $u_{i,j}=u_i$，则对其信誉值加 1；反之，当 $u_{i,j}\neq u_i$ 时，c_i 更新此邻居节点的信誉值为：

$$r_{i,j}\leftarrow r_{i,j}+\delta_{i,j} \tag{16}$$

信誉值越高，表示其邻居节点的可靠性越高。

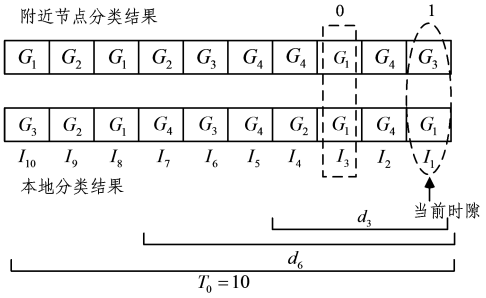


图 5 滑动时间窗下的信誉机制

Fig. 5 Reputation mechanism under sliding time window

3.3 加权协作频谱感知方法

c_i 根据前一轮协作频谱感知的结果为每个邻居节点更新信誉值，并将其作为当前一轮协作频谱感知的权重值。权重值计算方法如下：

$$w_{i,j}=\frac{r_{i,j}}{\sum_{j=1}^{N} r_{i,j}},j\in\{1,\cdots,N\} \tag{17}$$

然后 c_i 进行线性加权融合，计算出能量值：

$$z=\sum_{j=1}^{N} w_{i,j}\cdot Y_{i,j} \tag{18}$$

其中，$Y_{i,j}$ 表示 c_i 的第 j 个邻居节点的能量值。由式(18)可知：高信誉值的邻居节点具有更大的权重，对协作频谱感知的贡献更大，从而使得当地判决结果更准确。

4 实验设计与性能评价

本文在 MATLAB 平台上验证所提算法的有效性，并通过蒙特卡洛(Monte-Carlo)实验对 LDCSS 算法、RBCSS 算法与本文算法的协作频谱感知性能进行仿真分析。

本文算法的核心代码表述如算法 1 所示。

算法 1 基于能量分类器的抗 SSDF 攻击协作频谱感知算法

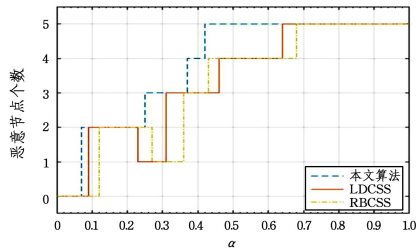
输入：N，λ，$y_i(t)$，$y_{i,j}(t)$

输出：z

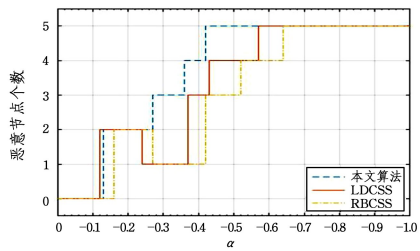
1. initialize：Set $y_i(t)=\sin(t)$
2. for i=1,2,…,N,j=1,2,…,N−1 do
3. Set Y_i，$Y_{i,j}$ by Eq. (2)
4. $\overline{Y}_i\leftarrow\frac{\sum_{i=1}^{N} Y_i}{N}$
5. while $\frac{1}{2\overline{Y}_i}\leqslant Y_{i,j}\leqslant\frac{3}{2\overline{Y}_i}$ do
6. Set r_i^*，$r_{i,j}^*$ by Eq. (9)
7. if $r_{i,j}^*=r_i^*$ then
8. $I_{i,j}\leftarrow 0$
9. else
10. $I_{i,j}\leftarrow 1$
11. end if
12. Set $\delta_{i,j}$ by Eq. (15)
13. $r_{i,j}\leftarrow r_{i,j}+\delta_{i,j}$
14. Set z by Eq. (17)，(18)
15. end while
16. end for
17. return z

4.1 攻击强度对性能检测的影响

为了验证本文算法识别恶意用户的能力，设计系统拓扑结构(见图 1)。假设系统中随机分布着 10 个 CR 用户，其中 2，4，6，8，10 号 5 个节点为恶意用户，这些节点通过动态地改变攻击强度的比例系数 α 来改变攻击强度。在 H_0 情况下，α 可以从 0 改变到 1；在 H_1 情况下，α 可以从 0 改变到 −1。假设 PU 发射的信号为 $s(k)=1$ 的 BPSK 信号，占用频段的概率为 0.5，PU 信号通过 AWGN 信道传输，CR 用户之间为理想信道。在仿真过程中，假设各个判决结果相互独立。系统设定 CR 用户的虚警概率为 0.1。下面通过 500 次蒙特卡洛实验对本文提出的算法、文献[16]的 LDCSS 算法以及文献[18]的 RBCSS 算法的检测性能进行仿真分析。图 6 展示了攻击强度变化时本文算法、RBCSS 算法与 LDCSS 算法检测到网络中的恶意用户个数的情况。在 H_0 情况下，当 α 达到 0.42 时，本文算法就能识别出所有恶意用户，而当 α 逐渐增大到 0.64 时，LDCSS 算法才能识别出所有恶意用户，当 α 逐渐增大到 0.68 时，RBCSS 算法才能识别出所有恶意用户。在 H_1 情况下，当 α 达到 0.42 时，本文算法就能识别出所有恶意用户，而当 α 逐渐增大到 0.57 时，LDCSS 算法才能识别出所有恶意用户，当 α 逐渐增大到 0.64 时，RBCSS 算法才能识别出所有恶意用户。因此本文算法的检测性能大大提高。同时可见，当 $\alpha=0.2$，$\Delta\approx\lambda$ 时，LDCSS 算法和 RBCSS 算法很难排除恶意用户攻击，导致协作频谱检测性能下降，而本文算法克服了传统方法的不足，在 $\Delta\approx\lambda$ 时能有效地识别出恶意用户，大大提高了协作频谱检测精度。



(a) H_0 状态



(b) H_1 状态

图 6 不同攻击强度下识别恶意用户的个数

Fig. 6 Number of malicious users under different attack powers

4.2 检测性能与鲁棒性分析

本节通过 1 000 次蒙特卡洛实验对本文算法、LDCSS 算法以及 RBCSS 算法的感知性能进行仿真分析。针对仅设置图 1 中节点 3 为恶意节点的情况和设置图 1 中节点 3 和节点 7 均为恶意节点的情况，图 7 给出了 ROC 性能曲线。设置攻击强度的比例系数 $\alpha=0.2$，假设 PU 发射的信号为 $s(k)=1$ 的 BPSK 信号，占用频段的概率为 0.5，PU 信号通过 AWGN

信道传输，CR 用户之间为理想信道。在仿真过程中，假设各个判决结果相互独立。由图 7 可见，面对动态 SSDF 攻击，本文算法的检测性能远远优于 LDCSS 算法和 RBCSS 算法。例如 $p_f=0.1$ 时，单个恶意用户攻击时采用本文算法、LDCSS 算法、RBCSS 算法得到的 p_d 分别为 71%，56%，5%；在两个恶意用户攻击时得到的 p_d 分别为 59%，43%，37%。可见，本文算法的检测性能优于 LDCSS 算法和 RBCSS 算法。这是因为当攻击强度接近阈值时，LDCSS 算法和 RBCSS 算法不易识别出恶意用户的动态攻击，而本文算法依据动态 SSDF 攻击的特征，使用能量分类器判断出邻居节点的恶意攻击，再依据能量值偏离程度设定各诚实邻居节点的实时信誉度，有效降低了动态 SSDF 攻击对协作频谱感知的影响，大大改善了协作检测精度。

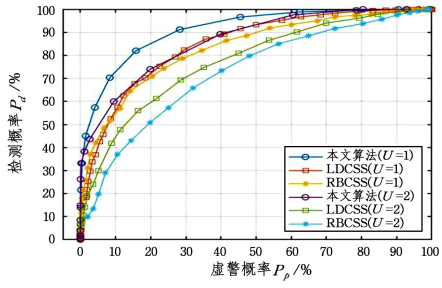


图 7 SSDF 攻击时的 ROC 性能曲线

Fig. 7 ROC under SSDF attack

另外，比较图 7 中一个恶意节点和两个恶意节点下的 ROC 曲线可知，相较于 LDCSS 算法和 RBCSS 算法，本文算法受恶意用户数目增多的影响较小，具有更强的鲁棒性。

为进一步比较恶意用户数目增多对 3 种算法的影响，图 8 给出了不同数量恶意节点下 3 种算法检测性能的对比。仿真中，恶意用户以等概率发起动态 SSDF 攻击。假设系统中随机分布着 30 个 CR 用户参与本地感知，其中恶意用户的数量从 0 变化到 15，其余节点为诚实用户。假设 PU 发射的信号为 $s(k)=1$ 的 BPSK 信号，占用频段的概率为 0.5，PU 信号通过 AWGN 信道传输，CR 用户之间为理想信道。在仿真过程中，假设各个判决结果相互独立。系统设定认知用户的虚警概率分别为 0.1 和 0.3，漏检概率为 0.15，$\alpha=0.2$，其余用户初始值为 0。采用蒙特卡洛仿真法进行 1 000 次实验。

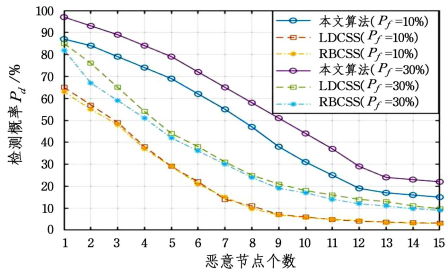


图 8 不同数量的恶意节点攻击时的检测概率

Fig. 8 Detection probability with varying malicious node attacks

由图 8 可见，3 种算法的检测性能均随着恶意节点数目的增多而降低，但本文算法检测性能降低的速度小于 LDCSS 算法和 RBCSS 算法，并且在恶意用户数量相等的条件下，本文算法的检测性能均明显优于 LDCSS 算法和 RBCSS 算法。这是因为本文算法考虑到攻击强度的动态性，在滑动时间窗下建立了信誉模型，依靠历史感知结果进行频谱判决，优化了传统方法仅依靠当前感知结果进行频谱判决存在的不足，增强了算法的鲁棒性。

结束语 针对协作频谱感知中动态 SSDF 攻击的特点，本文提出了一种新型的基于能量分类器的抗 SSDF 攻击模型以提高协作判决的性能。首先，CR 用户通过能量分类器对各邻居节点的能量值进行分类，以识别出恶意用户的 SSDF 攻击；然后，CR 用户根据能量分类结果更新各邻居节点的信誉值，以当前信誉值作为权重因子实施加权协作频谱感知，获得高精度、高效率的本地判决结果。仿真结果显示，对比传统的抗 SSDF 攻击方法，相较于 LDCSS 算法和 RBCSS 算法，本文算法在恶意节点的干扰下检测概率分别提高了 15% 和 16%，且本文算法受恶意用户数目增多的影响较小，具有更高的频谱检测准确率和较强的鲁棒性。本文深入研究了基于能量分类器的抗 SSDF 攻击协作频谱感知算法，但仍有很多研究工作有待完善。本文研究的基于能量分类器的抗 SSDF 攻击协作频谱感知算法在恶意用户已探知到抗御方法并采用了更加灵活的攻击策略的情况下，无法实现较高的检测概率。下一步将研究如何在攻击模式不断改变的情况下得到比较高的频谱感知检测概率，并尽可能将算法开销降到最低。

参 考 文 献

[1] SASABE M, NISHIDA T, KASAHARA S. Collaborative spectrum sensing mechanism based on user incentive in cognitive radio networks[J]. Computer Communications, 2019, 147(8): 1-13.

[2] SHRIVASTAVA S, RAJESH A, BORA P K. Defense against primary user emulation attacks from the secondary user throughput perspective[J]. AEU-International Journal of Electronics and Communications, 2018, 84(2): 131-143.

[3] SHARMA G, SHARMA R. Performance comparison of hard and soft fusion Techniques for Energy Efficient CSS in Cognitive Radio[C]// 2018 International Conference on Advanced Computation and Telecommunication (ICACAT). IEEE, 2018: 1-4.

[4] SEO D, NAM H. A Parallel Multi-Channel Cooperative Spectrum Sensing in Cognitive Radio Networks[C]// 2018 International Symposium on Antennas and Propagation (ISAP). IEEE, 2018: 1-2.

[5] DU R, ZHOU Y, LIU F, et al. An effective collaborative spectrum sensing method against SSDF attack[C]// 2017 29th Chinese Control and Decision Conference (CCDC). IEEE, 2017: 5698-5702.

[6] DAS D, DAS S. An intelligent resource management scheme for SDF-based cooperative spectrum sensing in the presence of primary user emulation attack[J]. Computers & Electrical Engineering, 2018, 69(7): 555-571.

[7] ZHANG L, DING G, WU Q, et al. Byzantine attack and defense in cognitive radio networks: A survey[J]. IEEE Communications Surveys & Tutorials, 2015, 17(3): 1342-1363.

[8] PENG T, CHEN Y, XIAO J, et al. Improved soft fusion-based cooperative spectrum sensing defense against SSDF attacks

[C]// 2016 International Conference on Computer, Information and Telecommunication Systems (CITS). IEEE, 2016: 1-5.

[9] ESLAMI A, KARAMZADEH S. Performance analysis of double threshold energy detection-based spectrum sensing in low SNRs over Nakagami-m fading channels with noise uncertainty[C]// 2016 24th Signal Processing and Communication Application Conference (SIU). IEEE, 2016: 309-312.

[10] LI L, LI F, ZHU J. A method to defense against cooperative SSDF attacks in Cognitive Radio Networks[C]// 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013). IEEE, 2013: 1-6.

[11] SUN Z, XU Z, HAMMAD M Z. Defending Against Massive SSDF Attacks from a Novel Perspective of Honest Secondary Users[J]. IEEE Communications Letters, 2019, 23(10): 1696-1699.

[12] AL-MATHEHAJI Y, BOUSSAKTA S, JOHNSTON M, et al. Defeating SSDF attacks with trusted nodes assistance in cognitive radio networks[J]. IEEE Sensors Letters, 2017, 1(4): 1-4.

[13] GHAZNAVI M, JAMSHIDI A. A low complexity cluster based data fusion to defense against SSDF attack in cognitive radio networks[J]. Computer Communications, 2019, 138(4): 106-114.

[14] YUE W J, ZHENG B Y, MENG Q M, et al. Robust cooperative spectrum sensing schemes for fading channels in cognitive radio networks[J]. Science China Information Sciences, 2011, 54(2): 348-359.

[15] GUL N, QURESHI I M, NAVEED A, et al. Secured Soft Combination Schemes Against Malicious-Users in Cooperative Spectrum Sensing[J]. Wireless Personal Communications, 2019: 1-20.

[16] TANG H, YU F R, HUANG M, et al. Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks[J]. IET communications, 2012, 6(8): 974-983.

[17] HUANG Q D, SUN Q, YAN Q Q. Communication spectrum sensing scheme based on median anti-SSDF attack[J]. Journal of Xi'an University of Posts and Telecommunications, 2017, 22(2): 12-17.

[18] ZENG K, PAWELCZAK P, CABRIC D. Reputation-based cooperative spectrum sensing with trusted nodes assistance[J]. IEEE Communications Letters, 2010, 14(3): 226-228.

[19] LI F W, LIU F, ZHU J, et al. Reputation-based secure spectrum situation fusion in distributed cognitive radio networks[J]. The Journal of China Universities of Posts and Telecommunications, 2015, 22(3): 110-117.

[20] WANG J, CHEN R, TSAI J J P, et al. Trust-based cooperative spectrum sensing against SSDF attacks in distributed cognitive radio networks[C]// 2016 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR 2016). IEEE, 2016: 1-6.

DING Shi-ming, born in 1995, postgraduate. Her main research interests include wireless multimedia sensor network and so on.

SHEN Hang, born in 1984, Ph.D, associate professor, postgraduate supervisor, is a member of China Computer Federation. His main research interests include wireless multimedia sensor network, mobile Internet and wireless multimedia communication protocol.