



协作频谱感知中的动态信任评估机制

王美璎¹, 冯景瑜^{1,2}, 卢光跃¹, 韩定坤¹

(1. 西安邮电大学通信与信息工程学院, 陕西 西安 710121;

2. 中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093)

摘要:针对动态性 SSDF 攻击对协作频谱感知技术的危害性, 实时观察分析认知用户的感知行为, 提出一种动态信任评估机制。根据认知用户的历史感知变化情况, 引入时间衰减因子、加性奖励因子和加性惩罚因子, 计算出随时间和协作次数不断变化的动态信任值, 选取可信认知用户参与协作感知, 提高了数据融合中心的协作判决准确性。仿真结果表明, 动态信任机制可以有效抑制恶意用户的信任值增长, 降低对“OR”、“AND”和“Majority”3 种常用协作频谱感知数据融合准则的攻击成功率。

关键词: 认知无线电; 协作频谱感知; 动态信任; SSDF 攻击

中图分类号: TN929

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016051

A dynamic trust evaluation scheme for cooperative spectrum sensing

WANG Meiyin¹, FENG Jingyu^{1,2}, LU Guangyue¹, HAN Dingkun¹

1. Institute of Communication Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

2. State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China

Abstract: Considering the harmful effect of dynamic SSDF attack against cooperative spectrum sensing technologies, a dynamic trust evaluation scheme based on the real-time observation and analysis of cognitive users' sensing behaviors was proposed. Time attenuation, additive reward and additive penalty factors based on the historical sensing variation of cognitive users were introduced to calculate the dynamic trust value which changes with time and the number of collaborations. Meanwhile, trusted cognitive users were selected to participate in cooperative sensing, and thus improving the accuracy of the final sensing decision. Simulation results show that the scheme can effectively suppress the growth of trust of malicious users, and reduce the attack success rate for “OR”, “AND” and “Majority” which are three kinds of cooperative spectrum sensing data fusion schemes.

Key words: cognitive radio, cooperative spectrum sensing, dynamic trust, SSDF attack

收稿日期: 2015-05-18; 修回日期: 2016-01-06

基金项目: 国家自然科学基金资助项目 (No.61301091); 陕西省自然科学基金资助项目 (No.2014JQ8321, No.2014JM8299); 中国科学院信息安全国家重点实验室开放课题 (No.2015-MS-14)

Foundation Items: The National Natural Science Foundation of China (No.61301091), The National Science Foundation of Shaanxi Province (No.2014JQ8321, No.2014JM8299), The Open Foundation of State Key Laboratory of Information Security (No.2015-MS-14)

1 引言

认知无线电技术^[1]通过认知用户(cognitive user, CU)检测频谱空洞,伺机接入主用户(primary user, PU)暂时不用授权频段的方式,显著提高了频谱利用率,是解决频谱资源短缺的重要技术。协作频谱感知是实现认知无线电技术的关键环节,其感知性能的好坏影响到整个认知无线电的性能。协作感知的特点是多个认知用户共同感知频谱状态,融合中心(fusion center, FC)综合各认知用户的感知结果做出最终判决,这种多用户感知为恶意用户(malicious user, MU)提供了可乘之机。恶意用户会实施频谱感知数据伪造(spectrum sensing data falsification, SSDF)攻击,将伪造的虚假感知数据以认知用户的身份发送给数据融合中心,使融合中心不能做出正确判决,从而损害协作频谱检测性能。

在 SSDF 攻击的抑制方法研究方面,目前研究界倾向于信任评估机制。而信任评估机制适用于协作频谱感知的主要原因在于,凡是涉及分布式协作的行为活动,都会存在信任问题,协作频谱感知正是一种典型的分布式协作活动。参考文献[2]通过将每个认知用户的本地检测结果与融合中心的全局检测结果进行比较,得到各认知用户的频谱检测信任值,选择可信节点进行融合判决,以此提高协作频谱感知性能。参考文献[3]提出一种基于贝叶斯信任加权的可信序贯概率比检测算法,对抗恶意用户的间歇性 SSDF 攻击行为。参考文献[4]基于 D-S 证据理论的信任评估机制,通过保护硬判决融合算法,可以有效抑制 SSDF 攻击。参考文献[5]通过模糊逻辑理论建立认知用户的信任机制,减轻 SSDF 攻击带来的感知性能下降。参考文献[6]利用认知循环建立信任模型,保障协作频谱感知的安全性。参考文献[7]考虑将虚假感知次数作为信任值的衰减因子,用以惩罚恶意用户,但忽略了动态性 SSDF 攻击的间歇性特征。引入信任评估机制后,融合中心计算认知用户的信任值,作为衡量各认知用户感知能力优劣的标准,区别对待不同用户的检测结果,选择信任值高的认知用户的感知数据进行融合,在一定程度上对抗了 SSDF 攻击,提高了系统的整体检测性能。但这些算法没有考虑到恶意用户更为复杂的攻击形式,如果恶意用户只是单纯地提交影响 FC 判决的虚假感知数据,其信任度会持续下降,很容易就会被融合中心识别。然而,恶意用户如果交替地提交诚实感知数据和虚假感知数据,若其在

恶意状态中没有被及时移除,则在下一次协作感知中恶意用户会继续累积信任值,从而一直处于高信任度状态。具有这种攻击行为的恶意用户,能一直伪装为正常认知用户,持续不断地实施攻击,对协作频谱感知性能造成严重危害。

本文综合考虑时间因素和认知用户的动态感知行为对信任值的影响,引入信任值的时间衰减和对认知用户的奖惩机制,优化信任值的评估方法,提出一种动态的信任评估机制,实时更新信任值,在恶意用户进行虚假感知时信任值很快低于阈值,被融合中心剔除,使其不再有机会通过正确感知重新获得高信任值来伪装诚实认知用户。同时,借鉴切尾平均数法^[8],去掉影响认知用户稳定信任值的极端信任值,削弱偶然性因素对信任值的影响,使信任值的估计具有更高的稳健性,以此抵制恶意用户的动态性 SSDF 攻击。

2 协作频谱感知及其安全威胁

协作频谱感知融合多个认知用户的频谱感知结果,解决了单个认知用户频谱感知的不确定性问题^[9],可以显著提高频谱感知的性能。分布式数据融合结构传输的数据量少^[10],对数据可以高效处理和响应,适用于认知无线电的应用环境。基于分布式数据融合结构的协作频谱感知模型如图 1 所示。

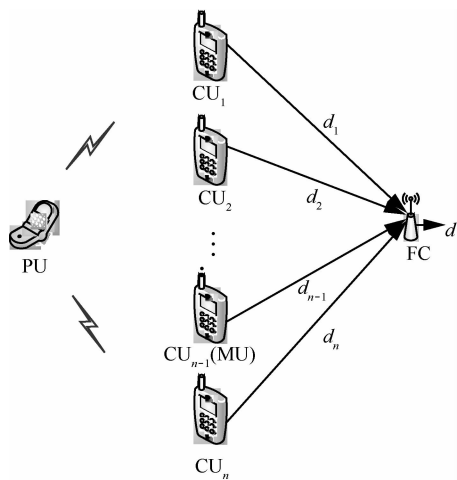


图 1 协作频谱感知系统模型

图 1 中,有一个主用户和 n 个认知用户的单信道网络, n 个认知用户相互独立地均匀分布在融合中心周围。协作感知可分为 3 个连续的部分执行:初始检测、数据汇合和融合判决。



- 初始检测:每个认知用户作为本地感知终端独立接收来自授权用户的信号,利用本地频谱检测算法对主用户信号进行检测。
- 数据汇合:各认知用户将初始检测得到的初始检测结果汇报给数据融合中心。
- 融合判决:FC采用合适的数据融合算法,综合各认知用户的初始检测数据,做出主用户频谱是否可用的最终频谱感知决策。

各CU将各自的初始检测结果 d_i 发送到融合中心,FC利用这些感知数据得到最终判决结果 d 并告知各CU。判决结果中“0”状态表示PU信号不存在,“1”状态表示PU信号存在^[10],融合中心利用“OR”、“AND”和“Majority”数据融合准则^[12]进行最终的融合判决。

- “OR”融合准则:当有一个 CU_i 的初始检测结果 $d_i=1$ 时,融合中心便做出 $d=1$ 的最终判决。其优点在于可最大化保护主用户免受认知用户由于漏检而造成的有害干扰。
- “AND”融合准则:当所有 CU_i 的初始检测结果 $d_i=1$ 时,融合中心才做出 $d=1$ 的最终判决。与“OR”数据融合准则相反,其注重资源利用率的最大化,即虚警概率的最小化。
- “Majority”融合准则:至少一半 CU_i 的检测结果 $d_i=1$ 时,融合中心做出最终判决结果 $d=1$ 的判决。

这些传统的协作频谱感知数据融合准则不加选择地使用所有认知用户的感知结果,缺乏对初始感知数据安全性的考虑,某些CU可能被敌方控制成为MU,它们通过篡改初始感知结果而实施SSDF攻击。如图1中的第 $n-1$ 个认知用户为恶意用户,它故意发送虚假感知结果 d_{n-1} 给FC,以扰乱融合判决。按发送虚假数据的不同,SSDF攻击分为全“0”攻击和全“1”攻击^[13]。

- 全“0”攻击:恶意用户始终发送PU不存在的感知数据给FC,使其他用户误认为主用户的频谱资源一直处于“空闲”状态而接入频谱,对主用户使用频谱造成干扰或干扰其他CU的正常通信。
- 全“1”攻击:恶意用户始终发送PU存在的感知数据给FC,误导其他CU认为频谱一直被占用,从而长期占用大量空闲频谱资源。

3 协作频谱感知的动态信任保护

信任是主体对客体能否正确地、非破坏性地完成某项

协作活动的主观可能性预测^[14]。历史感知行为反映认知用户信任值的变化状况,据此引入贝叶斯信任描述认知用户的基本信任度量,然后在此基础上建立协作频谱感知的动态信任评估机制,抑制恶意用户的动态性SSDF攻击行为,有效规避其带来的安全风险。最后,给出了动态信任评估机制在协作频谱感知环境下保护“OR”、“AND”和“Majority”3种融合准则的实现流程。

3.1 贝叶斯信任值

认知用户历史行为的二元性影响着信任值的评估。提供诚实感知数据的认知用户信任值会增加,而提供虚假感知数据会使认知用户的信任值降低,对于这样的二元事件,预测其下一次产生有利事件的概率,就是一个基于之前行为预测后来行为的后验概率^[15]:

$$P_{\alpha\beta}(x) = P(x|\alpha, \beta) = \frac{P((\alpha, \beta)|x)P(x)}{\sum P((\alpha, \beta)|x)P(x)} \quad (1)$$

其中, α, β 分别表示认知用户在某一次协作感知中诚实感知次数和虚假感知次数。

二项事件后验概率服从Beta分布。已知Beta概率密度函数^[16]的表达式为:

$$Beta(\theta|\alpha, \beta) = \frac{G(\alpha+\beta)}{G(\alpha)G(\beta)} \theta^{\alpha-1} (1-\theta)^{\beta-1} \quad (2)$$

其中, θ 表示感知事件发生的概率, $0 \leq \theta \leq 1, \alpha > 0, \beta > 0$,且当 $\alpha < 1, \theta \neq 0$,当 $\beta < 1, \theta \neq 1$ 。

信任值的概率分布函数可以用贝叶斯推理中的Beta分布描述,可以得到信任值 T_i 的计算式为:

$$T_i = \frac{\alpha_i + 1}{\alpha_i + \beta_i + 2}, T_i \in [0, 1] \quad (3)$$

其中, α_i 和 β_i 分别对应于第 i 个认知用户历史感知的诚实感知次数和虚假感知次数,当 $\alpha_i = \beta_i = 0$ 时, $T_i = 0.5$,由于信任值 $T_i \in [0, 1]$,可设置信任值的阈值 $\lambda = 0.5$ 。当 $T_i > \lambda$ 时, CU_i 处于可信状态; $T_i < \lambda$ 时, CU_i 为不可信。

3.2 动态信任评估

为有效对抗恶意用户的动态性SSDF攻击,考虑信任的动态特性和基于时间的衰减特性,本文引入奖惩因子和时间衰减因子进行动态信任评估。

(1) 奖励因子 $r(k)$

在动态性SSDF攻击中,恶意用户交替提交诚实和虚假感知数据,一般信任机制无法识别这样的攻击行为,恶意用户会一直处于可信状态,对此,引入奖励和惩罚因子,根据认知用户行为特征决定其信任状况,及时对提供虚假

感知的用户的信任值进行衰减,有效防御其动态性攻击,同时,对连续诚实感知的认知用户予以奖励,激励其不断提交诚实感知数据。

假设 CU_i 在 $k-h$ 时刻开始正确感知,且在之后的 $k-h+1, k-h+r, \dots, k$ 时刻连续存在诚实感知,则奖励因子起作用,对其信任度进行修正。设 T_i^k 为 CU_i 在第 k 次感知中的信任值, k 时刻奖励因子 $r(k)$ 的计算方法如下:

$$r(k) = \left| \frac{1}{h} \sum_{l=k-h}^k T_i^l - \max T_i^l \right| \quad (4)$$

其中, h 为连续诚实感知次数,这里 $h > 2$ 。

$r(k)$ 的计算利用 CU_i 的 h 个诚实感知信任值 T_i^l , 这里奖励力度不是持续不变的,而是随累计信任值不断动态调整,针对恶意用户通过连续提供诚实感知数据,在短时间内容积累高信任值进行虚假感知的投机行为, $r(k)$ 的计算中去掉了 CU_i 连续感知的 h 个信任值中最大的信任值 $\max T_i^l$, 减小对诚实感知的奖励力度,感知用户只有持续不断地提交诚实感知数据才能为自身建立一个良好的信任状况,以此激励认知用户积极贡献。

(2) 惩罚因子 $p(k)$

若 CU_i 在 $k-m$ 时刻开始虚假感知,且在之后的 $k-m+1, k-m+r, \dots, k$ 时刻连续存在虚假感知,则惩罚因子起作用,抑制其不良行为。 k 时刻惩罚因子 $p(k)$ 的计算方法如下:

$$p(k) = \left| \frac{1}{m} \sum_{l=k-m}^k T_i^l - \min T_i^l \right| \quad (5)$$

其中, m 为连续虚假感知次数,这里 $m > 2$ 。

与奖励因子相同,惩罚因子的计算去掉了 m 个信任值中的最小值,不仅减弱偶然因素对信任度的影响,而且认知用户会为短期机会主义行为付出很大代价,达到抑制恶意用户不良行为的目的。

(3) 时间衰减因子 $d(k)$

历史感知信息对信任值更新过程有远近效应,近期感知对当前信任值的影响大,远期感知对当前信任值影响小,计算中根据历史感知时间距当前感知时间的远近不同,给予信任值不同的时间权重。该时间权重随着距离当前时间距离的增大而递减。这个时间权重的函数为时间衰减因子。

设认知用户 CU_i 的当前感知时刻为 k , k_h 为 CU_i 最近一次出现诚实感知行为的时刻,则 CU_i 的时间衰减因子 $d(k)$ 可描述为:

$$d(k) = \frac{k - k_h}{k} \quad (6)$$

随着距离当前感知时刻越来越远,即使恶意用户获得高信任度,在它伺机进行攻击的这段时间,信任值也会随时间逐渐衰减;对于长时间没有进行感知的认知用户,衰减因子也会督促用户不断提交正确感知。

(4) 动态信任值

认知用户的动态信任值综合考虑上面3种因素。用 T_i^k 表示 CU_i 在 k 时刻的信任值, $k=0$ 时为 CU_i 初次参与感知的初始信任值,其值设为 θ , θ 为筛选可信协作感知用户的信任值的门限值。则 CU_i 的信任值的具体计算式如下:

$$\begin{cases} T_i^k = \theta, k=0 \\ T_i^k = d(k)T_i^l + a \times p(k) + b \times r(k), k > 0 \end{cases} \quad (7)$$

其中, a 、 b 的确定方法如下:

$$a = \begin{cases} 0, & \text{无虚假感知行为} \\ -1, & \text{存在连续虚假感知} \end{cases} \quad (8)$$

$$b = \begin{cases} 0, & \text{偶尔诚实感知} \\ 1, & \text{存在连续诚实感知} \end{cases} \quad (9)$$

3.3 实现流程

基于动态信任值的协作频谱感知,在融合中心进行数据融合之前,对各参与协作的认知用户建立信任评估机制。针对恶意用户交替提交正确或虚假感知结果的行为,通过设置奖惩因子来控制感知行为对信任值的影响,奖惩因子的计算借鉴切尾平均数法思想,利用认知用户连续诚实感知和虚假感知的信任值进行计算,每次感知的好坏都会反映在信任值中;此外,认知用户的信任值是随着时间不断衰减的,并与历史行为密切联系,以认知用户的贝叶斯信任值为基础,并加入乘性时间衰减因子,信任值每时每刻都在动态更新,及时更新信任值是实时观察认知用户感知行为的具体体现。设置信任门限值,剔除那些信任值低于门限的用户,利用准确性更高的数据进行融合,得到存在动态性 SSDF 攻击时的可靠频谱感知决策。动态信任评估实现流程如图2所示,算法实现步骤如下。

步骤1 初始时刻($k=0$),初始化信任门限值 $\theta=0.5$,此门限值的设定可以根据具体要求设置不同的值,信任值高于此门限值的认知用户为可信认知用户,其本地感知结果参与融合中心的数据融合,信任值低于此门限值的认知用户为不可信认知用户,其本地感知结果不参加融合中心数据融合且该用户被剔除。如果认知用户第一次参加协作感知,其初始信任值 $T_i^k = \theta$,连续诚实感知次数 $h=0$,连续虚假

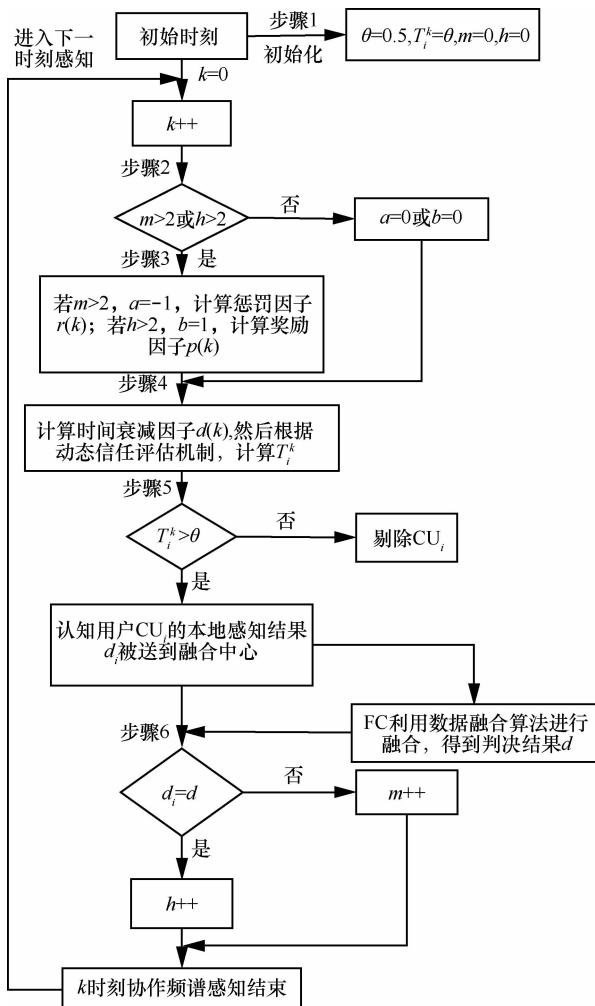


图2 动态信任评估实现流程

感知次数 $m=0$ 。

步骤2 判断连续虚假感知次数 m 和连续诚实感知次数 h 的值是否大于 2, 若 $m>2$, 则 $a=-1$, 惩罚因子起作用; 若 $h>2$, 则 $b=1$, 奖励因子起作用; 否则, $a=0, b=0$, 惩罚和奖励因子都不起作用, 直接执行步骤 4。

步骤3 根据已给出的公式计算奖励因子 $r(k)$ 和惩罚因子 $p(k)$ 。

步骤4 计算时间衰减因子 $d(k)$, 然后根据动态信任评估机制, 计算认知用户 CU_i 的动态信任值 T_i^k 。

步骤5 比较动态信任值与门限值, 若 $T_i^k > \theta$, CU_i 为可信认知用户, 其感知结果 d_i 参与融合中心的融合判决; 若 $T_i^k < \theta$, CU_i 为不可信认知用户, 此用户被剔除, 其感知结果不参加最终融合判决。融合中心利用诚实认知用户的本地感知结果 d_i , 运用“OR”、“AND”和“Majority”3 种融合准则进行最终的融合判决, 得到最终判决最终结果 d 。

步骤6 判断 CU_i 的本地感知结果 d_i 与最终判决结果 d 是否一致, 若 $d_i=d$, 则 CU_i 提交的数据为诚实感知数据, 连续诚实感知次数 h 加 1; 若 $d_i \neq d$, 则 CU_i 提交的数据为虚假感知数据, 连续虚假感知次数 m 加 1, 然后进行下一次融合判决。

4 仿真实验及结果分析

利用 MATLAB 搭建的实验平台, 通过循环仿真法, 分析动态信任评估机制的性能。仿真环境参数设置见表 1。

表1 仿真环境参数设置

参数	描述	缺省值
N	认知用户总数	60
P	主用户总数	5
$cycle$	循环仿真次数	200
mp	恶意用户比例	0~90%
θ	信任门限值	0.5

考虑到实际协作频谱感知中可能存在多径衰落和阴影效应, 仿真中设置正常用户以 0.8 的概率进行正确感知。

为了突出动态信任评估机制的仿真效果, 提取出信任评估机制^[17,18]中最典型的贝叶斯信任进行仿真对比。如图 3 所示, 在动态性 SSDF 攻击下, 贝叶斯信任中恶意用户的信任值随着感知时刻不断波动, 且基本都大于信任门限值, 处于可信状态。在加入时间衰减因子、奖励因子和惩罚因子的动态信任机制中恶意用户的信任值很快处在信任门限值之下, 对动态性 SSDF 攻击进行了一定的抑制。

攻击成功率反映对恶意用户的抑制程度, 分别仿真对比了在贝叶斯信任、参考文献[7]中的简单奖惩信任机制和动态信任评估机制保护下全“0”和全“1”攻击模式对“OR”、

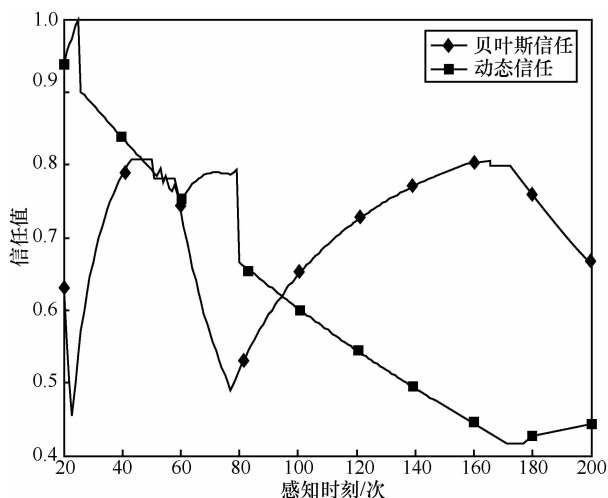


图3 恶意用户信任值变化情况

“AND”和“Majority”融合准则的攻击成功率。图4为全“0”模式攻击对“OR”融合准则的攻击成功率。如图4所示,随着恶意用户数增多,攻击成功率呈增长趋势,但在动态信任保护下的恶意用户的攻击成功率始终低于在贝叶斯信任和简单奖惩机制保护下的攻击成功率,而且增长也比在其他两种机制中缓慢。

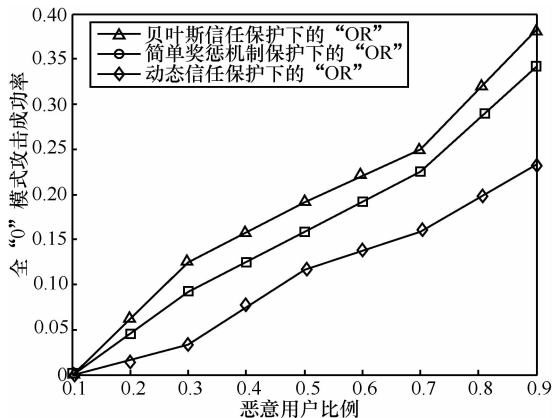


图4 全“0”攻击对“OR”准则攻击成功率

图5为全“0”模式攻击对“AND”融合准则的攻击成功率。在全“0”攻击下,3种信任机制对“AND”融合准则的攻击成功率抑制效果一般,这是因为只要有一个认知用户发送“0”,“AND”融合准则的融合结果就为“0”。

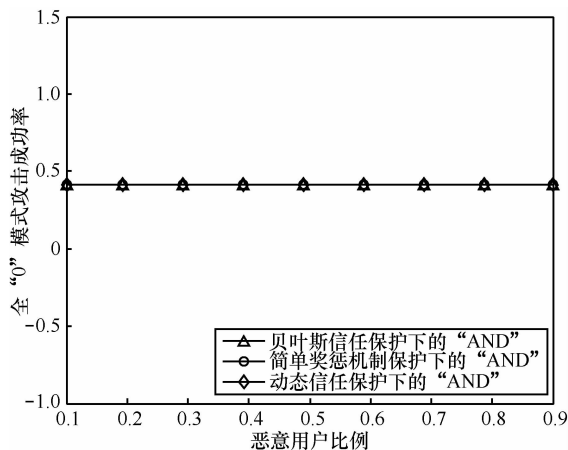


图5 全“0”攻击对“AND”准则攻击成功率

图6为全“0”模式攻击对“Majority”融合准则的攻击成功率。在贝叶斯信任下,当恶意用户达到认知用户总数的一半时,攻击成功率就达到最大值;在简单奖惩机制下,恶意用户达到70%时,攻击成功率达到最大值,而在动态信任保护下,恶意用户达到90%时,攻击成功率才达到最大值,在恶意用户较多时动态信任机制的优势更为突出。

图7为全“1”模式攻击对“OR”融合准则的攻击成功

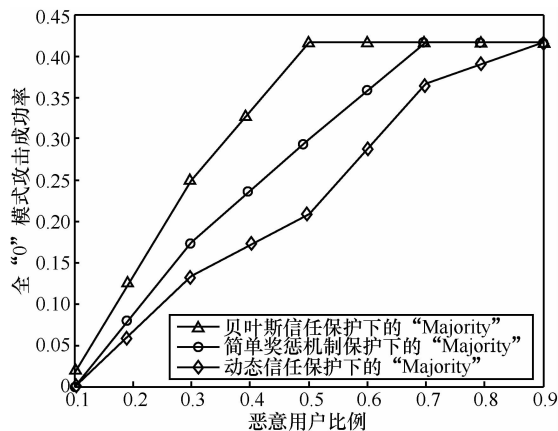


图6 全“0”攻击对“Majority”准则攻击成功率

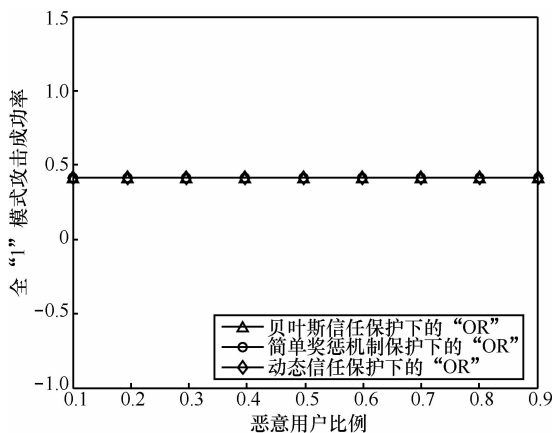


图7 全“1”攻击对“OR”准则攻击成功率

率。同样,3种信任机制在“OR”融合准则中对全“1”攻击抑制效果一般,这是因为只要有一个认知用户发送“1”,“OR”融合准则的融合结果就为“1”。

图8为全“1”模式攻击对“AND”融合准则的攻击成功率,图9为全“1”模式攻击对“Majority”融合准则的攻击成功率。在“AND”和“Majority”融合准则中动态信任保护下的

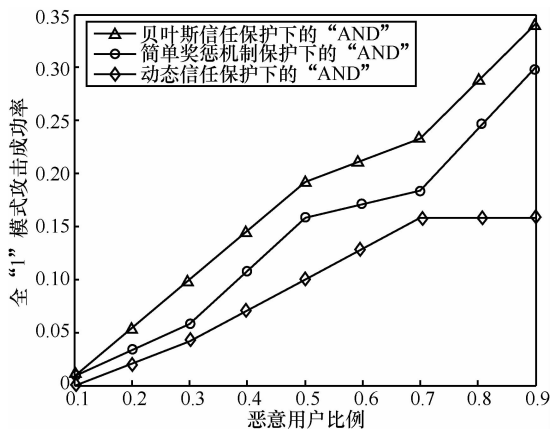


图8 全“1”攻击对“AND”准则攻击成功率

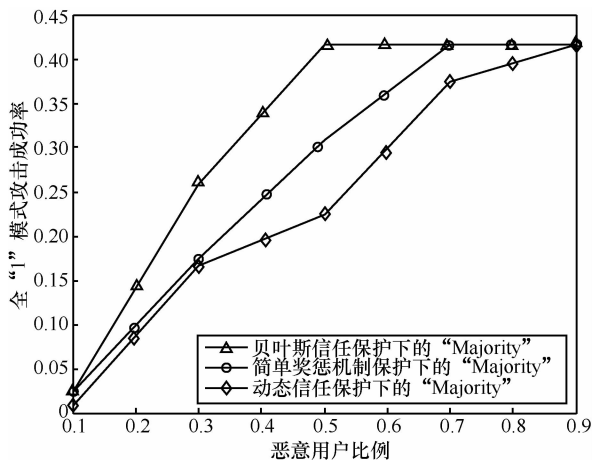


图9 全“1”攻击对“Majority”准则攻击成功率

攻击成功率始终低于贝叶斯信任和简单奖惩机制保护下的攻击成功率,随着恶意用户数的增加这种优势越明显,其中动态信任对两种融合准则的保护作用更加突出说明,引入时间衰减因子、加性奖励因子和加性惩罚因子的动态信任评估机制过滤掉了恶意用户,在一定程度上抑制了其动态性 SSDF 攻击成功率。

5 结束语

针对动态性 SSDF 攻击对协作频谱感知的危害,提出了一种动态信任评估机制,利用时间衰减和认知用户的历史行为实时更新信任值,实时识别交替提交虚假和诚实感知数据的恶意用户,抑制其攻击行为,并给出了动态信任评估机制的具体实现流程。仿真结果表明,该算法可以有效抑制恶意用户信任度的增长,降低了其对“OR”、“AND”和“Majority”数据融合准则的攻击成功率,保持了较好的协作频谱感知性能。

参考文献:

- [1] MITOLA J, MAGUIRE G. Cognitive radio: making software radios more personal [J]. IEEE Personal Communications, 1999, 6(4):13-18.
- [2] 王海莲, 张士兵, 郭莉莉. 基于可信度的加权协作频谱检测算法[J]. 数据采集与处理, 2014, 29(3): 472-477.
WANG H L, ZHANG S B, GUO L L. Reliability-based weighted cooperative spectrum sensing algorithm [J]. Journal of Data Acquisition & Processing, 2014, 29(3): 472-477.
- [3] FENG J Y, ZHANG Y Q, LU G Y. A soft decision scheme against intermittent SSDF attack in cooperative spectrum sensing [C]// The 14th IEEE International Conference on Computer and Information Technology, September 11-13, 2014, Xi'an, China.

New Jersey: IEEE Press, 2014.

- [4] 冯景瑜, 李金龙, 卢光跃. 协作频谱感知中抗 SSDF 攻击的认知用户不确定性行为评估 [J]. 电信科学, 2015, 31(2): 2015025.
FENG J Y, LI J L, LU G Y. Evaluating uncertainty behaviors of cognitive users against SSDF attack for cooperative spectrum sensing[J]. Telecommunications Science, 2015, 31(2): 2015025.
- [5] WANG Y H, LI Y L, YUAN F, et al. A cooperative spectrum sensing scheme based on trust and fuzzy logic for cognitive radio sensor networks [J]. International Journal of Computer Science Issues, 2013, 10(1): 275-279.
- [6] PEI Q Q, YUAN B B, LI L, et al. A sensing and etiquette reputation-based trust management for centralized cognitive radio networks[J]. Neurocomputing, 2013, 101(3): 129-138.
- [7] FENG J Y, LU G Y, BAO Z Q, et al. Supporting trustworthy cooperative spectrum sensing in cognitive radio networks [J]. Journal of Computational Information Systems, 2014, 10(10): 1-12.
- [8] 龚曙明, 朱海玲. 应用统计学[M]. 北京:中国水利水电出版社, 2010: 79-80.
GONG S M, ZHU H L. Applied statistics [M]. Beijing: China Water & Power Press, 2010: 79-80.
- [9] 陈亚琨, 赵海峰, 穆晓敏. 认知无线电基于感知信息量化的合作频谱感知[J]. 电视技术, 2012, 36(17):106-109.
CHEN Y K, ZHAO H F, MU X M. Cooperative spectrum sensing based on quantization of observed energy in cognitive radio network[J]. Video Engineering, 2012, 36(17): 106-109.
- [10] AKYILDIZ I F, LO B F, BALAKRISHNAN R. Cooperative spectrum sensing in cognitive radio networks: a survey [J]. Physical Communication, 2011, 4(1): 40-62.
- [11] PEI Q Q, LIANG R, LI H N. A trust management model in centralized cognitive radio networks [C]//The 2011 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, October 10-12, 2011, Beijing, China. New Jersey: IEEE Press, 2011: 491-496.
- [12] SHEN J, LIU S, ZENG L, et al. Optimisation of cooperative spectrum sensing in cognitive radio network [J]. IET Communications, 2009, 3(7): 1170-1178.
- [13] BLASCO M J, RIFÀ-POUS H, GARRIGUES C. Review of robust cooperative spectrum sensing techniques for cognitiveradio networks [J]. Wireless Personal Communications, 2012, 67(2): 175-198.
- [14] 徐文拴, 辛运韩, 卢桂章. 普适计算环境下信任机制的研究进展[J]. 计算机科学, 2008, 25(2): 52-57.
XU W S, XIN Y W, LU G Z. Research and development of trust mechanism for pervasive computing. Computer Science, 2008, 25(2): 52-57.
- [15] 康松林, 王彦东, 李慧. 信任模型在无线传感器网络入侵检测中的应用[J]. 计算机工程与用, 2012, 48(5): 89-92.

KANG S L, WANG Y D, LI H. Application of trust model in wireless sensor networks intrusion detection [J]. Computer Engineering and Applications, 2012, 48(5): 89-92.

[16] JSANG A, ISMAIL R. The Beta Reputation system [C]//The Bled Electronic Commerce Conference, June 17-19, 2002, Bled, Slovenia. [S.l.: s.n.], 2002: 1-14.

[17] QIN T, YU H, LEUNG C. Towards a trust-aware cognitive radio architecture [J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2009, 13(2): 86-95.

[18] FENG J Y, ZHANG Y Q, Lu G Y, et al. Securing cooperative spectrum sensing against rational SSDF attack in cognitive radio networks [J]. KSII Transactions on Internet and Information Systems, 2014, 8(1): 1-17.

[作者简介]



王美瓔(1989-),女,西安邮电大学通信与信息工程学院硕士生,主要研究方向为认知无线电、协作频谱感知等。



冯景瑜(1984-),男,博士,西安邮电大学通信与信息工程学院副教授,主要研究方向为无线通信安全、认知无线电、协作频谱感知等。



卢光跃(1971-),男,博士,西安邮电大学通信与信息工程学院教授,主要研究方向为通信信号处理、认知无线电、协作频谱感知等。



韩定坤(1990-),男,西安邮电大学通信与信息工程学院硕士生,主要研究方向为认知无线电、协作频谱感知等。