



分布式协作认知无线电 SSDF 攻击的防御策略综述

卢光跃, 苏杭

(西安邮电大学无线网络安全技术国家工程实验室, 陕西 西安 710121)

摘要: 协作频谱感知可以提高频谱感知的可靠性, 但其融合机制使得其易受频谱感知数据篡改 (spectrum sensing data falsification, SSDF) 攻击影响。为深入了解 SSDF 攻击防御算法的发展现状及趋势, 总结了 SSDF 攻击典型的分布式防御策略, 并对相应分布式防御算法进行了比较。最后依据目前相关研究中所发现的问题, 对 SSDF 攻击分布式防御策略未来的研究方向进行了展望。

关键词: 认知无线电; 频谱感知数据篡改; 协作频谱感知

中图分类号: TN92

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017022

Survey on SSDF attack and defense for distributed cooperative cognitive radio

LU Guangyue, SU Hang

National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Abstract: Cooperative spectrum sensing (CSS) improves the reliability of spectrum sensing, however, it is susceptible to spectrum sensing data falsification (SSDF) due to the fusion mechanism. To insight into the current research and development trend of defense strategy against the SSDF attack, several typical distributed strategies were concluded and the types of distributed algorithms were analyzed in several aspects. Finally, the future research of SSDF distributed defense strategy was prospected based on the problems found in the current research.

Key words: cognitive radio, spectrum sensing data falsification, cooperative spectrum sensing

1 引言

在无线设备和多媒体应用发展迅猛的今天, 可用频谱资源已经十分匮乏。目前的频谱资源分配机制已不能满足现实的需求, 所以寻求一种高效利用频谱资源的技术迫在眉睫, 而认知无线电 (cognitive radio, CR) 技术作为一种动

态智能频谱管理技术, 将是解决频谱资源日益匮乏、频谱利用低效等问题的关键技术手段^[1-3]。

认知无线电的中心思想是在主用户 (primary user, PU) 不占用其授权频段时, 允许次用户 (secondary user, SU) 动态接入该频段, 而当 PU 重新接入该授权频段时, SU 应当及时撤出, 以免对 PU 通信造成干扰。可见, 认知无线电的

收稿日期: 2016-10-21; 修回日期: 2017-01-06

基金项目: 国家自然科学基金资助项目 (No.61271276, No.61301091); 国家高技术研究发展计划 (“863”计划) 基金资助项目 (No.014AA01A705)

Foundation Items: The National Natural Science Foundation of China (No.61271276, No.61301091), The National High Technology Research and Development Program of China (863 Program) (No.014AA01A705)



首要工作是频谱感知(spectrum sensing, SS), 即 SU 能够快速且准确感知 PU 信号是否存在, 以实现频谱动态接入和撤出授权频段。

在接收到信号后, SU 既可以独自判断 PU 是否存在, 也可以与其他 SU 合作共同完成判决, 后者被称作协作频谱感知(cooperative spectrum sensing, CSS)^[4]。相较于非协作频谱感知, CSS 有着独特的优势。例如, 某一 SU 在接收信号时受到阴影效应等不利影响, 其将很难独自做出准确判决, 而 CSS 可通过 SU 之间感知信息的分享来解决这一问题^[5]。依据整个认知网络中是否存在融合中心, CSS 分为集中式 CSS 和分布式 CSS。集中式 CSS 网络存在一个融合中心, 整个认知网络由融合中心收集各 SU 本地感知数据, 并根据某种规则融合感知数据, 以完成统一判决^[6,7]。而分布式 CSS 网络不存在融合中心, 节点自身与各自所有邻居节点构成该节点的本地认知网络。此类网络中的节点在接收到信号后, 会将本地信号传给所有的邻居节点, 同时接收邻居节点发送的信号, 然后节点根据融合规则更新本地状态值, 本地状态值更新后即表示完成一次数据融合过程^[8-12]。整个网络各节点将重复以上信息交互与数据融合过程, 直到所有节点状态值达到收敛状态。

由此可知, CSS 实质是多个 SU 一起确定频谱资源的使用情况, 通过融合不同 SU 的感知数据来提高频谱感知的准确性和可靠性。但 CSS 的协同特性在获得较高感知技术收益的同时, 也可能带来更多风险。例如 CSS 网络中存在多种潜在的安全威胁, 其中最为常见的有模仿主用户 (incumbent emulation, IE) 攻击和频谱感知数据篡改 (spectrum sensing data falsification, SSDF)^[13,14]攻击。IE 攻击时, 恶意用户 (malicious user, MU) 模仿 PU 信号特征欺骗其他 SU, 以干扰其他 SU 的感知与判决^[15]; SSDF 攻击时, MU 会在每一次信息交互过程中将错误的感知值发送给邻居节点, 最终影响整个认知网络的收敛状态值。本文将重点论述 SSDF 攻击的防御策略。

MU 发动 SSDF 攻击时, 若认知网络的收敛值偏离了正确范围, 其最终的判决结果就将出现错误, 整个认知无线电系统也就无法进行正常的动态频谱切换, 进而出现频谱资源被 MU 控制利用或干扰到 PU 的正常使用的不利状况^[16]。因此, 防御 SSDF 攻击, 确保认知网络在遭受 SSDF 攻击时仍能保持较高的检测性能, 是 CR 技术持续发展的关键。目前, 国内外对 CSS 网络中 SSDF 攻击的研究尚处于初始阶段, 但已有不少研究成果。

根据 CSS 网络结构, SSDF 攻击的防御策略同样可分为集中式和分布式两种。在现有的研究成果中, 集中式防御策略比重较大, 其中应用较多的主要有以下 3 类: 基于贝叶斯理论的 SSDF 防御策略^[17-19]、基于加权序贯概率比检测的 SSDF 防御策略^[20,21]和基于信誉机制的 SSDF 防御策略^[22-26]。其他集中式防御策略, 例如参考文献[27]利用相近度估计节点可靠程度, 提出的基于 DS 证据理论的防御策略, 参考文献[28]利用感知结果的相似性排除错误感知结果, 提出的基于回归平面的防御策略等, 也都取得了不错的防御效果。

然而, 集中式 CSS 网络自身存在缺陷, 其融合中心位置较为固定, 且融合中心与少数偏远的 SU 之间存在某些通信约束, 因此集中式 CSS 的防御策略具有较大局限性^[8]。分布式 SSDF 攻击的防御策略起步较晚, 但近年得到了快速发展。现有的分布式防御策略大致可分为 4 类, 即基于最大差值^[29-31]、基于中值滤波^[32]、基于信任机制^[33-40]以及基于权值的分布式防御策略^[40]。

2 系统模型

通常, SS 可表述为一个二元假设检验问题, 即: H_0 表示 PU 不存在, SU 可接入该频谱; H_1 表示 PU 存在, SU 不可接入该频谱。因此, SS 的数学模型^[29]可描述为:

$$y_i(m) = \begin{cases} w_i(m), & H_0 \\ h_i s(m) + w_i(m), & H_1 \end{cases} \quad (i=1, 2, \dots, N) \quad (1)$$

其中, $y_i(m)$ 是第 i 个次用户 SU_i 在 m 观测时刻 ($m=1, 2, \dots, M$) 接收到的采样信号, $w_i(m)$ 是加性高斯白噪声, $s(m)$ 是 PU 发送的信号, h_i 为信道增益。

一般情况下, 分布式 CSS 算法通常包括节点感知、数据融合、判决 3 个阶段。在节点感知阶段, 所有节点对信号进行感知并得到状态值 $x_i(0)$ 。在数据融合阶段 (如图 1 所示), 节点 SU_i 根据其自身属性, 在第 k 个迭代时刻, 需将其状态值 $x_i(k)$ (正常节点时) 或篡改后的状态值 $f(x_i(k))$ (恶意节点 (如图 1 中 SU_4) 时) 与其邻居节点进行交换, 然后根据迭代融合规则更新状态值, 得到 $x_i(k+1)$ 。重复以上过程, 直到所有 SU 状态值达到收敛。在判决阶段, 节点 SU_i 将最终本地状态值 x_i^* (及其收敛值) 与检测门限 V_α 进行比较, 判断 PU 信号是否存在。

由此可知, 非安全环境下, 数据融合阶段是 MU 的攻击时期, 亦是判别 SU 是否为 MU 的关键时期。正常 SU 在数据融合阶段接收到所有邻居用户传输值后, 其应及时判

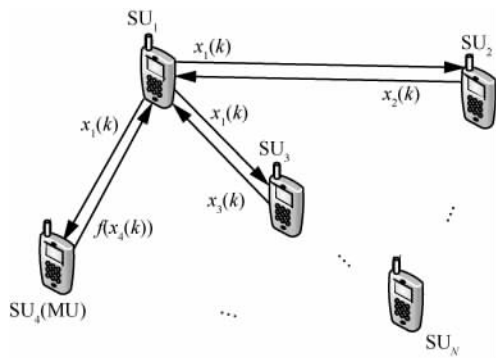


图 1 非安全环境下认知网络节点间数据交换

断传输值是否恶意。一旦该阶段 SU 因漏判 MU 而接收了 MU 的篡改传输值，或是因将正常 SU 误判为 MU 而未融合该 SU 的正常传输值，就可能在判决阶段出现判决错误，进而发生干扰 PU 或频谱资源浪费现象。因此，认知网络需要有一种防御机制，能够帮助 SU 有效甄别 MU，保证频谱感知的准确性。非安全环境下认知网络分布式 CSS 防御策略的步骤如图 2 所示。而在给出具体的 SSDF 攻击的防御策略之前，有必要了解一下 SSDF 攻击的攻击类型。

3 SSDF 攻击类型

SSDF 攻击的特点是 MU 在 CSS 网络中将本地感知值篡改为错误的数值，以虚假的感知信息干扰认知网络的判决，从而达到恶意攻击的意图。现有的很多参考文献，已经从不同角度对 SSDF 攻击类型进行了分析^[9,42-46]。例如，若从攻击手段角度进行分析，SSDF 攻击可分为全 1 攻击、全 0 攻击、取反攻击等；而从攻击策略角度进行分析，SSDF 攻击又可分为静态攻击、动态攻击、变换身份攻击等。

无论 MU 发动何种方式 SSDF 攻击，其传输值都是 MU 对其自身的本地感知值进行数值篡改的结果。定义 MU 发动 SSDF 攻击时，MU 本地感知值 $x_j(k)$ 被篡改为 $f(x_j(k))$ 。于是篡改值 $f(x_j(k))$ 可统一表示成如下形式：

$$f(x_j(k)) = \begin{cases} \lambda x_j(0), & \text{攻击时 (概率为 } p) \\ x_j(0), & \text{未攻击时 (概率为 } 1-p) \end{cases} \quad (2)$$

式(2)为 SSDF 攻击的统一攻击模型，其中 p 为攻击概率， p 值越大，表示发动 SSDF 攻击的频率越高； λ 称作 SSDF 攻击强度， $\lambda=1$ 时，表示该 MU 未发动攻击，而 λ 值偏离 1 越远，表示 SSDF 攻击强度越大。

依据 MU 发动攻击强度和攻击概率的大小，可将所有 SSDF 攻击归结为 3 种攻击方式：间歇攻击、恒定攻击、随机攻击。下面将详细介绍 3 种方式的 SSDF 攻击，并给出其具体的攻击模型。

3.1 间歇攻击

MU 在每次信息交互过程中，均依概率确定其是否发动攻击，在攻击时发送篡改值给邻居节点，而非攻击时发送正常状态值，该类攻击方式称作间歇攻击。

发动间歇攻击时 MU 攻击概率 p 、攻击强度 λ 均不等于 1，因此间歇攻击的攻击模型可表示为：

$$f(x_j(k)) = \begin{cases} \lambda x_j(0), & \text{攻击时 (概率为 } p) \\ x_j(0), & \text{未攻击时 (概率为 } 1-p) \end{cases} \quad (3)$$

其中， λ_j 为非 1 常数。

间歇攻击属于非持续型攻击，其对认知网络判决的影响也依攻击概率 p 值大小变化。发动间歇攻击的 MU 具有较高的隐蔽性，其篡改规律也难以被掌控。而现有文献所给出的防御策略，对间歇攻击的防御性能普遍较差。

3.2 恒定攻击

MU 在每次信息交互过程中都给邻居节点发送固定数值的篡改值，该类攻击方式称作恒定攻击。即恒定攻击时 MU 攻击概率 $p=1$ ，攻击强度 λ 为定值，因此，恒定攻击的攻击模型可表示为：

$$f(x_j(k)) = \lambda_h \cdot x_j(0) \quad (4)$$

其中， λ_h 取固定常数。当 $\lambda_h > 1$ 或 $1/\lambda_h > 1$ 时，该类 SSDF 攻击称强恒定攻击；当 $\lambda_h \rightarrow 1$ 时，该类 SSDF 攻击称弱恒定攻击。

依据 MU 进行恒定攻击的时间选择及目的不同，恒定攻击可分为自私型 SSDF 攻击和干扰型 SSDF 攻击。若主信号不存在而 MU 发送较大的篡改值，其目的是给其他

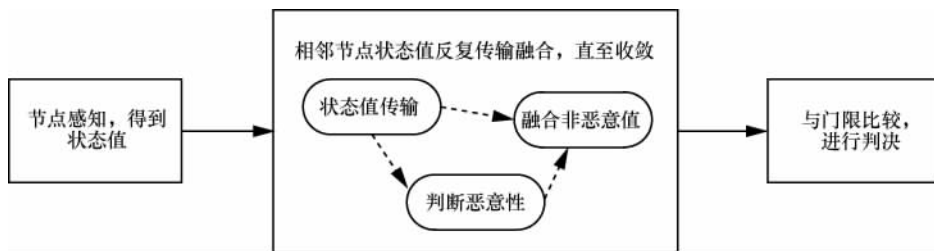


图 2 非安全环境下认知网络节点分布式 CSS 防御策略步骤



SU 造成 PU 正占用频谱的假象, MU 自身便可自由地使用该段空闲频谱, 该类恒定攻击称为自私型 SSDF 攻击; 若主信号存在而 MU 发送较小的篡改值, 其目的是使得其他 SU 误以为频谱处于空闲状态, 进而造成 SU 干扰 PU 的不利情况, 该类恒定攻击称为干扰型 SSDF 攻击。

恒定攻击属于持续型攻击, 其使得状态值始终变大或变小, 对认知网络的最终判决造成了较大影响。尤其是强恒定攻击, 严重干扰了认知网络的正常判决。但恒定攻击对数据的篡改是有规律可循的, 因此抵御该类攻击相对较为容易。现有文献所给出的防御策略, 通常都能有效对抗恒定攻击。

3.3 随机攻击

无论 PU 是否存在, 在每次信息交互过程中, MU 都在特定攻击强度范围内随机取值, 并据此篡改本地感知值, 且将其发送给邻居节点, 该类攻击方式称作随机攻击。随机攻击的取值范围由 MU 自身设定。

发动随机攻击时 MU 攻击概率 $p=1$, 而攻击强度 λ 的取值通常服从某一分布, 因此随机攻击的攻击模型可表示为:

$$f(x_i(k)) = \lambda_s \cdot x_i(0) \quad (5)$$

其中, λ_s 为随机常数, 且服从某一分布, 如均匀分布、高斯分布等。

随机攻击同样属于持续型攻击, 发动随机攻击的 MU 甚至不需要参与感知过程, 该类攻击使得状态值变化大小摇摆不定, 严重影响到认知网络的最终判决; 而且随机攻击对数据的篡改规律很难被发现, 因此较好地抵御该类攻击相对困难。现有文献所给出的防御策略, 对随机攻击的防御性能参差不齐。

综合上述分析可知, 不同的 SSDF 攻击方式拥有不同的攻击特性, 相应的, 不同方式的 SSDF 攻击有不同的攻击模型, 这为实际中的 SSDF 防御增加了难度。

4 SSDF 攻击的分布式防御策略

认知网络中的 SU 通常在收到所有邻居用户发送来的状态值后, 依据某种规则判断各邻居用户是否属于 MU, 从而确定后续数据融合及判决的策略。不同的判断规则及后续处理方式, 将得到不同的 SSDF 攻击分布式防御算法。

一般情况下, SSDF 攻击的分布式防御算法的步骤如下所示。

步骤 1 SU_i 实时感知感兴趣频段的信号, 得到初始

状态值; 而且, 考虑到实施的简便性, 通常所有节点均采用能量检测 (ED)^[47, 48] 得到各自的统计量 $Y_i = \sum_{m=0}^{M-1} |y_i(m)|^2$, 并将其取为 CSS 防御策略中 SU_i 的初始状态值, 即 $x_i(0) = Y_i$ 。

步骤 2 在 k 个迭代时刻, SU_i 将状态值 $x_i(k)$ 发送给所有的邻居用户, 同时接收所有邻居用户状态值。

步骤 3 SU_i 依据某种规则区分并处理 MU 状态值。

步骤 4 SU_i 依据融合规则迭代融合各状态值, 得到更新后的本地状态值 $x_i(k+1)$ 。

步骤 5 重复步骤 2~4, 直到所有 SU 状态值达到收敛。

步骤 6 SU_i 将收敛后的本地状态值 x_i^* 与检测门限 V_c 进行比较, 判断 PU 信号是否存在。

可见, 步骤 3 中区分并处理 MU 状态值的规则以及步骤 4 中状态值融合规则是决定分布式防御算法性能的关键, 这两个规则的设计也将是整个 SSDF 攻击分布式防御算法的核心。

目前, 国内外已有不少文献对 SSDF 攻击进行了分析研究, 并给出了相关防御策略, 但其中分布式防御策略较少。而现有成果中的分布式防御策略主要可分为以下 4 类。

(1) 基于最大差值的 SSDF 防御策略

该类策略一般是利用邻居节点传输值与本地节点局部节点平均值间的最大差值作为 MU 的判断依据。

(2) 基于中值滤波的 SSDF 防御策略

该类策略认为 MU 发动 SSDF 攻击时, 其攻击值大小应分布于传输值集合的两侧, 于是利用中值滤波的思想, 将其排除在节点融合范围之外。

(3) 基于信任机制的 SSDF 防御策略

是最常见的 SSDF 防御策略。该类策略引入各形式的信任机制, 持续更新邻居节点的信誉值, 并依据信誉值大小融合邻居节点传输值。

(4) 基于权值的分布式防御策略

该类策略中, 本地节点依据某种原则为邻居节点传输值设定权值, 然后对各传输值进行加权融合, 更新本地状态值。

各类防御策略对不同方式的 SSDF 攻击防御性能有所差异, 下面详细介绍这 4 类 SSDF 防御策略。

4.1 利用最大差值的分布式防御策略

Tang 和 Yu 等人^[29]最早提出 SSDF 攻击的分布式防御方法——基于最大差值的 CSS (largest deviation-based distributed cooperative spectrum sensing, LDCSS) 算法。

LDCSS 算法将邻居节点传输值与本地节点局部平均值之间最大差值作为 MU 唯一的判定依据。当邻居节点个数大于 2 时,节点 SU_i 将邻居节点中传输值与本地认知网络平均值之间差值最大的节点视为 MU 并剔除,此后不再接收该节点传输值,即邻居节点个数可视为减少了 1;当邻居节点个数不大于 2 时, SU_i 不再剔除任何邻居节点。随后节点 SU_i 将依据留下的邻居节点传输值更新本地状态值。

LDCSS 算法在状态值迭代更新时需要网络最大度这一先验知识,具有较大局限性。之后 Ejaz W 等人^[30]针对 LDCSS 算法状态值迭代更新公式进行了改进,提出了基于梯度的 CSS (gradient-based distributed cooperative spectrum sensing, GCSS) 算法。该算法迭代时根据本地状态值与邻居节点传输值间的比值大小,定义了邻居节点梯度值,并由此完成状态值迭代,因此不需要网络最大度先验知识。

然而 LDCSS 和 GCSS 算法均一直假定本地认知网络中存在 MU,该方式很容易将正常 SU 误判为 MU 而剔除,使得很多节点间的双向通信路径变成单向通信路径,甚至整个网络分裂成数个断开的节点板块,进而认知网络无法快速收敛甚至无法收敛,检测性能和稳定性降低。因此,对于利用最大偏差来排除 MU 的防御算法,其通常可有效降低 SSDF 恒定攻击的影响,但在面对随机攻击或间歇攻击时,该类算法性能较差。

4.2 基于中值滤波的分布式防御策略

正常情况下,大多数节点的感知值是相似接近的。对于发动攻击的 MU,若要对认知网络产生较大影响,其篡改值应偏离大多数节点的感知数值范围,或者高于这个范围,或者低于这个范围。这种情况下,MU 篡改值将排在本地认知网络中传输值集合的两端。

利用中值滤波的分布式防御 (median filtering-based distributed cooperative spectrum sensing, MFCSS) 算法^[32]正是以此作为核心思想来排除 MU 篡改值影响。该算法从节点选择的角度入手,用中值滤波的方法替换了利用最大偏差排除 MU 的思想,同样可达到拒绝 MU 篡改值进入融合步骤的目的,从本质上还可以说是 LDCSS 算法的一种改进。MFCSS 算法解决了利用最大偏差来排除 MU 此类算法易将正常 SU 误判为 MU 的缺陷,且实现简单,计算量也小于 LDCSS 算法。虽然 MFCSS 算法在面对 3 种不同方式的 SSDF 攻击时都能取得一定防御效果,但该类算法在每一次迭代时刻都会略去较多的正常传输值,这不利于所有正常节点的信息融合,整个网络也因此无法获得更高的检测性能。

4.3 基于信任机制的分布式防御策略

所谓“信任机制”,是指关系网络中构成、影响个体间相互信任关系的各部分及其之间的关系管理机制。信任机制最早由 Blaze 等人^[49]运用于解决网络安全问题,其在无线传感器网络、社交网络及物联网等环境中得到了广泛应用。只要涉及协作,就必然存在信誉值大小问题,而分布式 CSS 正是一种协作活动。

基于信任机制的 CSS 算法是在传统信任机制课题基础上,结合 CSS 的特点而形成了适用于 CSS 的研究成果,其对于 SU 防御 SSDF 攻击、进而准确找出可用的空闲频谱发挥着重要作用。基于信任机制的 CSS 算法一般思路为:某数据传输中心(比如集中式认知网络中的融合中心)在接收到其他节点传输来的状态值后,会综合节点历史传输值和当前传输值来计算该节点的信誉值。在得到各节点信誉值后,数据传输中心取其中信誉值较高的节点传输值完成融合。因此,设计基于信任机制 CSS 算法的核心在于如何计算节点信誉值。

现有的基于信任机制 CSS 算法中,绝大多数是运用于存在融合中心的网络环境中,分布式 CSS 防御算法较少。已有的分布式防御算法中性能较好的是 Li 等人^[39]于 2015 年提出的基于信誉值的分布式 CSS (reputation-based distributed cooperative spectrum sensing, RCSS) 算法。该算法中,在第 k 个迭代时刻对于节点 SU_i ,其邻居节点 SU_j 的信誉值 $T_{ij}(k)$ 由即时信誉值 $Q_{ij}(k)$ 与前一时刻信誉值 $T_{ij}(k-1)$ 两部分构成,这将有利于信誉值的合理更新,性能保持相对稳定。

RCSS 算法同样解决了利用最大差值易将正常 SU 误判为 MU 的缺陷,且无论面对恒定攻击、随机攻击还是间歇攻击时,RCSS 算法均有不错的检测性能。但 RCSS 算法仍有一定局限性:其一,RCSS 算法同样需要网络最大度这一先验知识;其二,RCSS 算法在实际中建立信誉值自适应遗忘模型时,其最佳遗忘因子数值较难确定;其三,RCSS 算法不仅需要存储前一时刻的状态值,还需存储前一时刻信誉值,对应用设备提出了要求;其四,RCSS 算法在设定当前时刻信誉值时,会将历史信誉值考虑在内,因此该算法面对间歇攻击时的性能不如面对恒定攻击或随机攻击时。

4.4 基于权值的分布式防御策略

在面临多种 SSDF 攻击方式时,绝大多数算法存在着较大缺陷,这使得网络在应用这些算法时会受到限制。为此,分析并利用常见 SSDF 攻击方式的攻击特征,制定了每



一种常见攻击方式的应对策略,并提出了一种新的加权分布式 CSS (weighted distributed cooperative spectrum sensing using attack characteristics, ACWCSS) 算法。

对于恒定攻击,其特征是 MU 第 k 个迭代时刻传输值 $x_i(k)$ 与其第 $k-1$ 个迭代时刻传输值 $x_i(k-1)$ 相等或相差不大,这与达到收敛时的正常节点传输值特征相同。因此,对恒定攻击节点可采取依据其传输值偏离平均值的程度设定融合权值的方法。该方法下,强度较大的恒定攻击将会被给定较小的权值。

对于可能存在的高强度攻击, MU 传输值 $x_i(k)$ 与 $A_i(k)$ 偏差较大,因此还可以根据 $x_i(k)$ 与 $A_i(k)$ 的比值是否超出正常的偏差范围来判断高强度攻击。

对于随机攻击,其特征是 MU 传输值 $x_i(k)$ 与 $x_i(k-1)$ 不相关,即前后时刻 MU 传输数值无规律。正常邻居用户在历经数据融合后,其状态值 $x_i(k)$ 与 $A_i(k)$ 之差应变小,因此可以通过比较第 k 个迭代时刻的偏差值 $|x_i(k) - A_i(k)|$ 是否小于前一迭代时刻偏差值 $|x_i(k-1) - A_i(k-1)|$ 来判断随机攻击。

对于间歇攻击,其特征是 MU 攻击时的传输值与未攻击时传输值有较大出入,因此同样可以通过比较 $|x_i(k) - A_i(k)|$ 是否小于 $|x_i(k-1) - A_i(k-1)|$ 来判断间歇攻击。

于是,可设计如图 3 所示的 ACWCSS 算法加权规则,用以分辨恶意状态值,并为各状态值设定权值。图 3 中 $K = |x_j(k) - A_i(k)| - |x_j(k-1) - A_i(k-1)|$ 表示 SU_i 邻居节点 j 在第 k 个迭代时刻偏差值与第 $k-1$ 个迭代时刻偏差值之差。I 表示视作受高强度攻击,II 表示视作受随机攻击或间歇攻击,III 表示依据偏离程度设定融合权值。

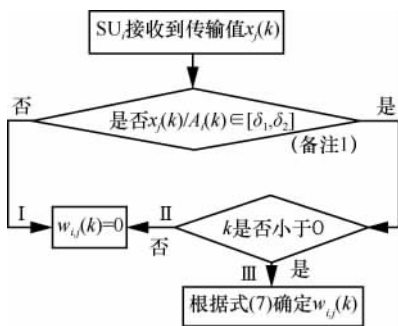


图 3 ACWCSS 算法加权流程

备注 1: 为了将处于正常取值范围边缘的传输值以及攻击强度较大的恶意值排除在外,定义正常值偏差范围 $[\delta_1, \delta_2]$, 其中 δ_1, δ_2 值由 SU_i 初始值 Y_i 的安全取值范围设定,具体方法为: SU_i 采用能量检测获取初始值,本地感知环境一定时 Y_i 范围仅与采样点数 M 有关,因此在设定 M

和卡方分布双侧概率 α (α 越大,算法抵御高强度攻击能力越强,但同时越可能将取值范围边缘的正常状态值排除)后,可查表得到 H_0 下 Y_i 的安全取值范围 $[\eta_1, \eta_2]^{[50]}$, η_1 与 η_2 的比值为 δ_1, η_2 与 η_1 的比值为 δ_2 。

对于处于图 3 中状态 III 的传输值,使用加权计算式给定融合权值。所提算法依据传输值 $x_j(k)$ 偏离 $A_i(k)$ 的程度设定权值。邻居节点 j 偏离程度可表示为:

$$\frac{|x_j(k) - A_i(k)|}{\sum_{j \in N_i(k)} |x_j(k) - A_i(k)|}, (j = 1, 2, \dots, |N_i(k)|)$$

而 ACWCSS 算法迭代计算式为:

$$x_i(k+1) = x_i(k) + \sum_{j \in N_i(k)} w_{i,j}(k) \left(1 - \frac{x_i(k)}{x_j(k)} \right) \quad (6)$$

式(6)是在 GCSS 算法迭代式基础上加入权值变量而来,为使各节点状态值可达到收敛,所提算法中各状态值权值均设定在 $[0, 1]$ 范围内,加权式如下:

$$w_{i,j}(k) = \frac{1}{3} \left[3 - \frac{|x_j(k) - A_i(k)|}{\sum_{j \in N_i(k)} |x_j(k) - A_i(k)|} \right] \quad (7)$$

其中, $w_{i,j}(k)$ 为第 k 个迭代时刻节点 SU_i 给 $x_j(k)$ 设定的权值,当 $w_{i,j}(k) < 0$ 时, $x_j(k)$ 为偏离 $A_i(k)$ 较远的攻击值,设定 $w_{i,j}(k) = 0$ 。

然后认知网络重复上述步骤,直至整个网络达到收敛状态。

ACWCSS 算法不仅解决了利用最大差值易将正常 SU 误判为 MU 的缺陷,而且保留了 GCSS 算法不需要网络最大度先验知识的优点。另外,ACWCSS 算法不存在确定最佳遗忘因子的难题,并在 RCSS 算法基础上进一步提升了认知网络面对 3 种 SSDF 攻击方式时的检测性能。

5 性能仿真

下面在瑞利信道下对 SSDF 攻击分布式防御策略的代表算法进行性能比较。仿真条件具体说明如下。

图 4 是包含 17 个 SU 的网络拓扑结构,其中节点 6 和节点 15 为潜在 MU,可以发动任意方式 SSDF 攻击,其余节点为正常 SU。若无特殊说明,仿真中时间带宽积 $TB=5$,各 SU 接收信号采样点数 $M=2TB=10$,设定 $\alpha=0.2$,平均信噪比为 0 dB,再由 M 和 α 设定 $\delta_1=0.3$ 和 $\delta_2=3.28$ 。

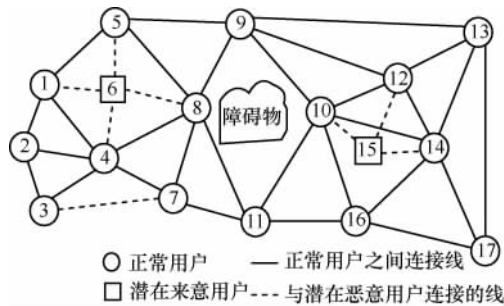


图 4 包含 17 个 SU 的网络拓扑结构

5.1 收敛性能分析

表 1 描述了 SU 面对不同方式 SSDF 攻击时各算法收敛性能的比较。节点收敛率可表述为各节点状态值经一定时间迭代融合后,达到统一状态值的节点数与全部节点数的比值,表 1 中所示数据为 3 种算法分别进行 10 000 次仿真后的平均节点收敛率值。LDCSS 和 GCSS 算法易将双向通信路径变为单向路径甚至断开路径,造成节点无法快速收敛甚至无法收敛,而 RCSS 和 ACWCSS 算法并非直接剔除可疑节点,获得了更高的节点收敛率。

5.2 检测性能与顽健性分析

图 5~图 7 分别给出了节点 6、15 两个 MU 发动恒定攻击、随机攻击、间歇攻击时各算法 ROC 性能曲线比较。

恒定攻击下,PU 存在时 MU 持续发送状态值 5,不存在时 MU 持续发送状态值 17。由图 5 可见,面对恒定攻击,MFCSS 算法由于略去了较多的正常传输值,因而影响

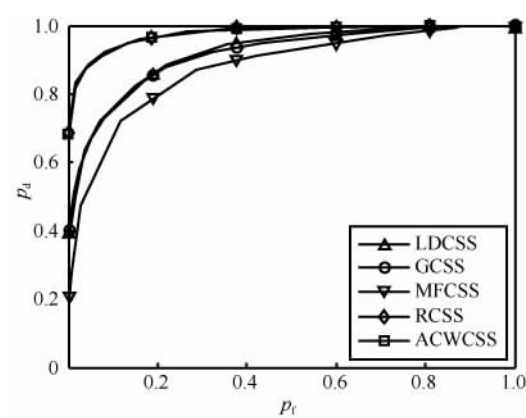


图 5 MU 发动恒定攻击

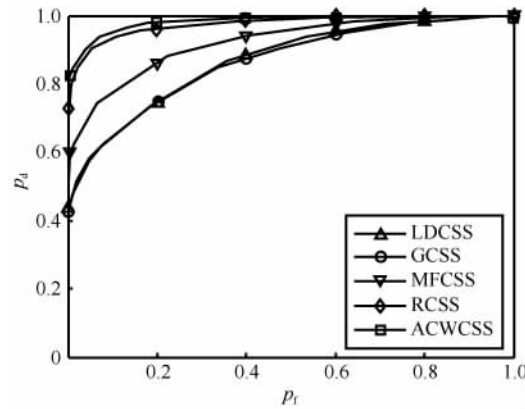


图 6 MU 发动随机攻击

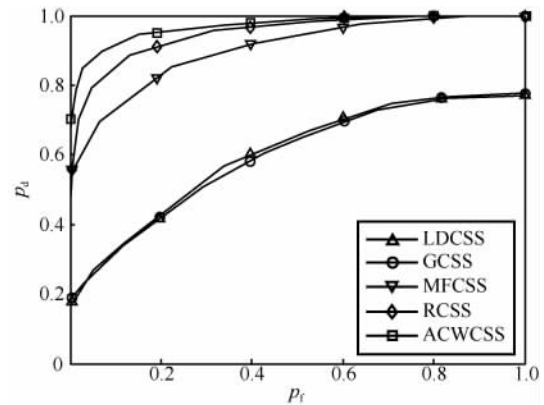


图 7 MU 发动间歇攻击

了检测性能。ACWCSS 算法检测性能与 RCSS 算法相当而优于 GCSS 和 LDCSS 算法。这是因为 ACWCSS、RCSS 算法均是依据偏离本地认知网络平均值远近来设定传输值的融合值,且两种算法均为高强度恒定攻击设计了防御措施,而 GCSS 和 LDCSS 算法易将正常 SU 判定为 MU 而造成性能降低。例如, $p_t=0.1$ 时,图 5 中采用 ACWCSS、RCSS、GCSS、LDCSS、MFCSS 5 种算法得到的 p_d 分别为 0.921 4、0.920 7、0.733 4、0.734 5、0.711 3。

随机攻击下,无论 PU 是否存在,MU 都在[5,17]范围内根据均匀分布随机取值发送。由图 6 可见,面对随机攻击,ACWCSS 算法检测性能略优于 RCSS 算法而大大优于 GCSS 和 LDCSS 算法。这是因为 GCSS 和 LDCSS 算法易将正常 SU 判定为 MU 而将其剔除,留下的 MU 将在之后的

表 1 5 种算法在不同 SSDF 攻击方式下的平均节点收敛率(迭代时间相同)

攻击方式	LDCSS 算法	GCSS 算法	MFCSS 算法	RCSS 算法	ACWCSS 算法
恒定攻击	90.34%	90.05%	93.37%	93.81%	96.15%
随机攻击	88.95%	88.57%	91.93%	93.06%	94.29%
间歇攻击	85.44%	85.68%	91.40%	93.12%	94.41%



迭代时刻干扰正常 SU, 最终影响检测性能。而 MFCSS 算法也不会冒然将邻居节点剔除, 获得检测性能也较 LDCSS、GCSS 算法好。例如, $p_t=0.1$ 时, 图 6 中采用 ACWCSS、RCSS、GCSS、LDCSS、MFCSS 5 种算法得到的 p_d 分别为 0.936 1、0.922 4、0.631 5、0.632 2、0.742 5。

间歇攻击下, PU 存在时 MU 在攻击时刻发送状态值 5, PU 不存在时 MU 在攻击时刻发送状态值 17, 非攻击时刻 MU 均发送正常状态值。由图 7 可见, 面对间歇攻击, ACWCSS 算法检测性能明显优于 GCSS 和 LDCSS 算法, 较 RCSS 算法也有较大提升。这是因为 RCSS 算法传输值融合时的信任值与历史信任值相关, 而间歇攻击时而攻击时而不攻击的攻击方式使得 RCSS 算法必然会受到该攻击方式的影响。例如, $p_t=0.1$ 时, 图 7 中采用 ACWCSS、RCSS、GCSS、LDCSS、MFCSS 5 种算法得到的 p_d 分别为 0.922 8、0.839 8、0.314 5、0.317 0、0.697 2。

为进一步比较 MU 数目增多对各算法的影响, 图 8 给出了不同数量 MU 下各算法检测性能的对比。仿真中 MU 等概率发动 3 种不同方式 SSDF 攻击, 给定 $p_t=0.1$, 总节点数仍为 17 个。由图 8 可见, 各算法的检测性能均随着 MU 数目增多而降低, 但 MFCSS、RCSS、ACWCSS 3 种算法检测性能降低的速度小于 LDCSS 和 GCSS 算法。而在 MU 数量相等条件下, RCSS、ACWCSS 算法检测性能均明显优于 GCSS 和 LDCSS 算法。

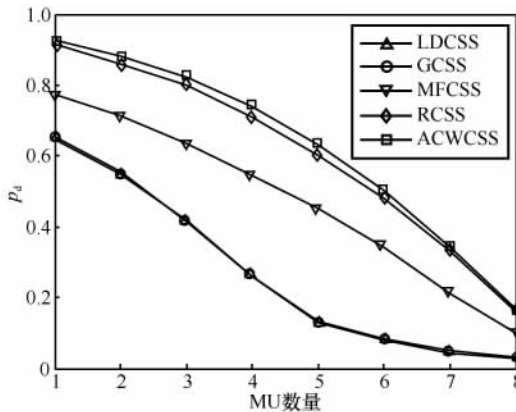


图 8 MU 不同 MU 数量下各算法检测概率比较

5.3 复杂度比较

表 2 描述了各算法的复杂度对比。考虑到分布式协作频谱感知算法的特殊性, 该类算法复杂度定义为认知网络完成一次迭代过程所需的运算复杂度。在一次迭代过程中, LDCSS 算法、GCSS 算法需计算出本地认知网络平均值以及该平均值与各邻居节点传输值之间差值, 且迭代前需进行一次排序; MFCSS 算法同样需要进行一次排序, 但其不需要进行本地认知网络平均值等计算, 因此其复杂度虽与 LDCSS、GCSS 算法一致, 但其计算量实际上是小于后两种算法的。ACWCSS、RCSS 算法需计算出邻居节点传输值的融合权值或信任值, 但不需要进行排序运算, 因此 ACWCSS 和 RCSS 两种算法的复杂度小于 LDCSS、GCSS 算法。

表 2 5 种算法复杂度对比

算法名称	算法复杂度
LDCSS	$O(N \cdot \Delta \cdot \ln \Delta)$
GCSS	$O(N \cdot \Delta \cdot \ln \Delta)$
MFCSS	$O(N \cdot \Delta \cdot \ln \Delta)$
RCSS	$O(N \cdot \Delta)$
ACWCSS	$O(N \cdot \Delta)$

5.4 典型防御算法比较

综合上述分析, 对所仿真的典型防御算法进行比较, 比较结果见表 3。

6 展望

在对典型分布式防御策略进行总结后, 对于今后分布式协作网络中 SSDF 攻击的防御工作, 可在以下几个方面进一步展开研究。

6.1 惩罚机制

节点网络中各次用户之间虽然是互相帮衬关系, 但即便是正常节点, 也可能会因为“懈怠”、一瞬间的“私心”等原因在某时刻不愿意分享正确的感知信息, 因此, 不妨考虑引入如下惩罚机制。

表 3 典型防御算法比较

算法名称	恒定攻击	随机攻击	间歇攻击	收敛速度	网络稳定性	先验知识
LDCSS	较好	较差	差	较快	低	需要
GCSS	较好	较差	差	较快	低	不需要
MFCSS	较好	较好	较好	快	较高	不需要
RCSS	很好	很好	好	快	高	需要
ACWCSS	很好	很好	很好	快	高	不需要

各节点在本地对信号进行感知并得到状态值后,网络间本地节点与邻居节点进行信息交互。对于传输恶意感知信息或非正常感知信息次数较多的邻居节点,本地节点可以对其发出警告,若其此后仍然较多次传输该类感知信息,本地节点可以联合其他正常节点对其进行惩罚。惩罚措施可以是本地节点在某段时间内不再发送感知信息给该邻居节点,也可以是彻底地孤立该问题节点。

惩罚机制可以用来规范用户网络,其可有效提高频谱感知中节点信息交互的积极性,在有效降低 MU 影响的同时,还可降低正常节点因消极懈怠等原因造成恶意行为的概率。

6.2 加密机制

要甄别 MU, 还可以借鉴信息安全领域中的密码学知识,引入加密机制。

每个节点在进入用户网络时,都为其自身设置唯一的身份信息。在信息交互过程中,若某个邻居节点被本地节点认可,本地节点将把代表自身的身份信息告知给该邻居节点。此后,带有本地节点身份信息签名的邻居节点传输值将被优先留用,且融合权值相对较高;而其他邻居节点传输值,将置于优先级降低的位置。

引入加密机制的分布式网络,不仅可以有效抵御 SSDF 攻击,对于其他类型攻击也都有着较大的抑制作用。

7 结束语

协作频谱感知中的安全问题是现阶段国内外研究的重点。本文结合当前 SSDF 攻击相关的研究成果,归纳了 SSDF 攻击的攻击类型,并对分布式防御策略中应用较多的算法进行了比较。分布式网络中的认知无线电技术应用将会越来越广泛,但目前 SSDF 攻击的 CSS 防御策略普遍侧重于集中式策略,分布式防御方法急需更深层次的拓展研究。

无线传感器网络、移动自组织网络及物联网等无线网络,均对频谱资源有较大需求,因此无线网络的高速发展离不开频谱感知技术的进步。对于不同类型、不同层次的无线网络,其 SSDF 攻击类型、攻击策略均存在较大差异。另外,进行分布式协作频谱感知的 SU 具备高度灵活性特点,其防御 SSDF 攻击的策略必须在感知设备成本和功能实现间进行权衡。因此,结合目前的研究成果来看,如何在有效抵御多攻击方式或多 MU 联合攻击前提下,进一步降低算法计算量,进而降低感知设备要求,将同样是今后的研究重点。

参考文献:

- [1] 卢光跃,徐偲,叶迎晖,等. 基于拟合优度的频谱感知技术研究[J]. 电信科学, 2016, 32(5): 52-61.
LU G Y, XU C, YE Y H, et al. Survey on the research of spectrum sensing technologies based on goodness of fit [J]. Telecommunications Science, 2016, 32(5): 52-61.
- [2] ZHANG R, LIANG Y C. Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks [J]. IEEE Journal of Selected Topics in Signal Processing, 2015, 2(1): 88-102.
- [3] 卢光跃,弥寅,包志强,等. 基于特征结构的频谱感知算法[J]. 西安邮电大学学报, 2014, 19(2): 1-12.
LU G Y, MI Y, BAO Z Q, et al. Cooperative spectrum sensing algorithms based on eigenvalue structure of the received signal [J]. Journal of Xi'an University of Posts and Telecommunications, 2014, 19(2): 1-12.
- [4] EBRAHIMZADEH A, NAJIMI M, ANDARGOLI S M H, et al. Sensor selection and optimal energy detection threshold for efficient cooperative spectrum sensing [J]. IEEE Transactions on Vehicular Technology, 2015, 64(4): 1565-1577.
- [5] HAGHIGHAT M, SADOUGH S M S. Cooperative spectrum sensing for cognitive radio networks in the presence of smart malicious users [J]. AEU-International Journal of Electronics and Communications, 2014, 68(6): 520-527.
- [6] SONG Q, HAMOUDA W A. Performance analysis and optimization of multi-selective scheme for cooperative sensing in fading channels [J]. IEEE Transactions on Vehicular Technology, 2016: 1.
- [7] LUAN H, LI O, ZHANG X. Cooperative spectrum sensing with energy-efficient sequential decision fusion rule [C]//2014 23rd Wireless and Optical Communication Conference, May 9-10, 2014, New York, NJ, USA. New Jersey: IEEE Press, 2014: 1-4.
- [8] ZHANG W, GUO Y, LIU H, et al. Distributed consensus-based weight design for cooperative spectrum sensing [J]. IEEE Transactions on Parallel & Distributed Systems, 2015, 26(1): 54-64.
- [9] CHEN R, PARK J M, HOU Y T, et al. Toward secure distributed spectrum sensing in cognitive radio networks [J]. IEEE Communications Magazine, 2008, 46(4): 50-55.
- [10] BAZERQUE J A, GIANNAKIS G B. Distributed spectrum sensing for cognitive radio networks by exploiting sparsity [J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1847-1862.
- [11] MALEKI S, LEUS G, CHATZINOTAS S, et al. To AND or to OR: on energy-efficient distributed spectrum sensing with combined censoring and sleeping [J]. IEEE Transactions on Wireless Communications, 2015, 14(8): 1.



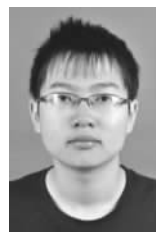
- [12] TEGUIG D, SCHEERS B, NIR V L, et al. Consensus algorithms for distributed spectrum sensing based on goodness of fit test in cognitive radio networks [C]//2015 International Conference on Military Communications and Information Systems, May 18–19, 2015, Cracow, Poland. New Jersey: IEEE Press, 2015: 1-5.
- [13] AMJAD M F, ASLAM B, ZOU C C. Reputation aware collaborative spectrum sensing for mobile cognitive radio networks [C]//2013 Military Communications Conference, November 18–20, 2013, San Diego, California, USA. New Jersey: IEEE Press, 2013: 951-956.
- [14] SUCASAS V, ALTHUNIBAT S, RADWAN A, et al. Lightweight security against combined IE and SSDF attacks in cooperative spectrum sensing for cognitive radio networks [J]. Security & Communication Networks, 2015.
- [15] NGUYEN-THANH N, CIBLAT P, PHAM A T, et al. Attack and surveillance strategies for selfish primary user emulator in cognitive radio network [C]//2014 IEEE Global Conference on Signal and Information Processing, Dec 3–5, 2014, Atlanta, GA, USA. New Jersey: IEEE Press, 2014: 1199-1203.
- [16] 李红宁, 裴庆祺, 李子. 认知无线网络中收敛感知算法安全性检测[J]. 西安电子科技大学学报: 自然科学版, 2014, 41(3): 157-161.
LI H N, PEI Q Q, LI Z. Security detection of the consensus-based spectrum sensing algorithm in cognitive networks [J]. Journal of Xidian University: Natural Science, 2014, 41(3): 157-161.
- [17] ZHOU M, SHEN J, CHEN H, et al. A cooperative spectrum sensing scheme based on the Bayesian reputation model in cognitive radio networks[C]//2013 Wireless Communications and Networking Conference(WCNC), April 7–10, 2013, Shanghai, China. New Jersey: IEEE Press, 2013: 614-619.
- [18] HUO Y, WANG Y, LIN W, et al. Three-layer Bayesian model based spectrum sensing to detect malicious attacks in cognitive radio networks [C]//2015 IEEE International Conference on Communication Workshop, June 8–12, 2015, London, UK. New Jersey: IEEE Press, 2015: 1640-1645.
- [19] SHARIFI A A, MUSEVI NIYA M J. Defense against SSDF attack in cognitive radio networks: attack-aware collaborative spectrum sensing approach [J]. IEEE Communications Letters, 2016, 20(1): 93-96.
- [20] CHEN R, PARK J M J, BIAN K. Robustness against Byzantine failures in distributed spectrum sensing [J]. Computer Communications, 2012, 35(17): 2115-2124.
- [21] SHARIFI A A, GHAZIJAANI H A, NIYA M J M. Secure collaborative spectrum sensing for distributed cognitive radio networks[EB/OL]. (2015–06–20) [2016–08–01]. https://www.researchgate.net/publication/278030010_Secure_Collaborative_Spectrum_Sensing_for_Distributed_Cognitive_Radio_Networks.
- [22] FENG J, ZHANG Y, LU G, et al. Defend against collusive SSDF attack using trust in cooperative spectrum sensing environment [C]//2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, July 16–18, 2013, Melbourne, Australia. New Jersey: IEEE Press, 2013: 1656-1661.
- [23] HYDER C S, GREBUR B, LI X, et al. ARC: adaptive reputation based clustering against spectrum sensing data falsification attacks[J]. IEEE Transactions on Mobile Computing, 2014, 13(8): 1707-1719.
- [24] SAGDUYU Y E. Securing cognitive radio networks with dynamic trust against spectrum sensing data falsification [C]//2014 Military Communications Conference (MILCOM), Oct 1–8, 2014, Baltimore, MD, USA. New Jersey: IEEE Press, 2014: 235-241.
- [25] DU J, WEN X, SHANG L, et al. A byzantine attack defender for censoring-enabled cognitive radio networks [C]//2015 International Conference on Wireless Communications & Signal Processing, Oct 11–13, 2015, Nanjing, China. New Jersey: IEEE Press, 2015: 1-6.
- [26] SHARIFI A A, NIYA J M. Securing collaborative spectrum sensing against malicious attackers in cognitive radio networks[J]. Wireless Personal Communications, 2016: 1-17.
- [27] HAN Y, CHEN Q, WANG J X. An enhanced D-S theory cooperative spectrum sensing algorithm against SSDF attack[C]//2012 75th IEEE Vehicular Technology Conference (VTC Spring), May 6–9, 2012, Yokohama, Japan. New Jersey: IEEE Press, 2012: 1-5.
- [28] CHATTERJEE P S, ROY M. A regression based spectrum-sensing data-falsification attack detection technique in CWSN[C]//2015 IEEE International Conference on Information Technology, Dec 21–13, 2015, Bhubaneswar, India. New Jersey: IEEE Press, 2015: 48-53.
- [29] 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.
- [30] EJAZ W, HASAN N U, KIM H S. Distributed cooperative spectrum sensing in cognitive radio for Ad Hoc networks [J]. Computer Communications, 2013, 36(12): 1341-1349.
- [31] LI H, LIU X, XU L. Analysis of distributed consensus-based spectrum sensing algorithm in cognitive radio networks [C]//2014 10th International Conference on Computational Intelligence and Security, Nov 15–16, 2014, Kunming, China. New Jersey: IEEE Press, 2014: 593-597.
- [32] 王凡, 卢光跃, 弥寅. 基于中值滤波的分布式扩散最小均方算法[J]. 西安邮电大学学报, 2015(5): 34-37.
WANG F, LU G Y, MI Y. An improved distributed diffusion least mean square algorithm[J]. Journal of Xi'an University of

- Posts and Telecommunications, 2015(5): 34-37.
- [33] ZENG K, PAWE C, PRZEMYS A, et al. Reputation-based cooperative spectrum sensing with trusted nodes assistance[J]. IEEE Communications Letters, 2010, 14(3): 226-228.
- [34] BHATTACHARJEE S, DEBROY S, CHATTERJEE M. Trust computation through anomaly monitoring in distributed cognitive radio networks [C]//2011 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Sept 11-14, 2011, Toronto, Canada. New Jersey: IEEE Press, 2011: 593-597.
- [35] ZHANG T, SAFAVI-NAINI R, LI Z. ReDiSen: reputation-based secure cooperative sensing in distributed cognitive radio networks[C]//2013 IEEE International Conference on Communications, June 9-13, 2013, Budapest, Hungary. New Jersey: IEEE Press, 2013: 2601-2605.
- [36] WANG J, CHEN I 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, May 10-12, 2016, Stevenson, WA, USA. New Jersey: IEEE Press, 2016: 1-6.
- [37] WEI Z, TANG H, YU F R. A trust based framework for both spectrum sensing and data transmission in CR-MANETs [C]//2015 IEEE International Conference on Communication Workshop, June 8-12, 2015, London, UK. New Jersey: IEEE Press, 2015: 562-567.
- [38] LIN H, HU J, HUANG C, et al. A secure cooperative spectrum sensing strategy for distributed cognitive radio networks [C]//IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Oct 26-28, 2015, Liverpool, UK. New Jersey: IEEE Press, 2015: 2198-2205.
- [39] LI F, LIU F, ZHU J, et al. Reputation-based secure spectrum situation fusion in distributed cognitive radio networks[J]. Journal of China Universities of Posts & Telecommunications, 2015, 22(3): 110-117.
- [40] CHEN H, ZHOU M, XIE L, et al. Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack [J]. IEEE Transactions on Vehicular Technology, 2016: 1.
- [41] CHEN C, SONG M, XIN C S. A density based scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks [C]//2013 IEEE Global Communications Conference (GLOBECOM 2013), Dec 9-13, 2013, Atlanta, GA, USA. New Jersey: IEEE Press, 2013: 623-628.
- [42] 冯景瑜, 卢光跃, 包志强. 认知无线电安全研究综述[J]. 西安邮电大学学报, 2012, 17(2): 47-52.
- FENG J Y, LU G Y, BAO Z Q. A survey on cognitive radio security [J]. Journal of Xi'an University of Posts and Telecommunications, 2012, 17(2): 47-52.
- [43] 曹龙, 赵杭生, 鲍丽娜, 等. 协作频谱感知及 SSDF 攻击研究[J]. 计算机科学, 2013, 40(S1): 307-310.
- CAO L, ZHAO H S, BAO L N, et al. Research on cooperative spectrum sensing and SSDF attacks [J]. Computer Science, 2013, 40(S1): 307-310.
- [44] 冯景瑜. 协作频谱感知中的 SSDF 攻击及其策略研究 [J]. 电信科学, 2014, 30(1): 67-72.
- FENG J Y. Research on SSDF attack and defense for cooperative spectrum sensing [J]. Telecommunications Science, 2014, 30(1): 67-72.
- [45] VEGI M K. Study of Byzantine attackers and countermeasures in spectrum sensing[J]. International Journal of Health Promotion & Education, 2014, 3(3): 100.
- [46] 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): 1.
- [47] YUCEK T, ARSLAN H. A survey of spectrum sensing algorithms for cognitive radio applications[J]. IEEE Communications Surveys & Tutorials, 2009, 11(1): 116-130.
- [48] SOBRON I, DINIZ P S R, MARTINS W, et al. Energy detection technique for adaptive spectrum sensing[J]. IEEE Transactions on Communications, 2015, 63(3): 617-627.
- [49] BLAZE M, FEIGENBAUM J, STRAUSS M. Compliance checking in the policymaker trust management system [J]. Financial Cryptography, 1998(1465): 254-274.
- [50] MOOD A M, GRATBILL F A. 统计学导论[M]. 北京: 科学出版社, 1978.
- MOOD A M, GRAYBILL F A. Introductory statistics[M]. Beijing: Science Press, 1978.

[作者简介]



卢光跃(1971-),男,西安邮电大学通信与信息工程学院教授,主要研究方向为现代移动通信中信号处理。



苏杭(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频谱感知技术。