

基于防伪码鉴定机制的数据伪造攻击检测方法

李鑫滨, 张 孜, 韩 松, 闫 磊

(燕山大学 工业计算机控制工程河北省重点实验室, 河北 秦皇岛 066004)

摘 要: 在认知无线网络中, 恶意用户会发送虚假信号给融合中心, 使融合中心做出主用户存在的错误判断。针对该问题, 提出一种基于鉴定机制的协作频谱感知方法。为每个认知用户本地检测信息附加防伪码对恶意用户进行识别, 以降低恶意用户对协作频谱感知性能的影响, 同时对防伪码的长度进行优化, 以减小系统的能量消耗, 并将感知效率作为评估感知性能的指标, 达到检测性能和系统开销之间的平衡。仿真结果表明, 在恶意用户存在的情况下, 与传统的 K-out-of-N 方法相比, 该方法有效地提高了系统的感知效率。

关键词: 协作频谱感知; 数据伪造攻击; 鉴定机制; 系统开销; 感知效率

中文引用格式: 李鑫滨, 张 孜, 韩 松, 等. 基于防伪码鉴定机制的数据伪造攻击检测方法[J]. 计算机工程, 2016, 42(8): 112-116.

英文引用格式: Li Xinbin, Zhang Zi, Han Song, et al. Data Falsification Attack Detection Method Based on Anti-counterfeiting Code Identification Mechanism[J]. Computer Engineering, 2016, 42(8): 112-116.

Data Falsification Attack Detection Method Based on Anti-counterfeiting Code Identification Mechanism

LI Xinbin, ZHANG Zi, HAN Song, YAN Lei

(Key Lab of Industrial Computer Control Engineering of Hebei Province, Yanshan University, Qinhuangdao, Hebei 066004, China)

[Abstract] In the Cognitive Radio Network(CRN), Malicious User(MU) can transmit false information to the fusion center, causing the fusion center to make a false decision that the Primary User(PU) is present. In order to solve this problem, a cooperative spectrum sensing algorithm based on identification mechanism is proposed. In this algorithm, anti-counterfeiting codes are attached to each of the local spectrum information to filter out the incorrect information so as to reduce the effect of MU on cooperative spectrum sensing. The anti-counterfeiting code length is also optimized to reduce the system overhead. Further, the sensing efficiency is introduced to evaluate the detection performance of this identification mechanism to achieve balance between detection performance and system overhead. Simulation results demonstrate that compared with the traditional K-out-of-N method, this method improves the sensing efficiency effectively in the presence of MU.

[Key words] cooperative spectrum sensing; data falsification attack; identification mechanism; system overhead; sensing efficiency

DOI: 10.3969/j.issn.1000-3428.2016.08.021

1 概述

随着无线通信技术的发展, 频谱资源匮乏的问题日益显现。传统的固定频谱分配政策已经无法适应未来发展的需要, 而基于动态频谱接入的认知无线电(Cognitive Radio, CR)^[1-2]技术能有效解决频谱资源紧张的问题。作为 CR 的关键技术, 频谱感知可以有效地避免对主用户(Primary User, PU)造成干

扰, 发现频谱空洞进而提高感知效率^[3]。但是在实际中, 由于多径衰落、阴影效应等因素的存在, 严重影响单节点频谱感知的性能。而协作频谱感知可以利用空间分集技术提高检测性能, 是目前最有效的频谱感知方法之一^[4-6]。

但是, 协作频谱感知没有解决认知无线网络(Cognitive Radio Network, CRN)中存在的数据假冒攻击的问题^[7], 即不能有效地检测出认知无线电网

基金项目: 国家自然科学基金资助项目(61172095)。

作者简介: 李鑫滨(1969-), 男, 教授、博士生导师, 主研方向为网络安全、传感器网络; 张 孜, 硕士研究生; 韩 松、闫 磊, 博士研究生。

收稿日期: 2015-07-06 **修回日期:** 2015-08-30 **E-mail:** lixb@ysu.edu.cn

络中存在的恶意用户(Malicious User, MU)。MU 会发送虚假信息给融合中心(Fusion Center, FC),造成错误的感知结果,使融合中心对主用户的存在情况作出错误的判决,从而导致网络频谱利用率的降低。因此,有效地检测出 MU 并且降低 MU 对感知结果的影响是至关重要的。

针对恶意用户仿冒攻击的问题,已有学者做了大量研究。文献[8]表明当认知无线网络中存在 MU 时,系统的感知性能恶化并且频带利用率降低。针对这一问题,文献[9]提出计算每个认知用户的信誉度和一致性因子来判断用户的合法性,从而淘汰恶意用户。文献[10]在文献[9]的基础上,提出了基于信誉度机制的检测方案,即将每个认知用户本地检测与全局检测结果不同的概率作为对手的信誉度来检测出恶意用户。文献[11]提出了利用自适应学习的方法来鉴别恶意用户,去除虚假信息。但是上述的研究均没有考虑信道状态信息在时间上的连续性。为了解决这个问题,文献[12]将 CU 和 MU 分别看作 2 个马尔科夫模型,根据马尔科夫模型中参数的不同检测出 MU。但是这种方法需要很长时间观测 CU 和 MU 的参数,因此,这种方法不适用于时变的认知无线网络。更严重的是这种方法还会将一些合法的认知用户错误地划分为恶意用户从而降低网络性能。除此之外,在文献[13]提出了广义 ESD 方法淘汰恶意次用户,提高协作频谱感知的效率。但是在淘汰恶意次用户的过程中会增加功率消耗和系统开销,并且假设至少有一条频段是空闲的,这种假设是不实际的。此外,这种方法运用软融合的方法对感知信息进行融合,大量感知信息的传输势必会使感知效率降低。文献[14]提出了一种基于能量指纹匹配的检测方案。在该方案中, CU 利用自身的位置分布特征,使用能量检测生成能量指纹,将其作为节点的身份标识,分析不同用户对频谱资源的使用方式,从而实现对仿冒行为的检测,但该检测方案不适用于 MU 发射功率变化的情况。文献[15]提出采用给合法用户加密的方法来鉴别恶意用户,为了提高检测概率采用软融合的方法,但是软融合和密码长度势必会导致能量消耗增加。

为了解决数据伪造攻击的问题,本文研究了恶意用户对协作频谱感知性能的影响,提出采用感知效率作为评估感知性能的指标,重点分析在恶意用户存在的情况下系统的感知效率,并且提出一种鉴别机制来降低恶意次用户的影响,即给每个认知用户都加上一段防伪码来辨别认知用户是否为合法用户。此外,为了解决这种机制带来的额外系统开销,通过优化防伪码的长度来减少系统开销。

2 系统描述

2.1 恶意用户不存在的情况

假设某一认知无线电系统中有 N 个 CR 用户和一个 FC,并且各个 CR 用户独立进行本地频谱感知。此时,第 i 个 CR 用户的频谱感知可以描述为相应的二元假设问题^[16]:

$$x_i(t) = \begin{cases} n_i(t) & H_0 \\ h_i(t)s(t) + n_i(t) & H_1 \end{cases} \quad (1)$$

其中, $x_i(t)$, $n_i(t)$ 分别表示第 i 个 CR 用户接收到的信号和噪声; H_1 和 H_0 分别表示 PU 存在与不存在。假设 PU 存在的概率为 α , 并且 CR 和 FC 之间的报告信道是非理想的, 假设误差概率为 q 。

所有的本地检测信息传递给 FC 之后, FC 依据 K-out-of-N 准则对感知信息进行融合, 则总的判决结果可以表示为:

$$D' = \begin{cases} H_0 & D < K \\ H_1 & D \geq K \end{cases} \quad (2)$$

其中, D 代表本地判决结果为 H_1 的认知用户的个数; K 为整数。当 $D < K$ 时, 本地判决结果为 H_0 , 即主用户不存在; 反之判决结果为 H_1 , 即主用户存在。显然, 当 $K=1$ 时为 OR 准则; 当 $K=N$ 时为 AND 准则。

在这种判决准则下, 虚警概率可以表示为:

$$Q_f = \sum_{n=K}^N \binom{N}{n} (P_f(1-q) + (1-P_f)q)^n \cdot ((1-P_f)(1-q) + P_f q)^{N-n} \quad (3)$$

其中, P_f 代表本地频谱感知的虚警概率。漏检概率可以表示为:

$$Q_m = 1 - \sum_{n=K}^N \binom{N}{n} ((1-P_m)(1-q) + P_m q)^n \cdot (P_m(1-q) + (1-P_m)q)^{N-n} \quad (4)$$

其中, P_m 代表本地频谱感知的漏检概率。

2.2 恶意用户存在的情况

本文假设融合中心收到的所有结果都是可信的, 但是在实际中, 认知无线网络中会存在数据仿冒攻击, 即恶意用户传递不可靠的信息给融合中心, 导致错误的检测结果。因此, 恶意用户的存在会降低认知无线网络的频谱利用率。

在某一认知无线网络中, 假设存在 M 个恶意用户, 恶意用户的数目可以根据文献[17]方法确定。并且所有的恶意用户都认为主用户存在。在这种情况下, 当 $M \geq K$ 时, 融合中心总会得到主用户存在的判决结果, 因此, 本文考虑 $M < K$ 的情况。在恶意用户存在的情况下, 虚警概率可以表示为:

$$Q_{f,M} = \sum_{n=K-M}^N \binom{N}{n} (P_f(1-q) + (1-P_f)q)^n \cdot ((1-P_f)(1-q) + P_f q)^{N-n} \quad (5)$$

漏检概率可以表示为:

$$Q_m = 1 - \sum_{n=K}^N \binom{N}{n} ((1 - P_m)(1 - q) + P_m q)^n \cdot (P_m(1 - q) + (1 - P_m)q)^{N-n} \quad (6)$$

从式(5)中可以看出,当 M 增大时,虚警概率会随之增大,表明恶意用户的存在减少了频谱利用的机会。

2.3 感知效率

本文以感知效率作为评价系统感知性能的函数,以有效地权衡检测性能和网络开销。感知效率的定义为系统的吞吐量与感知信息位数的比值,即:

$$\eta = \frac{(1 - \alpha)(1 - Q_{f-M})RT}{B} \quad (7)$$

其中, R 代表数据传输速度; T 代表传输时间; B 代表感知信息的位数。将式(5)代入式(7)可以得到:

$$\eta = (1 - \alpha) \left(1 - \sum_{n=K-M}^N \binom{N}{n} \cdot (P_f(1 - q) + (1 - P_f)q)^n ((1 - P_f)(1 - q) + P_f q)^{N-n} \right) RT/B \quad (8)$$

从式(8)可以看出,在数据传输速度 R 、传输时间 T 、感知信息位数 B 以及主用户存在的概率 α 不变的情况下,随着 M 的增大,虚警概率将会增大,从而使感知效率降低。

3 基于鉴定机制的频谱感知方法

3.1 性能分析

为了降低恶意用户对感知效率的影响,采用给认知用户加防伪码的方法鉴别来自恶意用户的虚假信息。在鉴定的过程中,防伪码将会附加到认知用户的本地检测结果上,与本地检测结果一并传送

$$\delta = \frac{(1 - \alpha) \left(1 - \sum_{i=0}^M \binom{M}{i} (2^{-A})^i (1 - 2^{-A})^{M-i} Q_{f-M}(N, i) \right) RT}{1 + A} \quad (15)$$

从式(15)可以看出,通过本文提出的鉴别机制,可以有效减少来自恶意用户的虚假信息,从而降低恶意用户对检测性能的影响,同时 A 的大小直接影响感知效率。从式(15)也可以看出, A 与 δ 并不是简单的线性关系, δ 的值不会随着 A 的增大而一直增大。这是因为, A 的值越大,恶意用户被误认为合法用户的概率就会越小,会增加合法用户接入空闲

给融合中心。融合中心通过检查每个数据包的防伪码来确定接收到的来自认知用户信息的真实性。恶意用户没有正确的防伪码,为了达到影响网络通信的目的,恶意用户会模仿合法用户的行为,随机生成一系列防伪码,生成的防伪码与合法用户的防伪码的长度相同。

假设防伪码的长度为 A 比特, P_r 代表恶意用户被融合中心鉴定为合法用户的概率,则:

$$P_r = 2^{-A} \quad (9)$$

在采用鉴别机制的情况下,可以推导出虚警概率和检测概率分别为:

$$Q_{f-MA} = \sum_{i=0}^M \binom{M}{i} P_r^i (1 - P_r)^{M-i} Q_{f-M}(N, i) \quad (10)$$

$$Q_{m-MA} = 1 - \sum_{i=0}^M \binom{M}{i} P_r^i (1 - P_r)^{M-i} \cdot (1 - Q_{m-M}(N, i)) \quad (11)$$

其中, $Q_{f-M}(N, i)$ 和 $Q_{m-M}(N, i)$ 可以由式(5)和式(6)得到,代表在一个认知无线网络中有 N 个合法用户和 i 个恶意用户,即:

$$Q_{f-M}(N, i) = \sum_{n=K-i}^N \binom{N}{n} (P_f(1 - q) + (1 - P_f)q)^n \cdot ((1 - P_f)(1 - q) + P_f q)^{N-n} \quad (12)$$

$$Q_{m-M}(N, i) = 1 - \sum_{n=K-i}^N \binom{N}{n} ((1 - P_m)(1 - q) + P_m q)^n (P_m(1 - q) + (1 - P_m)q)^{N-n} \quad (13)$$

在这种情况下,频谱感知效率可以表示为:

$$\delta = \frac{(1 - \alpha)(1 - Q_{f-MA})RT}{1 + A} \quad (14)$$

将式(9)、式(10)代入式(14)可以得到:

频谱的机会。但是,与此同时也会增加认知无线电网的能量消耗。所以,要限制防伪码的长度,这样就需要对 A 的值进行优化。

3.2 A 值大小的优化

由于 A 代表防伪码的长度,因此 A 必须是整数,即 A 的取值是不连续的,为了求解问题的方便,先将式(15)的优化问题转化为下面的无约束优化问题:

$$\max f(x) = \frac{(1 - \alpha) \left(1 - \sum_{i=0}^M \binom{M}{i} (2^{-x})^i (1 - 2^{-x})^{M-i} Q_{f-M}(N, i) \right) RT}{1 + x} \quad (16)$$

但是从式(16)中难以求出 A 的具体数学表达式,并且通过导数求极值的复杂度比较高。由于函数 $f(x)$ 具有一阶连续导数,因此考虑用最速下降法

求解,即沿着梯度上升的方向进行一维搜索,求得 $f(x)$ 的极大值。梯度方向通过对函数求导得到,步长由线性搜索方法来确定。

方法步骤如下所示。

步骤 1 给定初点 $x^{(1)} = 1$, 允许误差 $\varepsilon = 0.001$, 置 $k = 1$ 。

步骤 2 计算搜索方向 $d^{(k)} = \nabla f(x^{(k)})$ 。

步骤 3 若 $\|d^{(k)}\| \leq \varepsilon$, 则停止计算; 否则, 从 $x^{(k)}$ 出发, 沿 $d^{(k)}$ 进行一维搜索, 求 λ_k , 使 $f(x^{(k)} + \lambda_k d^{(k)}) = \max_{\lambda \geq 0} f(x^{(k)} + \lambda_k d^{(k)})$ 。

步骤 4 令 $x^{(k+1)} = x^{(k)} + \lambda_k d^{(k)}$, 置 $k = k + 1$, 转步骤 2。

通过最速下降法得到满足精度要求的近似最优解 x , 并对 x 取整, 得到 A 。

4 仿真结果与分析

对本文提出的方法进行仿真, 假设认知用户的个数 $N = 10$, 主用户存在的概率 $\alpha = 0.5$, 本地虚警概率 $P_f = 0.1$, 本地漏检概率 $P_m = 0.2$ 。数据传输速度 $R = 10$ Kb/s。

图 1 给出了恶意用户数量 M 不同的条件下, 系统感知效率与 K 的关系曲线。从图 1 可以看出, K 值不同, 感知效率不同, 因此, K 的大小对感知效率有很大的影响。由图 1 还可以看出, 随着恶意用户数量 M 的增大, 系统感知效率明显降低。当 $M \geq K$ 时, 感知效率减为 0。在这种情况下, 融合中心将会做出错误的判断, 即认为主用户总是存在, 合法的认知用户不能接入空闲频谱, 造成频谱资源的浪费, 降低频谱利用率。

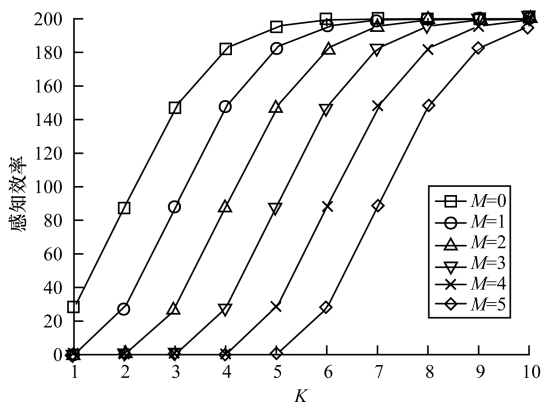


图 1 不同 M 值下的 δ - K 关系曲线

图 2 为在 $K = 4$, M 不同的条件下, 采用鉴定机制的感知效率随着防伪码长度 A 的变化情况。由图 2 可以看出, 随着 M 的增大, 感知效率降低。 A 越大, 融合中心被虚假信息误导作出错误判断的概率越低, 但是由图 2 可以看出, 感知效率并没有随着 A 的增大而一直增加。因此, 找到最优的 A 值使感知效率最大是非常重要的。

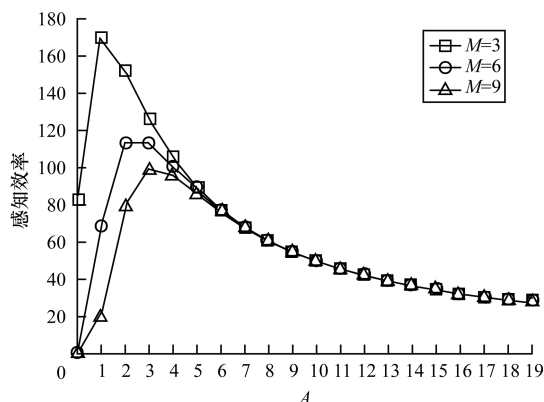


图 2 不同 M 值下的 δ - A 关系曲线

表 1 为利用最速下降法求得的近似最优解 x 与通过图 2 得到的实际最优解 A 的比较, 从表 1 的数据可以看出, 对利用最速下降法求得的理论最优值 x 取整之后得到的数据与实验方法得到的实际最优值是非常接近的, 因此, 通过最速下降法寻优是可行的。

表 1 理论最优值与实际最优值的比较

M	理论最优值 x	实际最优值 A
4	1.301	1
5	1.710	2
6	2.032	2
7	2.309	2
8	2.554	3
9	2.769	3

图 3 给出了在 A 取最优值, $K = N/2$ 的情况下, 本文方法与传统方法相比感知效率提高的比例。由于当 $M \geq K$ 时, 融合中心将误认为主用户存在, 无法检测出频谱空洞, 因此在图 3 中只考虑 $M < K$ 的情况。从图 3 中可以看出, 随着 M 的增大, 频谱感知效率提高的比例增大。这是因为通过采用鉴定机制和防伪码长度的最优值, 可以有效减少由恶意用户带来的效率损失。

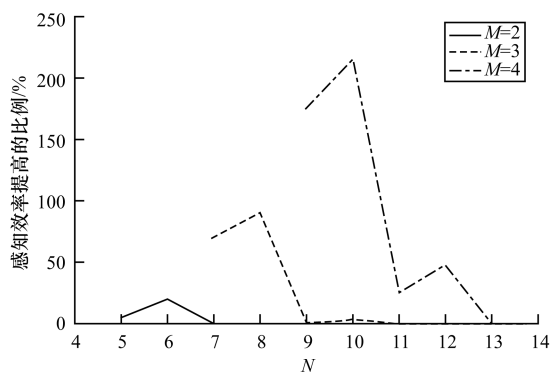


图 3 本文方法与传统方法相比感知效率提高的比例

5 结束语

本文针对认知无线网络中存在恶意用户的情况,提出一种基于防伪码鉴定机制的数据伪造攻击检测方法。该方法为每个用户的感知信息都附加了一段防伪码来删除虚假信息,同时,为降低系统能耗,对防伪码长度进行了优化。仿真结果表明,该方法能有效提高存在恶意用户时网络的感知效率。本文方法是在假定报告信道误码率为定值的情况下进行的,时变误码率情况下认知无线网络中恶意用户的检测将是下一步的研究方向。

参考文献

- [1] Haykin S. Cognitive Radio: Brain-empowered Wireless Communications[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(2): 201-220.
- [2] Mitola J, Maguire J G Q. Cognitive Radio: Making Software Radios More Personal[J]. IEEE Personal Communications, 1999, 6(4): 13-18.
- [3] Ghasemi A, Sousa E S. Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-offs[J]. IEEE Communications Magazine, 2008, 46(4): 32-39.
- [4] Chen Qian, Motani M, Wong W C, et al. Cooperative Spectrum Sensing Strategies for Cognitive Radio Mesh Networks[J]. IEEE Journal of Selected Topics in Signal Processing, 2011, 5(1): 56-67.
- [5] Letaief K, Zhang Wei. Cooperative Communications for Cognitive Radio Networks[J]. Proceedings of the IEEE, 2009, 97(5): 878-893.
- [6] Mu Hua, Tugnait J K. Joint Soft-decision Cooperative Spectrum Sensing and Power Control Multiband Cognitive Radios[J]. IEEE Transactions on Signal Processing, 2012, 60(10): 5334-5346.
- [7] Burbank J L. Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security[C]//Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications. Washington D. C., USA: IEEE Press, 2008: 1-7.
- [8] Chen Ruiliang, 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.
- [9] Wang Wenkai, Li Husheng, Sun Yan, et al. Securing Collaborative Spectrum Sensing Against Untrustworthy Secondary Users in Cognitive Radio Networks[J]. EURASIP Journal on Advances in Signal Processing, 2009, 2010(1): 1-15.
- [10] Rawat A S, Anand P, Chen H, et al. Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks[J]. IEEE Transactions on Signal Processing, 2011, 59(2): 774-786.
- [11] Vempaty A, Agrawal K, Varshney P, et al. Adaptive Learning of Byzantines' Behavior in Cooperative Spectrum Sensing[C]//Proceedings of IEEE Wireless Communications and Networking Conference. Washington D. C., USA: IEEE Press, 2011: 1310-1315.
- [12] He Xiaofan, Dai Huaiyu, Ning Peng. HMM-based Malicious User Detection for Robust Collaborative Spectrum Sensing[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(11): 2196-2208.
- [13] Srinu S, Sabat S L. Cooperative Wideband Sensing Based on Cyclostationary Features with Multiple Malicious User Elimination[J]. AEU—international Journal of Electronics and Communications, 2013, 67(8): 702-707.
- [14] 逢德明, 胡 昱, 徐 明. 基于能量指纹匹配的无线认知网络仿冒主用户攻击检测[J]. 计算机科学, 2011, 38(3): 28-33.
- [15] Zhang Linyuan, Wu Qihui, Ding Guoru, et al. Performance Analysis of Probabilistic Soft SSDF Attack in Cooperative Spectrum Sensing[J]. EURASIP Journal on Advances in Signal Processing, 2014, (1): 1-9.
- [16] Zhang Wei, Mallik R K, Letaief K. Optimization of Cooperative Spectrum Sensing with Energy Detection in Cognitive Radio Networks[J]. IEEE Transactions on Wireless Communications, 2009, 8(12): 5761-5766.
- [17] Kaligineedi P, Khabbazi M, Bhargava V K. Malicious User Detection in a Cognitive Radio Cooperative Sensing System[J]. IEEE Transactions on Wireless Communications, 2010, 9(8): 2488-2497.

编辑 刘 冰

(上接第 111 页)

- [11] Guo Linke, Zhu Xiaoyan, Zhang Chi, et al. Privacy-preserving Attribute-based Friend Search in Geosocial Networks with Untrusted Servers[C]//Proceedings of GLOBECOM'13. Washington D. C., USA: IEEE Press, 2013: 629-634.
- [12] Guo Linke, Zhang Chi, Sun Jinyuan, et al. PAAS: A Privacy-preserving Attribute-based Authentication System for eHealth Networks[C]//Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems. Washington D. C., USA: IEEE Press, 2012: 224-233.
- [13] Sun Wenhai, Yu Shucheng, Lou Wenjing, et al. Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud[C]//Proceedings of IEEE INFOCOM'14. Washington D. C., USA: IEEE Press, 2014: 226-234.
- [14] 吕志泉, 洪 澄, 张 敏, 等. 面向社交网络的隐私保护方案[J]. 通信学报, 2014, 35(8): 23-32.
- [15] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]//Proceedings of CRYPTO'01. Berlin, Germany: Springer-Verlag, 2001: 213-229.

编辑 刘 冰