认知无线电网络中频谱感知安全的研究进展

汪晓睿[1],刘 全[2]
(1.海军计算技术研究所,北京 100841;
2.海军工程大学 通信工程系,湖北 武汉 430033)

摘 要:频谱感知是认知无线电网络中的核心功能,它的引入可使次用户在不干扰主用户的前提下实现对授权频段的伺机接入,然而,同时也给网络带来了许多安全方面的新隐患。该文对频谱感知安全的最新研究进展进行了综述,针对物理层的伪装主用户攻击,分析了两种主流解决思路的可行性。针对链路层的篡改感知数据攻击,分别在信息融合式和分布式两种不同的感知场景下,归纳并比较了几种典型抗攻击策略的优劣。在此基础上,明确了下一步的主要研究方向。

关键词:认知无线电;频谱感知;感知安全;伪装主用户攻击;篡改感知数据攻击
中图分类号:TN92 **文献标识码**:A **文章编号**:1673-629X(2011)12-0155-05

A Survey on Spectrum Sensing Security Issues in Cognitive Radio Networks

WANG Xiao-rui[1],LIU Quan[2]
(1. Naval Computing Technology Institute,Beijing 100841,China;
2. Department of Communication Engineering,Naval University of Engineering,Wuhan 430033,China)

Abstract:In CRNs,spectrum sensing is the core functionality,and with the help of it, the secondary users are allowed to access the authorized spectrum bands in an opportunistic manner,without causing any interference to the primary users. However,it also brings in some new security threats. In this paper,the recent advances of security issues in CRNs are surveyed. For the primary user emulation attacks in the physical layer,the feasibility of two mainstream solutions is analyzed. For the spectrum sensing data falsification attacks in the link layer,the performances of several typical anti-attack strategies are summarized and compared,in the information-fusion-based CSS scenario and the decentralized CSS scenario,respectively. Furthermore,the main directions for the future research are viewed.

Key words:cognitive radio;spectrum sensing;sensing security;primary user emulation attack;spectrum sensing data falsification attack

0 引 言

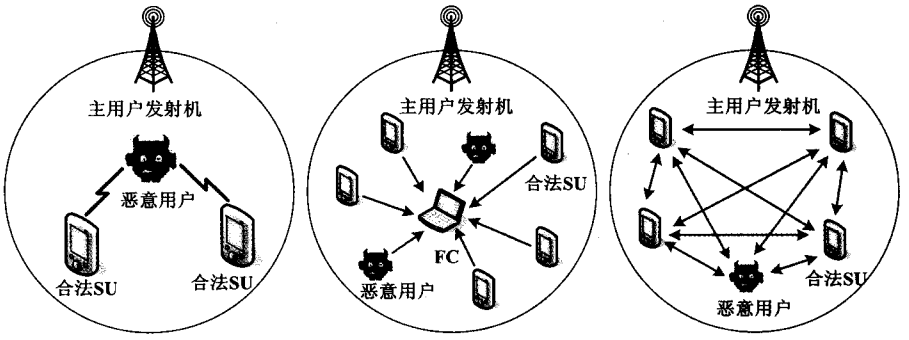
在传统的"条块分割"式静态频谱分配体制下,大量的授权频段中存在着极大的"浪费"。为了将这些浪费的频谱空洞有效地进行"二次利用",认知无线电(Cognitive Radio, CR)技术应运而生。近十年来,随着CR技术研究的不断推进,构建新型的认知无线电网络(CR Network, CRN)已经势在必行。然而,CRN在大大改善频谱效率的同时,也面临着许多安全方面的隐患[1]。一方面,由于无线信道的开放性,使得CRN中同样也存在着许多传统的网络安全问题[1,2];另一方面,由于CRN的伺机接入共享模型需要频谱感知等新功能的支持,这给敌方或恶意用户也带来了更多的可乘之机,利用这些新特性而发动许多CRN特有的攻击形式,可造成对主用户系统的干扰或者整体频谱效率的降低,导致网络运行紊乱甚至瘫痪[1,2]。因此,如何妥善解决CRN中各种潜在的安全威胁,是它能否最终走向实用化及商用化的关键所在,同时也是其应用于未来军事战场的必要前提。

文献[1~4]对CRN中潜在的各种安全问题进行了总结。其中,直接与频谱感知功能相关的安全威胁主要可分为两类[5],分别称作伪装主用户(Primary User Emulation, PUE)[6,7]攻击和篡改感知数据(Spectrum Sensing Data Falsification, SSDF)攻击[6]。

伪装主用户(PUE)攻击是CRN物理层中将面临的主要安全问题[6,7],它对单用户的本地频谱感知以及多用户的频谱感知协作都具有极大的威胁[8]。如图1(a)所示,在这一类攻击中,敌方向网络内发送与主用户信号特征类似的干扰信号,使得次用户检测时误以为当前信道被占用,导致大量可用频谱机会浪费,各种业务无法顺利展开。对于协作频谱感知(Coopera-

收稿日期:2011-05-04;**修回日期**:2011-08-16
基金项目:国家863计划资助项目(2009AAJ208, 2009AAJ116)
作者简介:汪晓睿(1984-),男,湖北黄石人,工程师,硕士,研究方向为认知无线电网络、网络安全、密码学。

tive Spectrum Sensing, CSS)而言,除了面临 PUE 攻击之外,大部分 CSS 方案中要求具备的感知信息融合或者局部信息交互更容易受到敌方或恶意节点的攻击,而且这些攻击通常都是通过恶意篡改本地感知结果来实现的,所以被统称为篡改感知数据(SSDF)攻击[6]。如图 1(b)所示,在信息融合式 CSS 场景中,敌方或恶意用户可以控制合法次用户向融合中心发送错误或者混乱的感知决策/数据,从而影响最终的融合判决结果。类似地,在分布式 CSS 场景中,同样也面临着严重的 SSDF 攻击[9]。如图 1(c)所示,在分布式 CSS 中,没有全局信息融合中心和通用控制信道,仅依靠相邻次用户之间的局部感知信息交互迭代使网络整体的感知状态趋于一致,然后各次用户根据最终的迭代状态独立地进行判决。因此,一旦敌方或者恶意用户入侵 CRN,这种局部信息交互过程很可能成为主要的攻击对象。



(a) PUE 攻击 (b) 融合式CSS中的SSDF 攻击 (c) 分布式CSS中的SSDF 攻击

图 1 频谱感知中的安全威胁示意图

1 PUE 攻击及其抵抗策略

PUE 攻击主要是针对物理层频谱感知技术的缺陷,通过模拟主用户信号的特征进行恶意频谱干扰,使合法次用户错失频谱机会。按照具体攻击目的不同,PUE 攻击又可细分为自私型和恶意型两种形式[6],前者旨在与合法次用户竞争更多的频谱接入机会,攻击者一旦检测到频谱空洞,则立即发动 PUE 攻击阻止其它合法次用户接入该"空洞",从而使自身占用的频谱资源最大化;而后者则是以循环方式在多频段上发射伪造的主用户信号,其主要目的仅在于阻止合法次用户正常通信。为了抵抗 PUE 攻击,首先必须快速而准确地区分主用户信号和干扰信号,目前主要有两种可行的思路:

(1)信号特征检测。这种思路主要是根据主用户信号的一些隐蔽特征,如导频同步信号、数字水印信息[3]等,研究可行的特征检测技术来识别主用户信号的存在性,典型的如:循环特征检测[3]、匹配滤波检测[3]等。但是这些方法的通用性并不强,因为很多情况下,合法次用户本身也很难获取主用户的先验信息;反而,如果敌方通过某些手段窃取了主用户信号的特征,那么这种抵抗策略将完全失效。

(2)主信号源定位防御机制。这种思路最早是由 Chen Ruiliang 等人于 2008 年提出来的[7],由于很多情况下,尤其是在 TV 发射系统中,攻击者很难同时模拟主用户的发送位置和能量等级,所以可通过定位信号源位置进一步确认信号检测的初步结果,从而区分有效信号和干扰信号[6,7]。在该防御机制下,比较棘手的问题是信号源定位。尽管定位算法目前已有很多相关研究,但是由于 CRN 的特殊性,次用户始终处于从属地位,对信号源的定位必须是非交互式的,即不可能与信号发送方有任何的信息交互。因此,这种思路在细节实现方面仍具有较大的挑战性,现有文献中主要提及了三种解决办法[7]:

①距离比检验技术,即通过一对位置校验器(Location Verifier, LV)得到接收信号强度的测量值来校验发射机的位置,这种技术可以快速确定信号源是否为 TV 发射塔,但其有效性受到传输模型精确度的影响,尤其是当授权主系统改变时,所使用的传输模型就需要相应调整;

②距离差校验技术,该技术利用了信号源与 LV 距离不同则信号到达时相位不同的特性,将相位差转换为时间差,进而转化为距离差,虽然这种技术受环境影响较小,但是需 LV 间的严格时间同步(精确到几百纳秒),故建设成本非常高;

③基于接收信号强度的"快照"技术,该技术通过部署一个传感器网络来得到整个 CRN 的 RSS 测量值的一幅快照,从而获得特定时刻的全网信号源分布图,故可同时定位多个信号源的位置,有效地发现多个恶意 PUE 攻击节点,然而这种方法仅限于 TV 系统的场景,在其它授权频段的推广较难,而且实施成本较高。

此外,在最新的研究进展中,Li Husheng 等人提出了一种类似随机跳频的 PUE 抵抗机制[10],次用户随机选择感知信道进行伺机接入以避开攻击,然后在未知环境下,以对抗性多臂博弈问题的求解方法设计最优的抵抗策略。

2 信息融合式 CSS 场景中的抗 SSDF 攻击策略

●在信息融合式 CSS 场景中,按照攻击目的不同,SSDF 攻击可大体分为以下 3 种形式[6,9]:

(1)自私型攻击(Selfish Attack, SFA),主要是指恶意用户始终向融合中心(Fusion Center, FC)发送决策'1',使 FC 误以为当前信道被占用,从而导致大量空闲频谱资源被浪费或被敌方侵占;

(2)干扰型攻击(Interference Attack, IFA),即恶意用户始终向 FC 上报决策'0',使 FC 误以为信道空闲而通知次用户盲目发射造成对主用户干扰;

(3)混乱型攻击(Confusing Attack, CFA),恶意用户以一定的策略随机向 FC 报告感知结果,时对时错,造成 FC 的决策融合混乱。

●目前,具有抵抗 SSDF 攻击能力的信息融合式 CSS 方案并不多见,现有文献中给出的抵抗性策略大体可分为三类:

(1)基于声望的融合策略[11~14]。这类抵抗策略通常需要根据历史决策,计算各次用户本地感知的可信度,然后以一定的方式整合到信息融合过程中。例如,文献[11]提出了加权序贯检测方案,该方案依据各协作次用户的本地决策信息与 FC 决策的比较结果,按一定的规则动态调整各用户的融合权重,将判决不一致的用户的融合权重逐渐降低,从而减小其对融合过程的不利影响;文献[13]在此基础上做了一些改进,给出了新的权值更新算法,进一步提高了检测性能,但没有考虑感知信道中多径/阴影衰落效应的影响;文献[12]提出了一种改进的基于声望加权的联合似然比检测方案,仅以确定的可靠节点的感知信息进行联合 LRT 检测,以其融合判决结果为参考,计算其它次用户的声望,由此判断它们是否可列入可靠节点集合,这种方案的问题在于没有明确如何选择已知的可靠节点。

(2)异常节点检测及剔除策略。在这类策略中,FC 通过一定的筛选手段检测异常的感知决策或数据,然后将它们从信息融合过程中直接剔除。例如,文献[15]提出了一种基于数据挖掘理论的异常节点检测算法,FC 通过比较多个次用户感知决策之间的欧式距离或汉明距离,计算不同次用户的可疑度水平,然后据此剔除潜在的异常信息再进行融合判决;而文献[16]则是在一定时间窗内比较各次用户的本地决策与 FC 的最终决策,找出并剔除行为异常的用户。这类抵抗策略在攻击形式多变、SNR 较低等恶劣条件下仍具有较高的稳健性;但是它们通常需要一定的迭代过程,故其计算复杂度和时间开销一般较大。

(3)基于节点聚类或分簇的融合策略。这类策略根据节点位置、信道衰落特性等信息将次用户进行分组(或分簇),然后在各组内分别完成一定的信息筛选、融合及判决,再将各组的判决结果进行融合并做出最终决策[17,18]。与前两类抵抗策略相比,这类策略的主要不同在于:各协作次用户的融合权重早在融合前就已经确定了,不需要将次用户的决策与最终决策进行比较。最典型的如文献[18]给出的方案,先根据各节点的位置信息进行分簇,然后在每一簇内比较各次用户的能量检测数据,将超过一定门限的异常节点剔除,再进行线性数据加权融合。然而,当异常节点攻击较为隐蔽时,该方法的稳健性并不强,且由于最终判决门限是固定的,故其对系统参数变化的适应性较差。

3　分布式 CSS 场景中的抗 SSDF 攻击策略

现有的大部分 CSS 方案都是建立在全局信息融合的基础之上,因此,需要特定的基站或者融合中心通过通用控制信道收集所有协作次用户的本地感知数据或决策[5]。但是在许多分布式网络中,这些信息融合式 CSS 方案并不实用,因为各次用户的通信距离和范围都十分有限,很难找到一个与所有协作次用户都能进行信息交互的节点充当融合中心,而且通用控制信道的设计也存在较大的难度[3]。

针对此问题,文献[19]首次将一致性的概念引入到分布式 CRN 中,提出了一种一致性 CSS 方案,该方案将分布式协作频谱感知建模为一个典型的多主体协作问题,整个网络等效为一个连通图 $G=(V,E)$,其中,$V=\{1,2,\cdots,N\}$ 表示顶点(即所有次用户)集合,E 表示所有边(即次用户间的链路)集合[19]。感知过程分为三步,如图 2 所示,首先,各次用户分别以能量检测算法进行本地频谱感知;然后,将本地检测结果作为初始状态,与各自的邻接用户进行信息交互迭代,其中任意第 $i(i\in[1,N])$ 个次用户的初始状态记为 $x_i(0)$;最后,依据各自的最终迭代状态分别独立地做出判决。针对第二步的信息交互迭代过程,文献[19]给出了最大度迭代规则:

$$x_i(k+1)=x_i(k)+\varepsilon_0\sum_{j\in Ne_i(k)}(x_j(k)-x_i(k)) \quad (1)$$

其中,k 表示迭代计数;$x_i(k)$ 和 $x_i(k+1)$ 分别表示第 i 个次用户在当前时刻和下一时刻的感知状态;$Ne_i(k)$ 表示第 i 个次用户的邻接点集合;ε_0 表示迭代的步进值,且必须满足 $0<\varepsilon_0<1/\Delta$,$\Delta=\mathrm{Max}\{d_i \mid i\in V\}$,$d_i$ 为次用户 i 的邻接点个数。

由于受到感知时间的限制,迭代次数必将存在一定的上限,即 $k<T_c$。当 $k\geq T_c$ 时,各次用户将被迫终止信息交互,并分别根据各自的最终迭代状态 $x_i(T_c)$ 做出最终决策 D_i,即

$$D_i=\begin{cases}1, & x_i(T_c)>\lambda_c\\ 0, & \text{otherwise}\end{cases} \quad (2)$$

其中,λ_c 表示统一设置的判决门限。理想条件下,只要 T_c 足够宽裕,则所有次用户的最终状态都将趋于一致,并渐进收敛于初始平均值[5]:

$$x_i(T_c) \to x^* = \frac{1}{N}\sum_{i=1}^{N} x_i(0), \text{as } T_c \to \infty \quad (3)$$

综上分析,该方案的独特之处在于:仅通过邻接点之间进行多次信息交互后就能使所有次用户状态趋于一致,而无需任何集中控制或全局信息融合[19]。

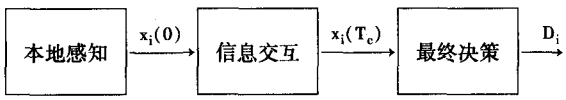


图 2 一致性协作频谱感知方案

然而,这种一致性 CSS 方案也面临着多种潜在的安全威胁。在物理层,PUE 攻击[6,7]是其将要面临的主要干扰形式;而在链路层,相邻用户之间的局部信息交互过程更容易受到敌方或恶意用户的攻击,鉴于这些攻击也是通过恶意篡改本地感知状态来实现的,所以也被统称为 SSDF 攻击[6]:

(1)自私型攻击(SFA),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,使邻接用户误以为当前信道被占用,从而使大量空闲频谱资源被浪费或被敌方侵占;

(2)干扰型攻击(IFA),即恶意用户在信息交互过程中始终发送相对较低的状态值,使其它用户误以为信道空闲而盲目发射,从而造成对主用户的干扰;

(3)混乱型攻击(CFA),是指恶意用户向外以一定的概率随机发送正常状态和恶意状态,使其它用户的迭代过程发生紊乱,从而导致整个网络的状态始终无法趋于一致。

目前,针对分布式 CSS 安全问题的研究尚处在起步阶段,文献[9]在一致性 CSS 方案的基础上引入了一定的抗攻击策略,直接将感知状态与邻接区域内平均值偏差最大的节点从各次用户的邻接点集合中剔除,即

$$Ne_i(k) = Ne_i(k)/j_0 \quad (4)$$

其中,

$$j_0 = \arg\max_{j \in Ne_i(k)} \{x_j(k) - u_i(k)\},$$

$$u_i(k) = \frac{x_i(k) + \sum_{j \in Ne_i(k)} x_j(k)}{1 + d_i(k)}$$

然后再按式(1)所示的规则进行信息交互迭代[9]和最终判决。然而,从仿真结果来看,该方案的有效性十分有限,难以抵抗多种形式的 SSDF 攻击,尤其是对 CFA 攻击最为敏感,几乎没有任何抵抗能力,这主要是因为该方案对邻接用户的筛选过于粗暴,使网络中合法次用户的信息交互链路迅速减少,不仅很难将真正的攻击节点剔除,反而中断了许多合法次用户之间的正常信息交互[4]。此外,以上两种一致性 CSS 方案在迭代过程中都需要预知网络的最大度数等先验知识,而这在实际中往往是很困难的。针对这些问题,文献[5]提出了一种改进的一致性 CSS 方案,主要进行了两方面改进:一是在信息交互迭代中引入了更为全面而稳健的邻接点筛选策略;二是利用基于 Metropolis 权重矩阵的迭代规则替代了最大度迭代算法,使各次用户无需网络的任何先验知识即可完成协作。仿真实验的结果显示,与前两种一致性 CSS 方案相比,这种改进方案在任意一种 SSDF 攻击条件下的稳健性均有明显的增强。

4 结束语

文中总结了 CRN 中频谱感知安全问题的最新研究进展,重点对其中涉及的两种主要的安全威胁分别进行了详细讨论,归纳并比较了这两类攻击的主要抵抗策略,并分析了其不足之处。有待下一步研究的重点问题包括:

(1)研究更隐蔽、更可靠的信号特征提取算法,以尽可能地避开 PUE 攻击;

(2)在无法获取主用户先验知识的情况下,重点解决其中的非交互式信号源定位问题,从而更有效地区分主用户和 PUE 攻击用户;

(3)针对信息融合式 CSS 场景,着力研究恶意用户的筛选以及加权信息融合策略,以提高信息融合的稳健性,并尽可能地减少由此带来的额外计算开销以及对正常融合过程的不利影响;

(4)针对分布式 CSS 场景,重点研究一致性算法的收敛性和稳健性,尤其是在主用户特性变化较快的应用场景中,一致性算法的收敛速度能否保证各次用户及时跟踪主用户的特性变化是需要特别关注的重点问题;

(5)研究各种智能型感知攻击策略及其相应的抵抗策略。

参考文献:

[1] Zhang X, Li C. Constructing secured cognitive wireless networks: experiences and challenges[J]. Wireless Communications and Mobile Computing, 2010, 10(1): 50-69.

[2] Leon O, Hernandez-Serrano J, Soriano M. Securing cognitive radio networks[J]. International Journal of Communication Systems, 2010, 23(5): 633-652.

[3] 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.

[4] 刘 全. 认知无线电网络中的频谱感知技术研究[D]. 武汉:海军工程大学, 2011.

[5] Liu Q, Gao J, Guo Y, et al. Attack-proof cooperative spectrum sensing based on consensus algorithm in cognitive radio networks[J]. KSII Transactions on Internet and Information Sys-

tems,2010,4(6): 1042-1062.

[6] Chen R, Park J, Hou Y T, et al. Toward secure distributed spectrum sensing in cognitive radio networks[J]. IEEE Communications Magazine,2008,46(4):50-55.

[7] Chen R, Park J, Reed J H. Defense against primary user emulation attacks in cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications,2008,26(1):25-37.

[8] Peng Q, Cosman P C, Milstein L B. Optimal sensing disruption for a cognitive radio adversary[J]. IEEE Transactions on Vehicular Technology,2010,59(4):1801-1810.

[9] Yu F R, Tang H, Huang M, et al. Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios [C]//IEEE Military Communications Conference, MILCOM. Boston, USA: IEEE, 2009:1-7.

[10] Han Z, Li H. Blind Dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems with unknown channel statistics[C]//IEEE International Conference on Communications, ICC. Cape Town, South Africa: IEEE, 2010:1-6.

[11] Chen R, Park J, Bian K. Robust distributed spectrum sensing in cognitive radio networks[C]//IEEE Communications Society Conference on Computer Communications. Phoenix, USA: IEEE, 2008:31-35.

[12] Kun Z, Paweczak P, Cabric D. Reputation-based cooperative spectrum sensing with trusted nodes assistance [J]. IEEE Communications Letters, 2010, 14(3):226-228.

[13] Zhu F, Seo S W. Enhanced robust cooperative spectrum sensing in cognitive radio[J]. Journal of Communications and Networks, 2009, 11(2):122-133.

[14] Hu F, Wang S, Cheng Z. Secure cooperative spectrum sensing for cognitive radio networks[C]// IEEE Military Communications Conference, MILCOM. Boston, MA, United States: IEEE, 2009:1-5.

[15] Li H, Han Z. Catching attacker(s): for collaborative spectrum sensing in cognitive radio systems: an abnormality detection approach[C]//IEEE Symposium on New Frontiers in Dynamic Spectrum. Singapore: IEEE, 2010:1-12.

[16] 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.

[17] Xu Shaoyi, Shang Yanlei, Wang Haiming. Double thresholds based cooperative spectrum sensing against untrusted secondary users in cognitive radio networks[C]//IEEE 69th Vehicular Technology Conference, VTC. [s. l.]: [s. n.], 2009:1-5.

[18] Min A W, Shin K G, Hu X. Attack-tolerant distributed sensing for dynamic spectrum access networks[C]//17th IEEE International Conference on Network Protocols, ICNP. Princeton, NJ, United states: IEEE CS, 2009:294-303.

[19] Li Z, Yu F R, Huang M. A cooperative spectrum sensing consensus scheme in cognitive radios [C]//IEEE Communications Society Conference on Computer Communications. Leblon, Brazil: IEEE, 2009:2546-2550.

(上接第 154 页)

4 结束语

文中将电子签章功能集成到公文流转系统中,从技术上保证签章文档的真实性、完整性和签署人的不可否认性,从法律上保证了签章行为的法律效力,提高了公文流转系统的安全性,扩展了系统的适用范围,可以实现真正意义上的无纸化办公。

参考文献:

[1] 刘宏伟. 基于身份的电子签章系统设计研究[J]. 计算机工程与设计, 2008, 29(7):1735-1738.

[2] 袁晓宇,张其善. 基于 ECDSA 的电子签章系统研究[J]. 计算机工程与设计, 2005, 26(5):1233-1235.

[3] 祁振杰,蒋朝惠. 电子签章控件透明化技术的研究与实现[J]. 计算机应用与软件, 2009, 26(11):124-126.

[4] 张　飞,肖　刚,程振波. 基于时间戳服务的电子签章验证方法研究[J]. 浙江工业大学学报, 2009, 37(3):300-305.

[5] 肖攸安,刘俊波. 一种新型的电子签章技术[J]. 武汉理工大学学报, 2009, 31(13):123-126.

[6] 盛津芳,王　斌,桂卫华. 基于 XPDL 的可视化流程定义工具及公文流转系统[J]. 计算机技术与发展, 2007, 17(7): 193-195.

[7] 王文玉,曲传幸,宋淑梅. 基于 Lotus Domino/Notes 平台的电子公文审批系统[J]. 计算机技术与发展, 2007, 17(2): 156-158.

[8] Denning D E. Protecting Public Keys and Digital Signatures [J]. Computer, 1993(2): 27-35.

[9] Polk W. Federal public key infrastructure (PKI) technical specifications (version 1) Part A: Requirements[EB/OL]. 1996. http:// citeseer. ist. psu. edu/394045. html.

[10] Kim S G. Designing a Domain Framework with Component Management Model[J]. Journal of Software, 2002, 13(3): 335-341.

[11] 陈雪珲,李建华. 电子签章系统在企业 OA 系统中的应用[J]. 信息技术与信息化, 2008(3):49-51.

[12] 袁珍珍,朱荆州. 基于 PKI 技术的数字签名在办公网上的实现[J]. 计算机与数字工程,2010, 28(2):104-109.