无线网络钓鱼 AP 攻击检测技术研究

金双齐 凌 捷
(广东工业大学计算机学院 广东 广州 510006)

摘 要 随着无线局域网应用的普及,针对无线网络的攻击方式也逐渐增多。无线钓鱼 AP 攻击通过被动或主动方式诱使用户连接钓鱼 AP,进而获取用户的敏感信息,是当前被滥用的攻击方式之一。针对这种情况,提出一种改进的钓鱼 AP 攻击检测方法,通过利用 TTL 值的递减变化,以及综合分析网关与路由信息,实现对 AP 的合法性检测。实验结果表明,该方法能够有效地检测无线钓鱼 AP 和无线中间人等攻击。

关键词 钓鱼 AP 攻击 WLAN Wifi

中图分类号 TP309 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2016.10.068

RESEARCH ON DETECTION TECHNOLOGY OF FISHING AP ATTACK IN WIRELESS NETWORK

Jin Shuangqi Ling Jie
(*Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, Guangdong, China*)

Abstract With the popularisation of WLAN, the attacks against wireless network are increasingly growing. Wireless fishing AP attack, through passive or active way, induces users to connect fishing AP, and then catches users' sensitive information, it is currently one of the abused attack modes. In light of this, we proposed an improved fishing AP attack detection method, by using diminishing variation of TTL value as well as comprehensively analysing the gateway and routing information, it realises validity detection on AP. Experimental results showed that this method can effectively detect the attacks including wireless fishing AP and wireless man-in-the-middle.

Keywords Fishing AP attack WLAN WiFi

0 引 言

无线局域网 WLAN 技术因其安装灵活性和移动性、易于扩展等特点而得到快速的发展。随着 3G/4G 技术的成熟及普及,基于 802.11 标准的 Wifi 无线网络在带宽、覆盖范围上得到迅速提升,已可承载无线校园、无线医疗、无线城市、无线定位、车载无线等丰富的无线应用,逐渐成为市场应用的主流。

无线 Wifi 为人们工作生活带来便利的同时,也存在多种网络攻击,具有很大的安全隐患。无线 Wifi 在通信工作站之间是以电磁波的形式进行传输的,在两个工作站之间的任何接收设备都可以接收到无线局域网传播的数据,恶意用户可以篡改接收到的数据或进行其他恶意操作[1]。在各种无线攻击中,无线钓鱼 AP 攻击是危害最严重的攻击方式之一。攻击者在公共场所搭建的一个伪装的无线 AP,具有与真实 AP 完全相同的服务集标识符 SSID、MAC 地址、加密方式等设置信息,诱使受害者连接到假冒的 AP,进一步获取用户的帐号密码等敏感信息[2-4]。国外有些学者也称之为"Evil Twin AP(邪恶双胞胎 AP)"或者"RogueAP(流氓 AP)"。传统的钓鱼 AP 检测技术,主要是在服务端依据无线嗅探器监测无线网络来检测可疑 AP。这种嗅探器是通过在 2.4 GHz 和 5 GHz 频谱上扫描未经授权的网络流量,嗅探出非法的网络流量。一些商业化的检测产品主要就使用了这项技术,如启明星辰的天清无线安全引擎、Motorola 公司的 AirDefense 产品。还有一些产品,使用特征指纹来区分合法 AP 与钓鱼 AP,这些特征主要包括:MAC 地址、供应商名称、信号强度、射频测量和 SSID 等。其他的一些替代方法还包括收集 RSSI 值、无线电频率的变化和时钟偏差作为特征指纹来识别无线钓鱼 AP[5]。

启明星辰公司的无线安全引擎能够通过安全策略阻断无线钓鱼 AP 及非法终端,Motorola 公司的 AirDefense 检测方案通过部署多个传感器实现全天候、全方位的无线局域网 AP 检测。然而,这些部署方案的代价是十分昂贵的,且这些方案一般不容易扩展,因此它涉及到大量基础设施的改建和大型网络改建。部署无线嗅探器要充分覆盖大型网络,成本昂贵,对于普通客户是不现实的。

本文通过对钓鱼 AP 的特征进行分析,并和传统的服务端检测钓鱼 AP 攻击的方法进行比较,深入研究无线局域网 IEEE802.11 系列协议,提出一种改进了的利用 TTL 值递减的变化,在客户端检测钓鱼 AP 的方法,设计并实现了对被动钓鱼攻

收稿日期:2015-06-02。广东省自然科学基金项目(S2012020011071);广东省科技计划项目(2013B040401017,2014A010103029);广州市科技计划项目(2014J4100201)。**金双齐**,硕士生,主研领域:信息安全技术。**凌捷**,教授。

击和中间人攻击的实验检验。实验结果表明,该方法能够有效地检测无线钓鱼 AP 和无线中间人等攻击。

1 钓鱼 AP 攻击原理分析

攻击者可以很容易地搭建一个钓鱼 AP。首先,通过一些分析软件为笔记本电脑进行简单的配置,搭建一个无线 AP。然后,攻击者通过配置与合法 AP 相同的 SSID、MAC 地址、信道及加密方式。最后,等待或诱使合法用户连接钓鱼 AP。根据 IEEE802.11 协议标准,通常无线钓鱼 AP 越靠近用户越容易成功,当周围出现多个配置相同的 AP 时,无线客户端会根据无线网卡选择信号最强的那个 AP 进行连接[6]。因此,攻击者只要具备配置与合法 AP 相同信息并提高信号强度或距离受害者越近就越容易达到攻击效果。

攻击者通常会在靠近商场、宾馆、咖啡厅或者图书馆等地方搭建钓鱼 AP。通过钓鱼 AP,攻击者可以通过发动中间人攻击截获用户的敏感信息,如帐号、密码等,也可以通过操作 DNS 服务器,控制路由,发起更多的服务器钓鱼攻击。总之,无线钓鱼 AP 严重危害了无线局域网的安全。

无线钓鱼 AP 攻击的基本步骤是:首先,攻击者挑选信号发射功率较大的 AP;其次,攻击者获取合法 AP 的 SSID 名称、无线频道、无线加密方式等配置信息。最后,攻击者部署好 AP 等待用户连接,或者攻击者主动发送欺骗报文给 AP,强制用户断开与合法授权 AP 的连接。无线钓鱼 AP 的攻击场景如图 1 所示。

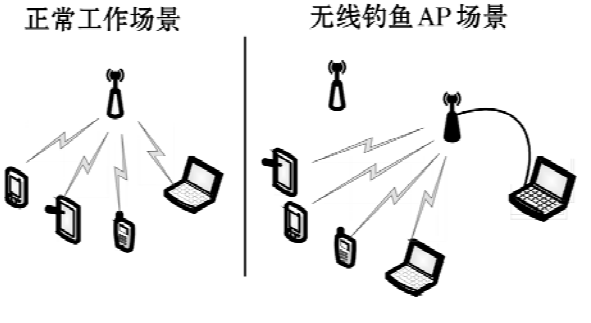

图 1 合法场景和无线钓鱼场景

目前,钓鱼 AP 攻击主要有两种类型[7]:第一种类型是使用典型的无线路由器作为无线钓鱼 AP,或者通过刷新无线路由器 Firmware 类建立钓鱼专用 AP。常见的第三方开源 Firmware 有 DD-WRT 和 Open-WRT。第二种类型是在一台便携式笔记本配置两块无线网卡,一块是用来连接真实的 AP,以便数据转发回互联网;另一块网卡使用 AP 模式,配置成一个可提供无线接入的 AP。其中比较著名的无线钓鱼软件就是 AirSnarf(http://airsnarf.shmoo.com/)。AirSnarf 是一个简单的恶意无线接入点设置使用程序,旨在展示一个无线钓鱼 AP 如何从公共无线热点窃取用户名和密码。AirSnarf 是一台跨平台的软件,目前已经支持 Windows XP、Linux 操作系统,甚至可以作为固件刷入 Linksys WRT54G 系列的无线路由器中。同时 AirSnarf 还需要其他自动化应答工具辅助形成完整的无线钓鱼 AP,如 DNS 域名解析服务、Web 应用服务、动态网站环境等。

2 钓鱼 AP 攻击检测技术现状

文献[8]中使用了 MAC 地址区分的方法。在各类无线局域网中,MAC 地址区分用于不同的网络设备。在无线 AP 发送给工作站的数据帧中同样包含 AP 自身的 MAC 地址信息和接收方的 MAC 地址。无线局域网中的网络设备 MAC 地址由 48 位比特位构成,分成两部分:前 24 位由 IEEE 统一分配,为厂商地址;后 24 位由厂商为设备分配。通过不同的 MAC 地址可以区分不同的网络设备。而开放的 ESSID 认证的 AP 会广播含有自身 MAC 地址信息的 Beacon 帧,处在 AP 广播范围内的工作站均可以接收到这类帧,因此攻击者同样可以获取合法 AP 的 MAC 地址信息,并将这些获取的 MAC 复制到非法 AP 的数据帧中。由于 MAC 地址可以轻易地被攻击者改变,因此使用 MAC 地址检测,存在很大的弊端。

Bratus 在文献[9]中提出了一种主动式基于指纹的检测方法。这种方法是通过发送一些特定的错误格式的数据帧来刺激无线 AP,通过检测无线 AP 的不同行为特征来获取针对无线 AP 网卡芯片或无线网卡驱动等这些特征指纹信息来区别无线钓鱼 AP 与合法授权 AP。这种方法以较低的成本为部署主动式的无线端检测方法提供了一种思路,即通过修改数据链路层的数据帧(MAC 帧)并使得某些数据帧位不符合 802.11 标准协议中所规定的数据帧位[10],但又不是明确禁止的。因此如果在标准协议中明确禁止情况下,该数据帧可能会被 AP 丢弃,比如在 MAC 管理帧帧头的帧控制域中,其中 FromDS 字段和 ToDS 字段按照协议要求应该置为“0”,将这两个比特设置“1”即可以制造出具有错误格式的“刺激”帧,这样可以刺激 AP,并使其做出某些特征行为的刺激响应。不同的无线网卡芯片或者不同的无线网卡驱动的 AP 表现出的行为特征是不一样的。另外在文献[5]中还提出了采用决策树的结构来实现自动化的刺激响应处理措施。这些基于 AP 特征指纹的检测方法可以检测钓鱼 AP,但是这些主动的检测方法容易被攻击者发现,并且是在服务端的检测。

Kim 等在文献[11]中讨论了 IEEE802.11 协议中有关隐藏标识符的影响,突出强调了 IEEE802.11 协议中的一些独一无二的标识符,使得用户不是匿名的,允许用户追踪。即使相关的标识符被刻意掩盖,也可以通过检测一系列 802.11 协议中的参数信息来追踪到用户。文中确定了 4 种相关的网络参数:在 802.11 协议探测帧中的网络目的地址网络名称(SSID)、802.11协议中配置选项和广播帧的大小。在加密流量的情况下,四分之三的参数信息仍可被获取到。但是在这种指纹识别技术中需要每个用户端至少持续一个小时的流量样本监控,监控时间长并且监控成本高。

3 改进的钓鱼 AP 检测方法

TTL 生存时间字段中设置了 IP 数据报能够经过的最大路由器数。TTL 字段由发送端初始设置,在每个处理该数据报的路由器需要将其 TTL 值减 1,当路由器收到一个 TTL 值为 0 的数据包时,路由器就会将其丢弃。TTL 字段的目的是防止数据报在选路时无休止地在网络中流动。当路由器瘫痪或者两个路由器之间的连接丢失时,可能会造成路由器环路,而路由器可能会根据其路由表将该数据包一直循环转发下去。在这种情况下,就需要一种机制来给这些循环传递的数据报加上一个生存上限,TTL 字段正是实现这种机制的手段。TTL 字段在 IP 头部的位置如图 2 所示。

4 位版本	4 位首部	8 位 服务类型	16 位总长度(字节数)	
16 位标识			3 位标志	13 位 片偏移
8 位生存时间(TTL)		8 位协议	16 位首部检验和	
32 位源 IP 地址				
32 位目的 IP 地址				
选项(如果有)				
数据				

图 2　TTL 字段在 IP 报头的位置

根据 TTL 值递减的变化,本文提出了一种改进的检测方法,用于检测 MITM 攻击的场景或双胞胎 AP 的场景。由于所有的钓鱼 AP 接入点并不会表现出相同的方式,因此这种方法能够在不同的场景中,检测出钓鱼 AP 的攻击。如图 3 所示,根据收集到的信息,有三种存在的状态:一种是 MITM 攻击的场景,另一种是双胞胎钓鱼 AP 欺骗场景,最后一种就是安全的网络环境。

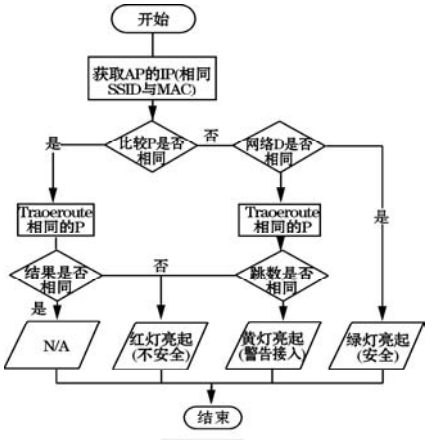

图 3　钓鱼 AP 检测流程图

如图 3 所示,在 Wifi 广播的环境中,我们收到两个相同 SSID、MAC 和 IP 地址和包路径完全相同点的两个接入点 AP。根据 IEEE802.11 网络层协议,在同一个网络中,不能同时出现两个相同的 IP 地址。如果发生了这种情况,会造成 IP 地址的冲突,客户端设备会停止工作。因此,在图中,这种情况会显示为“N/A”。

唯一出现的一种情况是,有相同的 IP 地址与不同的包路径情况,这种情况是 IP 欺骗的结果。出现这种情况,只能是双胞胎钓鱼 AP 攻击的场景,就会警告用户,慎重上网。

首先扫描当前网络环境,当发现有相同的 SSID 和 MAC 地址的两个 AP 的时候,连接 AP,并比较两个 AP 的 IP 地址。如果发现有不同的 IP 地址,这种情况下,为了做出下一步的决策,需要比较网络 ID。如果网络 ID 相同,表明两个 AP 是在相同的网络环境下,出现这种情况是网络负载均衡的结果。网络管理员可以使用两个接入点 AP(相同的网络 ID),让网络实现负载均衡,所以是一种安全的连接。这种情况下,绿灯亮起,提示用户可以安全接入当前网络。

第二种情况是,不同的 IP 地址和不同的网络 ID。这种情况下,该检测算法会执行跟踪路由访问点并比较访问点是否相同。通过 traceroute 命令,查看返回的路由器跳数,如果跳数结果不同,则红灯亮起,证明存在中间人攻击,提示用户接入了不安全的访问点 AP。因为这种情况下,是攻击者截取了一个 AP,并广播 SSID,黑客通过设置相同的 SSID 名字,诱使用户连接到钓鱼 AP 接入点。攻击者在合法 AP 和客户端之间,嗅探网络流量,截取用户的通信信息。

第三种情况是,不同的 IP 地址和不同的网络 ID。在这种情况下,执行 traceroute 命令,查看路由器跳数,发现并没有新增额外的跳数,执行了不同的 trace 路线,确定到达了相同的目的地,这种情况是攻击者设置了和合法 AP 相同的 SSID、IP 和 MAC 地址,诱使用户连接钓鱼 AP。这种情况下,黄色灯亮起,用于警告用户连接此网络是不安全的。

4　实验与结果分析

4.1　实验设计

实验模拟了无线钓鱼环境,图 4 显示了实验中的无线网络场景,其中包含真实的无线 AP 和伪装的钓鱼 AP,真实 AP 与路由器的连接带宽是 100 Mbps,AP 的传输带宽是 50 Mbps,伪装的钓鱼 AP 使用笔记本网卡发射的无线网作为接入口。为了更好地评估实验效果,在真实的环境中,我们选择了与客户端不同距离的四个点 A、B、C、D 做测试,分别代表 RSSI 的四个测试范围:A、B、C、D,如表 1 所示。

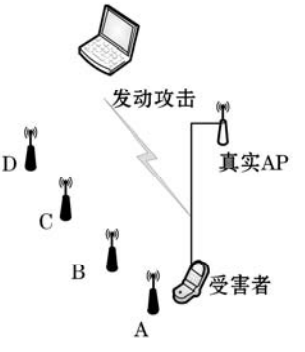

图 4　无线网络攻击

表 1　RSSI 等级范围描述

范围	A	B	C	D
高范围	100%	80%	60%	40%
低范围	80%	60%	40%	20%

在实验环境中,利用 Android 智能手机连接无线 Wifi,增加了主动钓鱼攻击的方便性。攻击者使用 DoS 攻击方式强制使受害者断网,并连接到攻击者搭建的钓鱼 AP,使用笔记本电脑的无线网卡截取用户的数据报文并转发数据。

4.2　实验结果与分析

利用中间人攻击或者双胞胎 AP 攻击,当强制受害者转到钓鱼 AP 上后,钓鱼 AP 可以将受害者的敏感信息截获,显示在攻击者的个人屏幕上。本次实验,通过比较两个 AP 的 SSID、MAC 地址、IP 地址信息,然后 traceroute 固定的 IP 地址或网址,通过返回的跳的信息,最后报警给连接 AP 的用户。在本次实验中,我们选择了四个不同的 RSSI 范围和两种 IEEE 协议 802.11b和 802.11g 评估方法的有效性。如表 2 和表 3 中所示,能够清晰地验证本文算法的有效性。此外,我们可以发现,802.11g 的结果优于 802.11b。

表 2　实验方法的检测率

协议范围	A	B	C	D
802.11g	99.65%	98.24%	96.89%	94.35%
802.11b	99.21%	97.79%	95.57%	93.88%

性能分析主要从检测效果、时间、成本三个方面进行比较。在检测效果方面,文献[8]有明显的不足,MAC 地址易被攻击者获取并复制,存在很大的弊端。在实时性方面,文献[9]需要建立大量的指纹库;文献[11]需要持续一个多小时的流量分析,实时性不够好,检测时间长。本文利用 TTL 值比较,不易被篡改,实时性也能保证,在检测效果、时间与成本上面有较大的提高。

下面是本实验方法与文献[8,9,11]进行比较分析。比较

结果见表 3 所示。

表 3 实验性能分析

文献比较方面	效果	时间	成本
文献[8]	MAC 地址易被改变,检测效果差	时间少	成本低
文献[9]	检测实时性差	提取指纹花费时间长	建立特征指纹库需大量开销
文献[11]	检测实时性差	需要持续一个小时以上的流量成本	检测成本高
本文	实时性效果好	花费时间短	检测成本低

5 结 语

本文分析了无线局域网中钓鱼 AP 攻击原理,提出了一种改进的钓鱼 AP 攻击检测方法,并分析了检测钓鱼 Wifi 的条件。该检测方法基于无线端检测。通过利用 TTL 值的递减变化,以及综合分析网关与路由信息,实现对 AP 的合法性检测。实验结果验证了这种检测方法的有效性。

本文提出的这种改进的钓鱼 AP 检测方法,用于检测基于 MITM 攻击的钓鱼和双胞胎 AP 的钓鱼场景。根据不同的检测结果显示灯的颜色,提醒接入无线网络的用户。针对文中检测方法,并不是在有线端,不需要大量的运行设备,方便了普通客户的检测。在今后的工作中,将进一步研究较为通用的检测方法,探讨无线网络的攻击方式及可以利用的漏洞,针对无线网络中各种漏洞进行分析,提出相应的防范措施。

参 考 文 献

[1] 齐惠英. 基于 EAP-TLS 的 WLAN 安全认证[J]. 科技通报,2012,28(10):25 - 27.

[2] Song Y M, Yang C, Gu G F. Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point[C]// Dependable Systems and Networks, IEEE/IFIP International Conference on. IEEE, 2010:323 - 332.

[3] Han H, Xu F Y, Tan C C, et al. Defending against vehicular rogue APs [C]// INFOCOM, 2011 Proceedings IEEE. IEEE, 2011: 1665 - 1673.

[4] Han H, Sheng B, Tan C C, et al. A Timing-Based Scheme for Rogue AP Detection[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(11):1912 - 1925.

[5] Han H, Xu F Y, Tan C C, et al. Defending against vehicular rogue APs [C]// INFOCOM, 2011 Proceedings IEEE. IEEE, 2011: 1665 - 1673.

[6] 陈伟,顾杨,于乐. 高隐蔽性的无线网络主动钓鱼攻击及其防范研究[J]. 武汉大学学报:理学版,2013,59(2):171 - 177.

[7] 陈伟,顾杨,李晨阳,等. 无线钓鱼接入点攻击与检测技术研究综述[J]. 武汉大学学报:理学版,2014,60(1):13 - 23.

[8] 朱建明,马建峰. 无线局域网安全:方法与技术[M]. 2 版. 北京:机械工业出版社,2009.

[9] Bratus S, Cornelius C, Kotz D, et al. Active behavioral fingerprinting of wireless devices[C]//Proceedings of the First ACM Conference on Wireless Network Security, 2008:56 - 61.

[10] 蒋华,阮玲玲,王鑫. 基于 SHA-256 消息认证的四次握手协议研究[J]. 微电子学与计算机,2014(8):155 - 158.

[11] Kim I, Seo J, Shon T, et al. A novel approach to detection of mobile rogue access points[J]. Security and Communication Networks, 2014, 7(10):1510 - 1516.

(上接第 293 页)

6 结 语

传统云存储平台虽然也在云端对数据进行了加密,但是拥有密钥的云服务商却能通过解密接触到明文数据。此外,在云端和客户之间的信道中数据以明文状态传递容易被黑客截获。在明文数据进入不安全信道之前加密,则可以降低云服务商和黑客造成数据泄密的风险。如果用一般的加密算法对数据加密后再上传到云端存储,势必会影响云服务器对数据的处理性能,而对加法和乘法都具有同态性的全同态加密算法则无此问题。针对全同态加密带来的密钥管理复杂和密文检索困难的问题,本文也提出了“密钥管理算法”和“密文检索算法”予以解决。在性能上,该技术增强了数据传输与存储的保密性,其密文检索效率高、结果准确且文档排序合理,值得推广与应用。

参 考 文 献

[1] 晏强,张晓锋,丁蕊. 云存储技术研究[J]. 计算机与信息技术,2011(12):35 - 37.

[2] Jay Heiser, Mark Nicolett. Assessing the Security Risks of Cloud Computing[EB/OL]. (2008 - 6 - 3)[2012 - 12 - 28]. www.gartner.com/id=685308.

[3] Bit network. HTC 泄密等 30 起泄密案的启示[EB/OL]. 2013 - 09 - 05. http://www.people.com.cn/.

[4] 郭璐璐,许春根. 云存储密文检索方法的研究[J]. 技术研究,2013(9):6 - 8.

[5] 李美云,李剑,黄超. 基于同态加密的可信云存储平台[J]. 信息网络安全,2012(9):35 - 40.

[6] 周可,王桦,李春花. 云存储技术及其应用[J]. 中兴通讯技术,2010,16(4):24 - 27.

[7] 刘赛,李绪蓉,万麟瑞,等. 云环境下资源调度模型研究[J]. 计算机工程与科学,2013,35(3):48 - 51.

[8] 黄永峰,张久龄,李星. 云存储应用中的加密存储及其检索技术[J]. 中兴通讯技术,2010,16(4):33 - 36.

[9] Riverst R, Adleman L, Dertouzos M. On data banks and privacy homomorphisms[M]. New York: Academic Press, 1978:169 - 180.

[10] 何劲. 基于同态加密与认证的 WSN 安全数据融合[J]. 计算机应用与软件,2014,31(9):314 - 316,321.

[11] Gentry C. Fully homomorphic encryption using ideal lattices[M]. New York: Association for Computing Machinery, 2009:169 - 178.

[12] Marten Van Dijk, Gentry C, Halev s, et al. Fully homomorphic encryption over the integers[C]//Pro of the 29th Annual International Conference on Theory and Application of Cryptograhic Technational. Berlin: Springer - Verlag, 2010:24 - 43.

[13] 林如磊,王箭,杜贺. 整数上的全同态加密方案[J]. 计算机应用研究,2013,5(5):1515 - 1519.

[14] Song D, Wagner, Perrig A. Practical techniques for searcheson encrypted data[C]//Proc. of IEEE Symposium on Seccurity and Privacy'00. 2000.

[15] Boneh D, Crescenzo G D, Ostrovsky R, et al. Public keyenccryption with keyword search [C]//Proc. of Eurocryp' 04, Volume3027 of LNCS. Springer, 2004.

[16] Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data[C]//Proc. of ICDCS'10. 2010.

[17] 冯贵兰,谭良. 云环境中基于多属性排序的密文检索方案[J]. 计算机科学,2013,40(11):131 - 136.