文章编号:1671-4598(2021)06-0219-05 DOI:10.16526/j.cnki.11—4762/tp.2021.06.042 中图分类号:TP399 文献标识码:A

基于动态策略的移动警务终端安全管控系统的设计与实现

樊志杰[1,2]，郑长松[3]，曹志威[1,2]
(1. 上海辰锐信息科技公司 研发中心，上海 200031；
2. 公安部第三研究所 信息安全技术部，上海 200031；
3. 四川省公安厅 科技信息化总队，成都 610041)

摘要：对移动警务安全接入平台中的终端设备的安全防护问题进行了研究，提出并研制了一种基于动态策略的移动警务终端安全管控系统，整个系统由客户端、前置服务端和内网服务端组成，前置服务端和内网服务端分别部署在前置区和公安内网，客户端部署在移动终端设备上，确保在移动接入区和公安内网区有效进行物理隔离的前提下，将系统制定的各种安全策略规则下发到客户端执行，规范用户对移动终端的本地软硬件资源和网络资源的使用，实现安全威胁检测、防护及预警，对移动终端用户的违规访问、操作行为进行全面监测和上报，实现终端设备安全和行为的统一管理。

关键词：动态策略；移动警务终端；安全管控系统；移动接入区；公安内网区

Design and Implementation of Mobile Police Terminal Security Management and Control System Based on Dynamic Strategy

Fan Zhijie[1,2], Zheng Changsong[3], Cao Zhiwei[1,2]
(1. Research and Development Center, Shanghai Chenrui Information Technology Company, Shanghai 200031, China;
2. Department of Information Security Technology, The Third Research Institute of the Ministry of Public Security, Shanghai 200031, China;
3. Science and Technology Information Corps, Public Security Department of Sichuan Provincial, Chengdu 610041, China)

Abstract: In this paper, we study the security protection of terminal equipment in mobile police security access platform, and proposes and develops a mobile police terminal security management and control system based on dynamic strategy. The whole system consists of client, front-end server and intranet server. The front-end server and intranet server are deployed in front-end area and public security intranet respectively, and the client is deployed in mobile terminal. In term of this, under the premise of physical isolation between the mobile access area and the public security intranet area, all kinds of security policy rules will be distributed to the client for execution, so as to standardize the user's use of the local software and hardware resources and network resources of the mobile terminal. Meanwhile, the proposed system can realize the detection, protection and early warning of security threats, comprehensively monitor and report the illegal access and operation behavior, and realize the unified management of terminal equipment security and behavior.

Keywords: dynamic strategy; mobile police terminal; security control system; mobile access area; public security intranet area

0 引言

移动警务安全接入平台主要基于社会移动公网接入公安网，便于充分利用公安信息资源，提升案件侦破、逃犯抓捕、人口核查、车辆比对、犯罪打击和预防等公安工作的效率。同时，移动警务应用有效地提升了公安干警快速反应、综合作战的能力，提高公安机关维护稳定、打击犯罪的水平，也进一步提升公安机关行政管理和服务群众的质量，提升公安的形象。

当前的移动警务平台主要通过终端设备的接入认证和端到端的数据加密，实现用户可信和链路安全传输。但随着黑客技术的不断变化和安全防护需求的逐步提升，终端自身的安全防护问题日益突出。同时，通过“一机两用”、外设端口访问、应用软件无管控和系统弱口令等带来的安全隐患也成为了亟待解决的安全问题。鉴于此，基于移动警务安全标准的终端安全管控系统（TSMS，terminal security management system）将作为重要方式来保障移动警务

收稿日期:2021-02-09； **修回日期**:2021-03-29。
基金项目:四川省科技计划项目(重点研发项目)(2021YFS0310);国家重点研发计划(2018YFC0807105)。
作者简介:樊志杰(1982-),男,山西朔州人,博士,副研究员,主要从事信息与网络安全方向的研究。
引用格式:樊志杰,郑长松,曹志威.基于动态策略的移动警务终端安全管控系统的设计与实现[J].计算机测量与控制,2021,29(6):219-223.

平台的安全。

《全国公安移动警务总体技术方案》中将移动终端依据安全受控程度，分为增强受控终端、一般受控终端和个人普通终端。其中增强受控终端与一般受控终端中需安装终端安全软件即移动设备安全管控系统。同时，终端安全管控系统应事前对安全事件进行报警预测，对终端主机能够做到预先规范使用行为，能够准确有效地实现行为可控制、可统计，将管控制度转化为有效的技术管控系统进行执行，从而有效提升整个系统的可管理性和信息安全水平[1-5]。

现有 TSMS 系统在使用过程中主要存在以下问题：

1）开发 TSMS 客户端需要与终端厂商进行大量的适配工作。TSMS 客户端用于接收 TSMS 后台控制策略并与手机底层硬件接口耦合，实现控制手机硬件（如蓝牙、WIFI 等）的开启或关闭、终端运行环境的检查以及安全日志的上报等功能。

2）已开发的 TSMS 很难进行直接复用。由于不同终端厂商的系统代码均基于原生安卓系统进行了个性化定制开发，故不同品牌、型号的终端系统必然存在一定的差异。

3）TSMS 客户端在实际使用过程中耗电量偏高。由于 TSMS 客户端一般是运行在系统应用层的独立程序(APP)，必须常驻内存，方可接收控制策略并提交系统日志。

针对上述问题，本文提出并研制一种基于模块化与动态策略的移动警务终端安全管控系统，主要优势包括：

1）降低系统耦合度。减少终端厂商与 TSMS 应用开发厂商之间的终端适配工作。

2）提高系统安全性。终端厂商不必对外开放过多的硬件调用接口，进一步降低系统被非法入侵的可能性。

3）推进系统标准化。对终端厂商、安全通道厂商以及后台策略控制系统开发商之间的数据接口进行标准化处理。

1 系统结构及原理

依据公安移动警务安全接入平台的网络特点，结合移动安全接入的需求，并按照公安主管部门的有关管理规范和建设要求，本文研制出一套终端安全管控系统，简称 TSMS。主要分为：客户端、前置服务端和内网服务端，其系统结构如图 1 所示[6-9]。

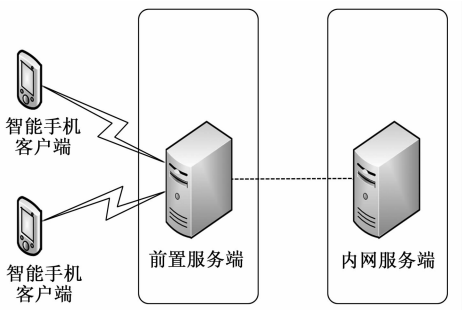

图 1 终端安全管控系统结构

其中，前置服务端主要部署在前置服务区内，内网服务端主要部署在内网管理服务区内。通过上述系统结构的部署方式，可确保在移动接入区和公安内网区有效进行物理隔离的前提下，实现前后置系统配置和安全策略同步，进而有效防止移动终端非法访问移动接入区的应用系统，降低网络风险。

本文研究的终端安全管控系统的策略执行原理如图 2 所示，其主要通过中心服务器平台制定终端 Agent 代理程序端的安全策略，并通过网络下发到各个终端。Agent 代理程序收到安全策略后，对移动终端本地状态及用户行为进行检测，对不满足安全策略的状态或行为形成审计信息并上报到中心服务器平台。最终，管理员通过中心服务器平台完成对下属所有移动终端的统一管理及审计。

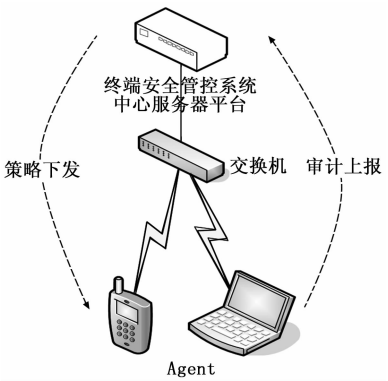

图 2 策略执行原理

2 软件系统架构设计

2.1 TSMS 软件设计整体框架

根据建立移动警务安全管控生态圈的理念，以及开放、共生、通用的原则，本文将 TSMS 模块按部署位置分为移动终端和控制后台两个部分，在通信层、数据层和应用层 3 个层次划分成不同的功能维度，最终形成整体解决框架。主要包括以下 3 个功能模块[10-13]：

1）终端安全模块。主要实现对设备硬件（如 WIFI、移动网络等）状态监控、硬件控制、日志收集等功能。

2）数据传输模块。分为终端通信模块（部署在终端上）与后台通信模块（部署于控制后台）。终端通信模块部署在移动终端上，以标准接口的方式与终端安全模块对接，实现终端控制策略接收、数据加密传输和终端日志回传等功能；后台通信模块部署于 TSMS 中，支持多级部署，提供标准通信框架接口，与 TSMS 后台策略控制模块对接，配合终端通信模块实现高并发条件下的控制策略数据传输、日志数据接收等功能。

3）策略控制模块。与数据传输模块间通过标准接口进行对接，实现已制定策略的安全下发、终端日志获取，同时实现对已接收的数据进行分析处理、深度挖掘、集中动态展示等功能。

2.2 TSMS 内部软件设计框架

本文提出的终端安全管控系统其内部可抽象为上层应

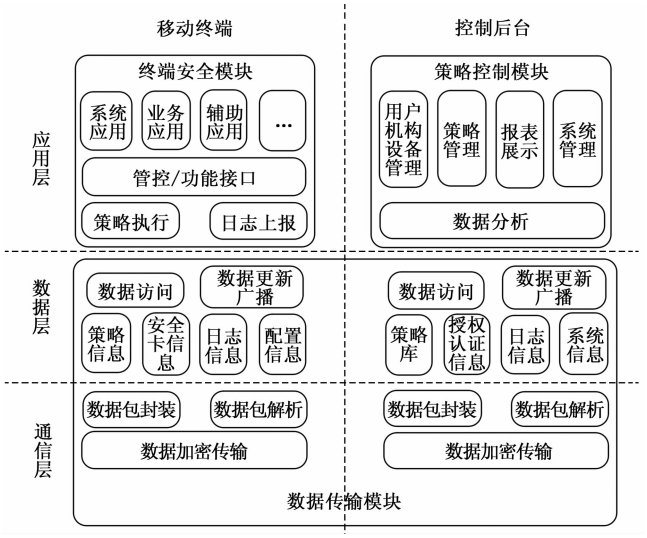

图 3　TSMS 软件设计整体框架

用、接口层及功能层，通过各层之间的相互封装调用，为用户提供统一的用户界面，并为系统的扩展进行保留。

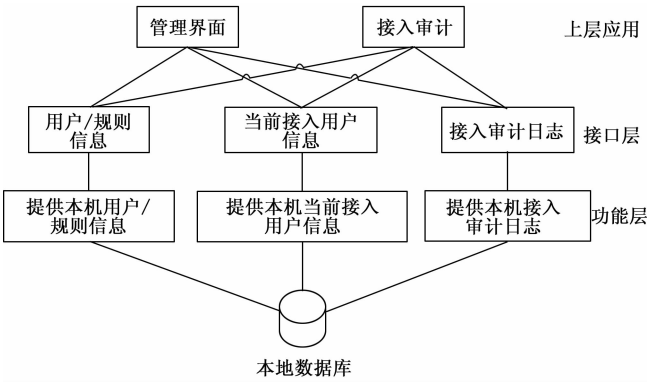

图 4　实现表示图

终端安全管控系统中心服务器平台内部结构如图 5 所示。

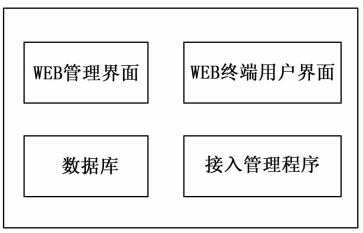

图 5　中心服务器平台内部结构

移动笔记本 Agent 代理程序内部结构如图 6 所示。

智能手机 Agent 代理程序内部结构如图 7 所示。

所提移动警务终端安全管控系统的界面设计如图 8 所示。

3　关键技术设计与实现

3.1　安全管控策略设计

本文提出的移动警务终端安全管控系统主要在中心服务器平台制定安全策略，并将安全策略下发到移动终端，相应的规则包括[14]：

1）全局安全规则管理。用于对系统中应用到移动终端主机或证书用户的安全规则进行集中管理，包括添加、编辑、复制、删除规则以及刷新规则等。

2）全部终端安全事件管理。用于对系统所有移动终端触发并上报的安全事件进行集中管理，包括查看事件详细、导出事件备份以及对事件进行搜索等。

3）网络访问规则控制。用于设置终端主机的网络访问规则，从而最大程度的保证系统网络正常有序地运行。

4）违规外联行为检测。用于检测当前用户是否接入互联网，如果发现用户移动终端接入互联网则立即进行断网处理，防止移动终端发生“一机两用”行为。

5）外设端口访问控制。用于设置终端主机指定外设端口的可用状态，从而保障网络数据安全。本系统支持对移动硬盘（U 盘）、软盘、CD/DVD 刻录机、串行口（COM 口）、并行口（LPT 口）、打印机、USB 控制器外设端口的管理，且不可更改。

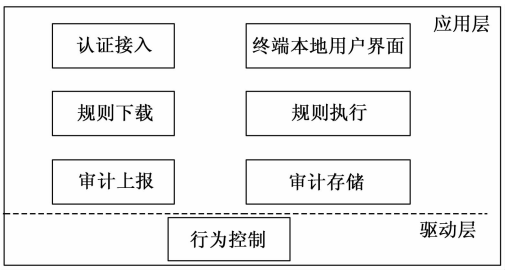

图 6　移动笔记本 Agent 代理程序内部结构

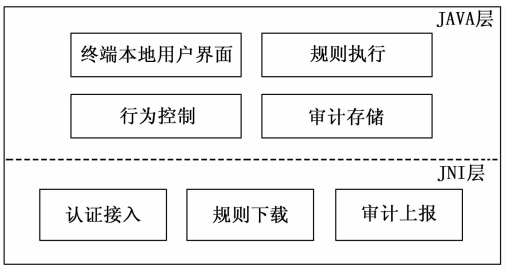

图 7　智能手机 Agent 代理程序内部结构图

图 8　系统首页原型图

6）违规软件主动卸载。用于防止终端侧违规使用的软件，并对发现的违规软件进行主动卸载。

7）应用程序白名单。用于设置终端可以可用的软件或指定供应商提供的软件，系统会对白名单中设定的内容进行自动放行，对未在白名单中设定的内容进行阻止。

8）强力终止进程功能。用于对终端主机运行的，且在规则配置中的进程进行强力终止，从而保证终端主机不能运行非法进程。

9）非法网站（页）访问控制功能。用于对终端主机访问非法网站（页）的情况进行管理，非法网站（页）可以根据需要进行配置。

10）防病毒软件检测功能。用于对终端主机常见防病毒软件安装情况进行检测，并对未安装任何常见防病毒软件的客户端进行安全预警。

11）网络防火墙检测功能。用于对终端主机网络防火墙软件安装情况进行检测，并根据配置对没有安装指定防火墙软件之一的主机进行安全预警。

3.2 安全管控功能实现

本文提出的 TSMS 系统的主要功能包括[15]：

1）统一管理：系统通过在移动终端（智能手机、移动笔记本）上部署专有的客户端软件，实现对各移动终端设备安全和行为的统一管理和规范。

2）资源访问控制：对移动终端的各类资源访问行为进行全面的控制和审计，包括网络访问行为、打印机访问行为和外设端口使用行为等。

3）数据安全保护：系统针对移动终端的运行使用特点，提供移动终端本地数据保护功能，控制和审计终端本地文件和网络数据的访问行为。

4）终端安全状态检测：对移动终端自身的各种安全状态进行检查和加固，主动防止安全状态不符合要求的移动终端接入网络。

5）系统综合审计：将各移动终端相关资产、违规行为等信息统一上报至管理平台并进行分类，提供各项安全功能的检查结果、终端用户行为的汇总报表，实现对移动终端各种安全状态及事件的全面审计。

6）客户端安全：客户端与操作系统进行紧密结合，使用者在软件安装后无法擅自卸载客户端，保证了系统实施的效果。

7）客户端安装功能：系统部署简单，提供独立的客户端安装包，安装便捷。

8）客户端引擎功能：客户端于后台运行无需任何工作界面，并采用事件驱动机制和休眠机制，使任何具体事务的处理不影响移动终端使用者的工作，既不浪费移动终端本身的资源，同时基于事件触发的高效工作模式最大可能地降低了对网络资源的使用。

9）基于 IE 的管理功能：采用 IE 浏览器作为其管理界面，在具体工作中方便管理员在网络可达的地点登陆系统，进行管理。

4 系统应用实施方案

4.1 运行环境

1）硬件环境：本系统运行所需要的硬件环境如表 1 所示。

表 1 设备硬件环境

序号	设备名称	系统版本	配置及安装软件说明
1	前置服务器	定制 Linux	CPU:Intel(R) Xeon(R) E5－2660 2.2 GHz、16 GB 内存、500 GB 硬盘；
2	内网服务器	定制 Linux	CPU:Intel(R) Xeon(R) E5－2660 2.2 GHz、16 GB 内存、500 GB 硬盘；
3	智能手机	Android 4.0 以上	CPU:400 MHz 以上 内存:128 M 以上 存储空间:50 M 以上
4	交换机	无要求	
5	安全接入网关	无要求	
6	移动应用管理服务器	无要求	
7	网闸	无要求	
8	移动应用代理服务器	无要求	
9	统一管理平台服务器	无要求	
10	人员统一管理服务器	无要求	
11	应用管控服务器	无要求	
12	鉴别评估管理服务器	无要求	

2）软件环境：本系统运行所需要的软件环境如表 2 所示。

表 2 设备软件环境

序号	类别	名称	系统版本	相关软件说明
1	移动终端	智能手机	Android 5.0 以上	移动警务安全接入网关客户端 V4.2.3.8 终端通讯组件 1.0.1

4.2 应用实施方案

TSMS 系统采用旁路模式部署于网络拓扑中，前置服务端部署于移动警务安全接入平台的移动接入区，内网服务端部署于移动警务安全接入平台的公安内网区，网络中其它设备的配置信息不需要进行修改。终端安全客户端软件分别安装于移动 Windows 终端和 Android 终端，在链路中 VPN 接入网关建立通道后，终端安全管理前置服务端自动检测与终端安全管理系统内网服务端的通信情况，自动获取安全策略，接受统一管控[16-18]。具体部署如图 9 所示。

本文提出的部署方案在保障移动警务安全接入方面具有以下特点[19-21]：

1）前后置服务端模式。在移动接入区和公安内网区有效进行物理隔离的前提下，实现前后置系统配置和安全策略同步，有效防止移动终端非法访问移动接入区的应用系统，降低网络安全风险。

2）安全策略“脱网”执行。当移动终端首次通过 VPN

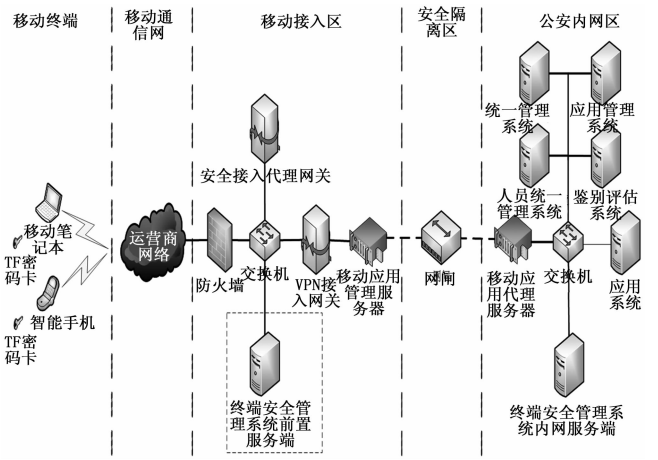

图 9　网络部署示意图

接入网关成功建立通道后，终端安全管理客户端自动到前置服务端进行安全策略下载，并保存于移动终端本地自动执行。实现移动用户在未连接 VPN 接入网关的前提下也能安全访问前置应用。

3）同时支持 Windows 终端和 Android 终端。安全管理客户端同时支持对移动笔记本和智能手机进行管理，适应用户需同时管控智能手机和移动笔记本的需求，降低了管理复杂度。

4）详细的资源访问控制。对移动终端的本地软硬件资源以及网络资源进行了严格限制，可以通过管理平台对移动终端的资源使用进行控制。

5）全面监测和预防控制。对各移动终端用户的违规访问、操作行为进行全面监测和预防，准确及时地进行审计。

6）客户端防卸载。当移动终端按照要求安装完成终端安全管理客户端后，用户无法手动卸载，确保移动终端环境的安全环境不变，同时配合 VPN 客户端做校验检测，若移动终端没有安装终端安全管理客户端，则 VPN 客户端无法启用，禁止拨号连接。

5　结束语

移动警务安全接入平台自 2006 年起即进行试点建设工作并逐步完善，平台的建设有效提升了公安干警快速反应和综合作战的能力，提升了公安机关行政管理和服务群众的质量，但是移动警务终端所处环境复杂、部分终端会与公安网进行数据交互，存在通过终端入侵公安网的安全风险。本文提出的移动警务终端安全管控系统采用前后置服务端模式，通过在服务端平台制定各种安全策略，实现安全策略下发到移动终端执行，各移动终端将相关资产、违规行为等信息统一上报至管理平台进行综合审计，实现了详细的资源访问控制，对各移动终端用户的违规访问、操作行为进行全面监测和预防。同时，本文提出的基于模块化架构的移动警务终端安全管控系统，有效地解决了客户端开发与终端厂商的适配对接工作，并且提高了客户端软件自身的安全性、软件开发效率和可复用性等。

参考文献：

[1] 卢　煜. 提升支撑能力一繁荣移动警务应用一全国移动警务应用发展现状分析与建议 [J]. 警察技术，2019 (2)：4－6.

[2] 沈昌祥，张大伟，刘吉强，等. 可信 3.0 战略：可信计算的革命性演变 [J]. 中国工程科学，2016，18 (6)：53－57.

[3] 张明德，郑雪峰，吕述望，等. 身份认证可信度研究 [J]. 计算机科学，2011，21 (11)：43－47.

[4] 卢　煜，浮　欣. 新一代移动警务终端技术要求及发展趋势 [J]. 警察技术，2018 (2)：65－71.

[5] 蒋　华，姚　莹，鞠　磊. 服务链中可认证的组密钥管理方案 [J]. 计算机应用研究，2018，6：1－4.

[6] 张雪亚. 计算存储数据安全访问控制机制研究 [J]. 计算机测量与控制，2018，26 (5)：242－244.

[7] 魏　琪，林增刚，郭阳明，等. 面向移动智能终端的人体心率监护系统设计与实现 [J]. 计算机测量与控制，2019，27 (11)：30－33.

[8] 董　煜. 基于 VPDN 的移动警务安全保障系统设计与研究 [J]. 信息安全与通信保密，2007 (1)：66－68.

[9] 洪小龙，陈崇平. 视频网终端安全准入系统的设计与实现 [J]. 广东公安科技，2018，26 (4)：5－7.

[10] Ding Y L，Zhai Y Q. Intrusion detection system for NSL－KDD dataset using convolutional neural networks [A]. Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence [C]. ACM，2018：81－85.

[11] Akbanov M，Vassilakis V G，Logothetis M D. Ransom ware detection and mitigation using software－defined networking：The case of WannaCry [J]. Computers & Electrical Engineering，2019，76：111－121.

[12] 王晓妮，段　群. 基于云计算的数据安全风险及防御策略研究 [J]. 计算机测量与控制，2019，27 (5)：199－202.

[13] 徐　艳，王　茜. 网络计算环境下大容量数据安全存储策略研究 [J]. 计算机测量与控制，2017，25 (8)：147－150.

[14] 韩秀德，陈昌前. 移动警务信息资源跨网络边界安全共享策略研究 [J]. 警察技术，2018，5：43－46.

[15] 赵闻宇. 移动警务终端在公安行业的应用 [J]. 中国安防，2016 (8)：30－33.

[16] 张玉清，王晓菲，刘雪峰，等. 云计算环境安全综述 [J]. 软件学报，2016，27 (6)：1328－1348.

[17] 毋晓英，刘　冬. 移动警务在公安信息网中的应用 [J]. 数字技术与应用，2018，36 (3)：65－67.

[18] 庄烁桂. 基于虚拟专用网络的警务安全接入系统的设计与实现 [D]. 长春：吉林大学，2015.

[19] 杨宗峰，崔　松. 基于云计算的统一通信警务协同研究与应用 [J]. 计算机测量与控制，2017，25 (5)：222－224.

[20] 丁　丹. 移动终端安全管控系统开发与实现 [D]. 成都：电子科技大学，2019.

[21] Cao Q，Shen H W，Gao J H，et al. Popularity prediction on social platforms with coupled graph neural networks [A]. Proceedings of the 13th International Conference on Web Search and Data Mining [C]. Houston，Texas，UAS，2020：70－78.