计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191000114

工业互联网网络传输安全问题研究

伍育红[1]　胡向东[2]
1 重庆邮电大学计算机科学与技术学院　重庆 400065
2 重庆邮电大学自动化学院　重庆 400065

摘　要　工业互联网数据要实现互联互通必将依赖网络传输，对工业互联网而言网络传输的安全问题至关重要，应配备信息传输过程中的安全机制，应在传输两端主体身份鉴别和认证、传输数据加密、传输链路节点身份鉴别和认证方面进行安全控制。文中就工业互联网的有线传输介质与无线传输介质涉及的安全风险提出了相应的规避措施，并就数据在传输过程中如何加密及如何选择密码算法进行了深入透彻的分析，提出了多因素认证办法，并就网络传输的其他各环节提出了相应的对策。

关键词：网络传输；加密算法；身份鉴别；多因素认证；密钥管理
中图法分类号　TP406

Study on Security of Industrial Internet Network Transmission

WU Yu-hong[1] and HU Xiang-dong[2]
1 School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2 School of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract　Industrial Internet data must rely on network transmission for interoperability, and the security of network transmission is crucial for industrial Internet. It should be equipped with security mechanisms in the process of information transmission. Security control should be carried out in identity authentication of the subject at both ends of the transmission, data encryption of the transmission, and transmission link node identification and authentication. This paper proposes corresponding measures to avoid the security risks involved in wired transmission medium and wireless transmission media of industrial Internet, and makes a thorough analysis on how to encrypt the data during transmission and how to choose cryptographic algorithms. It also puts forward the corresponding countermeasures for other aspects of network transmission.

Keywords　Network transmission, Encryption algorithm, Identity authentication, Multi-factor authentication, Key management

1　工业互联网网络传输安全机制

工业互联网网络传输需要控制各传输节点、链路以及端到端的加密过程，选用合适的对称加密和公钥加密算法。工业互联网网络传输的保密性用于实现传输数据流加密，防范工业互联网通信链路上的数据信息窃听、泄露、篡改以及破坏等。工业互联网网络传输的完整性是采用数字签名方式，通过哈希或 MD(Message Digest)算法，求取其消息摘要作为数字签名。接收方采用哈希或 MD 算法得出所接收数据的数字签名，并将两个数字签名进行比对，如一致则表明该数据未在传输过程中遭受篡改，完整性未遭破坏。

对于加密传输、签名验签、鉴别和验证，必须明确要求，制定能够实现各安全域内部、各安全域之间的网络传输接口规范。在传输协议方面，应采用 HTTPS，SSL/TLS，支持 IPSec 实现远程通道的安全加密，并对 IPv4 协议与 IPv6 协议具有兼容性。比如，采用 SSL/TLS 来进行工业网络传输，保证其机密性、完整性与可用性。采用 HTTPS 协议，以 HTTP 作为通信机制，并使用 SSL/TLS 对传输的工业数据包进行加密，既能够实现网络服务器的身份认证，也能够为传输数据提供完整性与隐私保护。工业互联网平台中各 VM 之间、VM 与存储资源之间、控制主机与各下位机之间，也需要采用数据加密通道。

工业互联网中大量采用远程网络传输，根据工业应用场景，可分别选用有线或无线介质来实现。可采用的有线传输介质有 RS485、工业总线(Modbus/TCP，OPC，DNP3，Ethernet/IP，EthernetCAT 等)、宽带、光纤等。可采用的无线传输介质有无线电、工业无线局域网、光载无线通信、4G/5G/DMA 移动通信以及卫星通信等。表 1 和表 2 分别择要给出工业互联网中的有线传输介质和无线传输介质及其安全风险规避分析。

在工业网络通信传输时，可设置特定安全域中启动的安全通道流量满足最低安全基线，对使用安全通道进行传输的所有用户数据全部加密，以实现身份验证，避免中间人攻击、重放攻击等。安全域成员启动的安全通道流量可协商是否加密通信。根据工业现场的实际通信需要，可选择对安全通道数据始终加密或签名。如果远程用户请求域内网络数据资源服务，且该远程用户账户处于受信任安全域中，需要进行用户身份验证，验证通过后，获得数据库访问权限。

通信作者：伍育红(753006330@qq.com)

表 1 工业互联网中的有线传输介质及其安全风险规避分析

Table 1 Analysis of wired transmission media and security risk avoidance in industrial internet

传输介质		特点及安全风险	安全风险规避手段
工业现场总线网络	RS485 网络	普通双绞线传输，传输速率低，采用终端匹配的总线型结构，可支持 32 个节点，不支持环型或星型网络，适用于小范围、适当距离传输	尽量用于传输小数据量，不传输视频等；以一条双绞线作总线建网并串接各节点，采用单一、连续的信号通道作为总线；采用差分平衡传输，使用低阻信号地；采用隔离或旁路保护，防护高频、瞬态电磁干扰
	采用 Modbus/TCP 协议	无身份认证机制，明文传输，无完整性与机密性保护，兼具 TCP/IP 及 Modbus 双重风险。可基于 Modbus 设备修改控制器 I/O 或寄存器数值、复位、禁用，或安装新版逻辑或固件	协议深度检测及防护，可定义 Modbus 指令、寄存器及线圈列表，阻止不合规流量，防范功能码滥用；认证通信客户端与服务端身份及设备状态，保证设备不可仿冒、操作系统和组态软件可信；采用 HMAC 等算法保证数据完整性；对 Modbus 控制指令进行安全分级，对关键功能码指令采用加密相传输，保证机密性
	采用 OPC 协议	基于 COM/DCOM，不使用固定端口（使用 1024-65535）；OPC Classic 访问权限限制较宽。OPC UA 安全模式，在应用程序级强制身份认证。OPC UA 使用强安全策略加密算法。将私钥或相应证书存储于操作系统的专用存储区，并设置访问权限	防护端口，跟踪 OPC 连续建立的动态端口，开放端口最小化；采用指令防护，深度解析 OPC 协议，实时监测 OPC 客户端与服务器指令传输请求，拦截不安全指令并报警；采用操作对象防护措施，监测操作对象值以保证字节安全、可识别、可控；防范 PRC 漏洞攻击；使用可信证书连接，避免过时授权
	采用 DNP3 协议	基于串行链路的 DNP3；基于以太网的 DNP3/UDP 和 DNP/TCP，数据格式、报文结构均为公开、开放标准，缺乏认证、授权、加密，协议复杂，网络传输易遭截取、窃听、盗改，存在功能码滥用风险	采用高安全级 Security DNP3；使用 TCP/IP 安全最佳实践；使用 TLS，增加验证和授权保护；使用 ECC 与 AES 扩展 SSL，避免明文传输；采用 MAC 等算法校验数据完整性；预设通信对象白名单，防范 DoS 攻击和中间人攻击；加密 DNP3 报文链路层和应用层报文头中功能码，既安全又高效
	采用 Ethernet/IP 协议	无显示或隐式安全机制，UDP 与广播数据无实时传输控制，易遭注入伪造及注入 ICMP 控制报文攻击	使用 CIP 安全协议，执行获批措施来保证完整性，避免损坏、延迟、插入、丢失和重复等信息错误；与其他以太网系统隔离
	采用 Ethernet CAT 协议	时间同步机制易遭网络注入帧干扰，无总线授权机制易遭中间人或身份伪造攻击	与其他以太网系统隔离；使用线缆冗余、功能安全、TSN 等技术

表 2 工业互联网中的无线传输介质及其安全风险规避分析

Table 2 Analysis of wireless transmission media and security risk avoidance in industrial internet

传输介质	特点及安全风险	安全风险规避手段
无线电	实时性强，工业应用广，覆盖范围受限，避障及防雷困难，电磁干扰大	适用于中小区域、开阔地带的油气田、农业等野外区域监控，避免大范围传输，避免电磁干扰
工业无线局域网（IWLAN）	支持 IEEE802.11n/802.1acWave 2.传输速率高，适用于多种自动化等级	使用无线加密协议；修改服务集标识符，且禁用 SSID 广播；绑定静态 IP 与 MAC 地址
光载无线通信	结合 wiFi 构成光载无线通信，具备 WiFi 路由、分配及光纤分布功能	适用于港口、货场、医疗机构、大型舰艇内部等场合，尽量做到信号源现场本地化，采用主动式冗余架构
4G/5G/CDMA 移动通信	利用运营商网络并依赖其通信可靠性、安全性。低速网络传输时，实时性可达毫秒级	适用城市燃气、自来水、污水等 SCADA 系统管网监测，水电气远程抄表，电力或环保远程监控等
卫星通信	适用于上行流量小、下行流量大的点对多点广播通信	工业网络传输中，应慎用此方式。可用于大范围全流域水文观测、大面积矿藏勘探等

2 工业互联网网络安全中的身份鉴别与认证问题

2.1 传输两端主体及传输节点的身份鉴别和认证

在工业互联网领域，智能摄像头、IED、RTU 等一个不可信终端节点可能会给整个工控网络带来风险。身份认证管理的工业应用场景包括访问工业应用服务资源、登录工控主机及服务器、访问工业 PaaS 云平台等，访问其中的工业关键设备、业务系统及云平台应采用多因素认证。

身份认证要求通信双方在相互鉴别对方身份后方可通信，并保证双方物理身份与数字身份的统一。在工业应用系统中，身份认证应与该企业的业务流程密切配合，以防范对通信的非法攻击。首先要对账户权限进行合理的分类设置，遵照最小特权原则为账户分配权限。对于 SCADA 软件、CS 软件、PLC 控制软件、工控设备、工业通信装置等登录账户及密码，建议使用强口令，不得使用弱口令，更不能使用默认口令，并且应对口令进行定期更新。此外，应避免在不同的网络与系统中进行身份认证证书共享。

在工业场景中，常用的身份验证因素有知识、拥有物及固有特征等 3 种类型。知识是指用户能证明其所知信息，比如，用户访问 ID 号、口令、设备登录密码、工业业务流程细节等；拥有物是指用户拥有能证明自己身份的相应物理设备，比如，工业主机启动 U 盾、RFID 阅读器、身份验证 APP、数字签名证书、手机短信验证码等；固有特征主要是指生物特征，比如，启动上位机 HMI 的指纹、门禁系统的视网膜、控制指令的语音等。

口令认证也是工业场景常用方式之一。请求认证方需具备一个 ID，该 ID 需在认证者的用户数据库中具备唯一性。为了保证口令安全，要求其在传输过程中不得被篡改或截获。而且系统管理员可以知悉所有用户的口令，这个问题可以通过在数据库中保存口令的哈希值来解决。此外，请求认证者在发送口令认证信息前，必须确认认证方的真实性，这一点通常需要采取双向认证方式来实现。

数字签名是工业场景常用的另一种认证方式，其本质是使用公钥加密算法，通信双方无须经由网络传送口令等身份相关秘密信息，而是通过请求认证者与认证者各自对一个随机数作数字签名与验证数字签名来实现。

2.2 多因素认证问题

单因素认证对于某些工业应用场景来说仍显脆弱。使用多因素认证可以增强安全性,用户应提供多项身份确认证据,若使用者能够准确提供所要求的所有验证因素,系统方可授予其访问权限。实践中通常采用双因素认证。

在工业应用中,应注意采用多因素身份验证也存在若干风险与不足。1)验证因素可能存在丢失的情况。工业主机启动 U 盾丢失的情况屡见不鲜。需要采用手机短信验证码进行验证时,也常有手机没电或移动通信网络无法联络的情况。如果某个因素被用于多个账户认证,一旦该因素丢失,需要重新恢复所有账户,这种操作通常非常烦琐。2)因素丢失情况下恢复选项的方便性与多因素认证的初衷相互冲突。一旦多因素验证中的某因素丢失,则恢复时正常用户和攻击者事实上是处于同样的困境。但是如果多因素认证不提供恢复选项,有可能会永远无法正常登录。3)多因素验证为攻击者阻止正常用户登录提供了可能。如果攻击者设法攻破了正常用户的账户,反过来设置或重新配置多因素身份认证,将会给正常用户登录带来极大困难。

传输链路节点均应部署独立的数字证书与公钥/私钥对,实现有效身份的鉴别与认证。对于重要的设备节点,还可以采用安全芯片来实现认证。比如,质询/应答安全认证方式要求被认证方持续持有密钥。对称加密密钥为通信双方共享的密钥,而公钥加密密钥则应是被认证方的私有密钥。上述密钥一旦泄露,就会导致该认证方式全部失效。此时,可采用安全芯片实现密钥与密码强保护。一是采用安全性认证芯片实现,基于共享密钥的安全认证,可使用基于 SHA 的认证方法,也可以使用基于 RSA 的公钥加密算法。二是可以通过可配置 EEPROM 存储器,存储配置、密钥、认证证书等 PKI 认证体系要素。

3 工业互联网网络安全加密及密钥管理问题

3.1 工业网络加密传输协议的选用

工业互联网网络传输协议加密,应考虑工业现场设备计算能力有限、工业网络实时性要求高的问题,通信加密应考虑因加解密带来的额外计算量和延迟。

(1)采用 HTTPS 协议的工业网络传输

HTTPS 与 HTTP 均为 OSI 模型中的传输层协议。HTTP 本为明文传输,通信双方交互及网络传输均未认证与加密,网络传输易遭劫持、窃听或篡改。HTTP 传输时,攻击者可将恶意网址嵌入服务器发给用户的 HTTP 数据包中,用户界面出现该恶意网址链接或被劫持至其他 URL。

HTTPS 在 HTTP 应用层及 TCP/IP 中附加 SSL/TLS 层,实现了传输数据加解密,保证了网络传输安全。服务端与客户端信息传输均通过 SSL/TLS 加密,传输密文数据。将证书中的公钥传送给客户端,客户端 TLS 通过解析证书来验证该公钥的有效性,如有效则用该密钥对生成随机值进行加密,并传送给服务端,服务端对其解密后,双方即可使用该随机值来实现通信加解密。HTTPS 在传输环节使用协议加密,但攻击者仍可在客户端截取数据包分析传输内容与协议,为此,可视情况进一步对传输数据内容加密。因为非对称加密在大素数生成、计算及分割上均需耗费较多资源,首次握手宜采用 RSA,DSA/DSS 等公钥算法来加密后续的对称加密密钥,后续网络传输宜使用 AES,RC4,3DES 等对称加密算法。哈希算法宜选用 SHA1,SHA256,应谨慎选用 MD5。但是,这种方式依然存在风险。虽然攻击者无法直接调用 API 来伪造数据,但对模拟器运行工业应用程序或者在工业应用程序运行的机器上来伪造数据的攻击方法有效。对数据内容进行加密,本质上仍然是在客户端采集数据、经由网络传输,因此这种方法只是提升了攻击难度,并未从本质上解决工业互联网网络传输的完整性问题。

(2)多种协议软硬件加密。

可在工业通信协议的基础上增加 VPN 加密通信方式,采用 IPSec,OPENVPN,GRE,SSTP 4 种加密协议实现加密传输。加密通信方式可选择硬件加密,也可以选择软件加密。软件加密依赖于操作系统等运行环境,加解密运算需要占用嵌入式系统微控制器或处理器资源,导致业务系统性能下降,而且易受攻击和出错。硬件加密采用定制 IC,无性能损失,而且可以对 IC 采取封装等物理攻击防范措施。不同的工业应用场景可采取不同的加密算法设计,比如智能终端配件验证可选用 ECC 163 椭圆曲线加密算法;现场智能设备的许可权管理等验证可选用 ECC 256、SHA 256 加密算法。有些 IC 模块还提供简单编程功能,甚至可以提供更高级别的安全能力,比如安全身份认证、加密通信、密钥安全存储及运行固件更新安全保护等。此外,还可以使用标准化可信平台模块,既能够实现高复杂性加密,也能够完成大量密钥及签名的安全存储,还能够对所存储数据的物理读取进行保护。

实现工业网络的加密传输及存储,不仅需要有效的加密工具,同时还需要完善的密钥管理机制来配合密钥存储、使用、分发、更新及销毁等全生命周期安全管理。

3.2 工业互联网网络安全中的密钥管理设计

传统信息系统中的密码设计 Kerckhoffs 在工业互联网环境中仍然适用,其核心是"密码系统安全性取决于密钥保护,而非密码系统保护",而且密钥需要由通信双方事先约定,并根据指定的协议定期更换。因此,工业环境中的密钥的保护与安全管理问题极为重要。有统计表明,数据加密存储的 5 个最差实践中,3 个与密钥管理有关,分别是密钥保存位置错误、密钥未集中管理、系统使用用户自己设计的密钥存储方案。在工业控制领域,这些最差实践较为常见。

现代密码学中的密钥管理多借助信息手段来实现自动化管理,由密钥分配中心(Key Distribution Center,KDC)负责密钥的集中管理。密码系统均有一定的保密期,需要及时更新,因此密钥管理愈加复杂。密钥管理覆盖了密钥自产生到最终销毁的全生命周期,包括系统初始化,密钥的生成、分配、存储、备份、恢复、吊销、销毁、保护、丢失等,其中,密钥的生成、分配与存储为其核心环节。KDC 的证书机构需要维护用户的公钥注册、存储、分配、查询、吊销等工作,这些工作又需要通过认证、时间戳、协议、签名、证书、加解密、可信第三方等手段来实现。

工业互联网中密钥管理设计的若干原则如下。

(1)密钥密文存储原则。除非密码装置足够安全,否则不得以明文存储密钥。在工业控制领域,使用人工分配密钥的情况仍较普遍,此时应注意,密钥不得以明文方式由单个实体控制,而应以密钥分量方式由多个具体信任关系的实体共同管理。

(2)密钥分离性原则。不同通信实体之间不应使用相同或具有相关性的密钥,避免因一对通信实体安全通信出现问题,影响其余实体的安全通信。

(3)密钥备份原则。如因系统故障等原因造成密钥丢失(而非失窃),可通过恢复密钥备份来修复系统。备份密钥的

安全强度应不低于原始密钥的安全强度。

(4)密钥时效性原则。一旦密钥超出有效期，必须更换为新密钥。而且，新旧密钥的安全性应该分离，即便旧密钥遭窃也不应影响新密钥的安全性。

(5)密钥多级管理原则。工业互联网中的关键网络传输需要一次一密，而密钥需由一个实体生成并安全传输至对方，因此，通信双方应使用同一个加密密钥来实现各工作密钥的加密。通常采取三级密钥管理措施。具体的密钥管理级别从上而下依次是：主机主密钥(Host Master Key，HMK)、密钥加密密钥(Key Encryption Key，KEK)、数据密钥(包含用户密钥以及会话密钥)，用于给主机、网络节点和网络用户等的保密通信分配大量的密钥。主机主密钥存于主机处理器中，为本地主密钥(Local Master Key，LMK)，用于对其他类型的密钥进行加密。工业应用场景中生成主机主密钥时，应通过自然随机现象中的随机模拟信号数字化来产生真随机数。比如，物理噪声源中的 MOS 晶体管、电阻等电子元器件热噪声，经过放大、滤波、采样、量化后，产生随机密钥。KEK 用于加密所传送的数据加密密钥，完成数据密钥的自动分配。KEK 又分为终端主密钥(Terminal Master Key，TMK)、区域主密钥(Zone Master Key，ZMK)等，既可用真随机性方法来产生，也可用 MK 作为某个强密码算法输入的方法来生成。数据加密密钥即工作密钥，由会话密钥和用户密钥组成，加密数据的密钥由会话密钥与用户密钥共同生成。数据加密密钥的可用形式有终端 PIN 密钥(Terminal PIN key，TPK)、终端认证密钥(Terminal Authentication Key，TAK)、区域 PIN 密钥(Zone PIN Key，ZPK)、区域认证密钥(Zone Authentication Key，ZAK)、PIN 校验密钥(PIN Verification Key，PVK)、卡校验密钥(Card Validation Key，CVK)等，用于工业应用中各种数据的加密、认证及数字签名等。

3.3 工业互联网网络安全中的密钥协商与分配

数据加密密钥的更新周期比较短，每次通信时均使用不同的会话密钥，即可满足所谓的“一次一密”，可在密钥加密密钥控制下，由密钥生成算法来动态地产生数据加密密钥。上级密钥用于下级密钥加密：主机主密钥数量最少、相对不变，用于对密钥加密密钥进行加密；密钥加密密钥数量较少，用于对数据加密密钥加密；数据加密密钥则用于对数量巨大的工业数据加密。需要保证仅有极少量的主机主密钥明文存储于采取严密物理保护的主机密码装置之中，密钥加密密钥和数据加密密钥在加密后密文存储于其他存储器中。此外，应对密码装置配备防窜扰设施，一旦核心密码装置遭到物理破坏，其中的主密钥和其他密钥可自动清除或自毁。

工业网络通信建立密钥可采用密钥协商或密钥分配方式，二者的主要区别在于是否有可信第三方参与。密钥协商通过一个交互协议来共同确定新会话密钥，无需可信第三方机构介入；密钥分配则需要通过可信第三方来选取密钥并分配给通信各方。

通信各方通过公开信道通信来协商，共同形成密钥，任一参与者均对协商结果产生影响，甚至不需要可信第三方参与，可通过 Internet 密钥交换协议(Internet Key Exchange，IKE)等密钥协商协议来实现。密钥最终由协商协议各参与者独立产生的参数作为输入量计算而得，计算值即为密钥。该密钥由协商各方共享，除可能的可信管理机构之外的任何他方均不可知。

证书型和无证书型两种密钥协商协议生成方式的区别在于是否有第三方可信管理机构(如 Certificate Authority(CA))等。证书型密钥协商协议由证书认证中心提供认证，生成密钥时，认证中心为参与密钥协商的各方各分发一个含有参与方公钥、ID 以及其他信息的证书。此方案的优势是可实现认证，如果资源允许，可直接使用 PKI 以便部署应用，同时，采用私钥生成器(Private Key Generator，PKG)又易于公私钥统一管理。在工业网络通信场景中，需要考虑到该协议需可信 CA 参与密钥协商运算，计算成本高，还需要维护相关证书。如果资源受限，应慎重选择。无证书型密钥协商协议无须使用证书和 CA，计算量小，而且其安全性不低于证书型密钥协商协议，特别适用于工业网络资源受限的环境，比如工业 WSN 等低耗环境。不过，这种协议的设计较为困难。

工业现场通信中，资源和通信有效期均受限的两个不信任节点，如要保证临时安全通信，可建立安全弱连接受限通信。在通信链路上协商出一个临时会话密钥，用于安全通信，一旦密钥超出有效期，即中断该安全通信。通信规模及节点数 n 较少而且节点不常增加时，可采用预设密钥方式，各方均存储 $(n-1)$ 个密钥，通信系统需存储 $n*(n-1)$ 个密钥，一旦节点增加，需要存储的密钥将会呈指数级增长。其他工业网络通信可借助一个中心节点，采取中间人保方式来实现密钥协商。一旦经由中心节点协商成功，在协商所得密钥失效前各方无法抵赖，且不再需要中心节点参与，这对于通信和计算资源受限的工业网络来说非常重要。这种密钥协商方案与具体的传输协议无关，可以采用 Blueteeth，WiFi，NB-IoT，4G/5G，LoRa 等通信体制传输。密钥有效期的存在还可以防御重放攻击。不过其安全风险在于：中心节点如果失效将导致整个加密通信系统密钥协商失败。当网络规模较大(比如油气田各种传感数据传输)时，可以采用完全去中心化的 P2P 区块链技术手段，网络规模大决定了欺骗成本高，间接保证了这种方案的安全性。

密钥分配问题较为复杂，因为密钥安全分发和传输相对困难。密钥分配协议对密钥分配的规则和约定进行了规定，并控制密钥分配过程。工业网络信息传输场景中，应尽量选用传输量和存储量都比较小的协议，尽可能采用自动分配机制，以适应工业场景的分配效率要求。密钥分配可采用网外分配(人工分配)、基于 KDC 的分配(自动分配)以及基于认证的密钥分配(自动分配)等方式。

人工分配借助非通信网络的可靠物理渠道来携带密钥，并分配给通信参与各方。比如，在工业网络通信中使用 U 盘来人工拷贝分发密钥。工业场景中，如用户量较大、通信较频繁，密钥需求量随之增加，密钥传输量和存储量也随之增大，密钥需频繁更换，成本较高。此外，对参与人员的可信任度要求很高。

自动分配以 KDC 为可信第三方来实现密钥分配。通信一方凭借己方密钥和 KDC 公钥，即可经由 KDC 获得另一方的公钥，构建保密通信信道。该方法常使用 Kerberos 协议的拉模式(Pull)和推模式(Push)，如图 1 和图 2 所示。拉模式中通信一方主动请求密钥，故此得名。推模式中，通信方 A 先联系另一方 B，推动 B 与 KDC 联系获取 A 和 B 之间的会话密钥。二者的安全性并无明显差异，可根据具体的应用环境选用。在工业网络本地环境中，可采用 Kerberos 协议实现认证管理。在采用 ANSI X9.17 的广域网环境中，可直接由服务器来方便获取密钥，因为客户机通常距 KDC 部署较远，

(下转第 380 页)

tional Publishing，2014：143-163.
[5] KORCZYNSKI M A. Classifying Service Flows in the Encrypted Skype Traffic[C]// 2012 IEEE International Conference on Communications (ICC). 2012：1064-1068.
[6] WANG T，CAI X，NITHYANAND R，et al. Effective attacks and provable defenses for website fingerprinting[C]// 23rd {USENIX} Security Symposium ({USENIX}. 2014：143-157.
[7] CHENG G，CHEN Y X. Encrypted Traffic Identification Method Based on Support Vector Machine[J]. Journal of Southeast University(Natural Science Edition)，2017(4)：655-659.
[8] CHEN W，HU L，YANG L. Fast Identification Method of Encrypted Traffic Based on Load Characteristics[J]. Computer Engineering. 2012(12)：22-25.
[9] ZHANG B Y. Analysis of the Principle and Application of HTTPS Protocol[J]. Network Security Technology and Application，2016(7)：36-37.
[10] XU P，LIN S. Traffic Classification Method Based on C4.5 Decision Tree [J]. Journal of Software，2009(10)：2692-2704.
[11] LIU K. Research on feature selection in network flow classification [D]. Yangzhou：Yangzhou University，2013：18-19.
[12] ZHOU Z H. Machine Learning [M]. Beijing：Tsinghua University Press，2016：73-79.

ZOU Jie，born in 1996，postgraduate. Her main research interests include machine learning and network traffic analysis.

ZHU Guo-sheng，born in 1972，Ph.D，professor. His main research interests include next-generation Internet and software-defined networks.

（上接第 368 页）

测效果的比较，随机森林算法的分类效果要好于 C4.5 决策树，但这并不否定决策树的分类作用，因为不同的数据挖掘算法都有其优势和劣势，我们应当从微博用户的各类特征出发，在提取有效特征的基础上与传统数据挖掘算法结合使用，以起到仅使用其中一种方法所不能达到的良好效果。

结束语　随着对微博用户行为研究的不断深入，对微博上的大量异常用户的检测与识别也引起了学术界和产业界的重视。本文基于用户特征对微博异常用户分类方法进行分析，在获取到的微博用户数据的基础上，通过对用户基本属性、行为模式和文本内容的分析，提取相关特征并进行聚合，完成对数据的预处理。随后选取 Weka 作为分析工具，以微博用户数据集为样本，对微博的传播特点以及用户属性、文本内容等特征进行综合考量，将数据挖掘算法融入对新浪微博异常用户的检测方法当中，建立起微博异常用户检测模型，先后选取 C4.5 决策树和随机森林分类算法完成了模型训练和实验预测，并对其准确率进行了评估。本文结果可以为公安机关开展舆情管控工作提供参考。

参 考 文 献

[1] 中国互联网信息中心. 第 43 次中国互联网络发展状况统计报告[R]. 北京. CNNIC，2019.
[2] FABRICO B，MAGNO G，RODRIGUES T，et al. Detecting spammers and content promoters in online video social networks [C]// Proceedings of the 32nd International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM，2009：620-627.
[3] BENEVENUTO F，MAGNO G，RODRIGUES T，et al. Detecting spammers on twitter[C]// Collaboration，Electronicmessaging，Anti-Abuse and Spam Conference. Washington，2010：6-12.
[4] STRINGHINI G，KRUEGEL C，VIGNA G. Detecting spammers on socia networks[C]// Proceedings of the 26th Annual Computer Security Applications Conference. ACM，2010：1-9.
[5] 彭希羡，朱庆华，刘璇. 微博客用户特征分析及分类研究——以“新浪微博”为例[J]. 情报科学，2015，33(1)：69-75.
[6] 刘勘，袁蕴英，刘萍. 基于随机森林分类的微博机器用户识别研究[J]. 北京大学学报，2015，51(2)：289-300.
[7] APHINYANAPHONGS Y，RAY B，STATNIKOV A，et al. Text classification for automatic detection of alcohol use-related tweets：A feasibility study[C]// 2014 IEEE 15th International Conference on Information Reuse and Integration(IRI). IEEE，2014：93-97.
[8] 蒋鑫. 基于属性约简的社交网络异常用户识别系统的设计与实现[D]. 北京：北京邮电大学，2016：2-3.
[9] 夏崇欢. 基于行为特征分析的微博恶意用户检测方法[D]. 南京：南京邮电大学，2018：5-6.
[10] 郝亚洲，郑庆华，陈艳，等. 面向网络舆情数据的异常行为识别[J]. 计算机研究与发展，2016，53(3)：611-620.
[11] 张玉清，吕少卿，范丹. 在线社交网络中异常帐号检测方法研究[J]. 计算机学报，2015，38(10)：2011-2027.
[12] 吴大鹏，司书山，闫俊杰，等. 基于行为特征分析的社交网络女巫节点检测机制[J]. 电子与信息学报，2017，39(9)：2089-2096.
[13] 刘琛. 基于行为分析的社交网络异常账号的检测[D]. 北京：北京交通大学，2017.
[14] 孙洋. LBSN 中基于好友聚类的社交搜索系统设计与实现[D]. 南京：东南大学，2017.

YUAN De-yu，born in 1986，Ph.D，lecturer. His main research interests include cyber security，and complex networks.

GAO Jian，born in 1982，Ph.D，lecturer. His main research interests include botnet，malware analysis and cyber crime.