[机器人]

油气田陆岸终端机器人巡检无线网络安全研究与设计

文/邓增利[1] 彭 晶[1] 陈建华[2]
1.中海石油（中国）有限公司湛江分公司；2.中海石油（中国）有限公司海南分公司

通过对油气田陆岸终端机器人巡检无线网络的建设，根据实际建设的环境，针对陆岸终端所处的环境及网络安全环境进行分析，通过网络安全架构规划、网络信息防泄密及网络安全设备这三个方面进行分析，提供相应的应对措施，并通过防火墙、上网行为管理及无线分析等方面的安全防护部署，提升陆岸终端巡检机器人的无线网络安全，进一步提升油气生产的信息安全。

石油行业正在遭受全球能源格局变化带来的巨大冲击，为了进一步提升开采效率，降低开采成本，新一代的信息技术将成为推动石油行业发展的动力源泉。国际各大石油公司陆续将数字化转型作为未来技术发展的方向之一，巡检机器人作为新一代信息技术的衍生品，可以代替人工巡检，从而大大减轻现场作业人员的工作量，同时提升油气设施的安全性，该技术目前正逐步在石油开采领域中推广使用，成为油气开发生产持续提质、降本增效的有效途径。巡检机器人在海上油气田设施使用的过程中，受所处环境制约，通常会采用无线网络覆盖的模式来实现管理系统与巡检机器人的数据通信。机器人无线通信的方式无论是基于4G/5G还是基于WiFi，其相对于有线网络而言，网络安全防护的难度都会有所提升。

油气田陆岸终端是海上油气田的陆地处理设施，通常处在海洋油气管线的上岸处，陆岸终端相对于海上采油平台而言，其无线网络安全受到的威胁更加严重。在陆岸终端，用于机器人巡检的无线局域网通常被部署在一个相对大的场所，以满足机器人巡检的基本要求，无线网络信号的覆盖范围不可避免地超出陆岸终端常规的护栏防御范围。随着计算机技术的不断发展、无线网络的大量使用及移动设备应用的普及，无线网络安全防御的提升也变得更加重要，对于陆岸终端来说，为了保证巡检机器人无线网络需求，同时还要保证油气生产数据安全，就需要综合利用各种网络安全防护技术来保障无线数据的信息传输过程。

机器人巡检无线网络安全的需求分析

机器人巡检无线网络的使用需求与传统无线网络的需求一致，只是在安全性上有更高的要求。机器人巡检传输的数据信息为工业系统的重要数据，机器人巡检目的是为了代替人工巡检，需要将现场重要设备的参数及图像传送到机器人巡检平台上，这些工业数据在油气生产中通常为企业的核心数据，数据安全方面需要得到高度保障。陆岸终端通常在海岸附近，有相关的安全防护措施进行厂区防护，一般人难以进入到终端内部进行数据窃取。但是机器人巡检的信息通过无线网络形式进行传送，很容易被附近的不法分子进行窃听和获取。虽然陆岸终端的信息安全做了基本的防护，但网络信息安全的技术更新很快，需要更多新设备来提升防护能力，以满足油气田的安全防护要求。

1. 提升无线网络安全规划

为了提升机器人巡检无线网络的安全性，无线网络安全架构至关重要，通常决定了网络安全防护的整体能力，网络安全架构对于网络安全防护来说就是防护的基础，决定着一个网络防护的成败。

2. 防止窃听和截取网络数据

由于无线网络的开放性，相对于传统的有线网络，安全性低很多。为了实现网络信息的保密性，必须实现该信息对除特定环境以外的任何人都不可读取。为了保证机器人巡检数据的安全，必须采取一定的手段来隐藏信息，从而防止机器人巡检的数据通过无线网络泄露出去。

3. 无线网络安全设备欠缺

在陆岸终端中，网络通常通过公司整体部署的基本有线网络设备进行防护，较少针对无线网络的无线信号进行安全防护。对于无线网络设备的安全来说，相对的开放性存在很大的安全隐患，没有坚固防护能力的无线网络安全设备，难以保障无线网络的安全。无线网络的安全保护系统通常由无线入侵检测系统（WIDS）和无线入侵防御系统（WIPS）组成。无线入侵检测系统用于无线局域网中监控各个用户的活动情况，分析和判断入侵事件，检测非法的网络活动，对异常的网络流量进行报警；无线入侵防御系统的工作原理是监测无线系统网络中未经授权的异常接入（入侵侦测），根据实际情况采取相应措施处理问题的网络设备。常规网络安全防护使用的主要是下列安全设备：防火墙、网行为管理系统、链路负载均衡、网络带宽管理系统及IPS入侵防御系统等，在陆岸终端，针对无线网络安全防护的设备能力较弱，亟需得到提高。

巡检机器人无线网络系统安全设计

1. 无线网络系统安全架构设计

本次的机器人巡检无线系统采用分层结构，全网分为接入层、汇聚层和核心层，网络层次间进行了安全区域边界的安全防护，无线系统接入的安全防护措施采用了集中管理、集中认证及集中部署的安全策略。

本次无线组网设计遵循X.805的网络安全隔离机制，体系架构组成如图1所示。

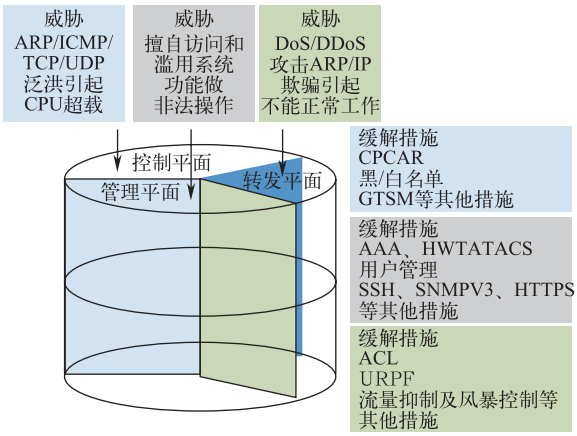

图1　X.805三层三面安全隔离与防御机制图

1）管理平面。主要职能是负责用户的数据安全，主要针对用户的应用和业务数据进行防护，也是管理用户的操作过程、维护过程和各种管理信息。

2）控制平面。由于WLAN设备是基于各种各样的公共通信协议来完成特定的业务功能，通信协议的开放性决定了通信协议不可避免地会被攻击和仿冒，因此需要关注各种通信协议的安全性。

3）转发平面。数据、信息数据包的转发都是基于相应IP报文的目的地址（如MAC地址和IP地址）进行转发和交互的，网络上对于信息转发过程的防护主要是防范入侵者对数据链路上各种转发设备进行的攻击，进而阻止入侵者获取数据或者入侵系统。

2. 无线安全策略设计

依据无线网络安全防护的需求，计划将机器人巡检无线组网安全加固策略分为Level-1、Level-2。

1）Level-1。代表的是必须要配置的安全加固策略。①无线用户接入安全；②无线控制器防攻击加固；③无线流量抑制。

2）Level-2。代表的是加强的安全加固策略，根据实际情况进行配置调优。①CAPWAP控制隧道加密；②无线攻击检测和反制；③防ARP欺骗攻击。

3. 无线网络安全设备设计

无线网络系统通过架设防火墙、上网行为管理、无线分析系统及日志审计系统等网络安全设备，对无线网络、油气田陆岸终端网络及服务器之

间的数据流和业务访问做了安全管控，通过精确检测和阻断各种类型的网络攻击，将各种网络攻击对被保护对象的影响降到最低，有效保护各个网络用户，稳定网络。

机器人巡检无线网络安全部署研究

1. 防火墙部署

防火墙部署的安全防护配置信息。

1）安全策略控制。当各种数据流量经过防火墙时，防火墙就会根据配置好的管理策略对数据流量的数据帧进行核查，也就是进行属性的匹配和识别，符合放行策略的数据包被放行，符合阻断策略的数据包被阻断，从而保障被保护网络的数据安全。此外，用户还可以根据需求设置其他的附加功能，例如记录设备的运行日志、配置会话的老化时间以及自定义长链接等，通过这些管理手段进行网络的运维管理。

2）防病毒检测。防火墙也具备防病毒入侵的功能，在某些数据放行策略中启用了防病毒检查后，可以对这些策略的数据流量进行防病毒检查，带有病毒特征的数据包被阻断丢弃，同时，防火墙的病毒库还可以定期更新，从而有效保障被保护网络的数据安全。防火墙一般放置于被保护网络的出入口，可以将病毒有效抵御于被保护网络之外，为机器人巡检无线网络的安全提供一个坚固的保护层。

3）入侵防御。防火墙带有入侵防御功能，通过分析流经防火墙的数据流量，针对网络上常见的攻击行为（如DDoS攻击、缓冲区溢出攻击及木马活动等）进行有效的阻断。通过在放行流量策略中启用入侵防御功能，同时定期更新入侵库，可以有效保护机器人巡检信息系统和网络架构免受各种网络侵害。

2. 上网行为管理系统部署

上网行为管理部署的基本配置。

（1）完善的网络安全接入部署

1）网络安全接入的安全认证包含有用户名/密码认证等的Web认证、短信认证以及第三方认证等，通过网络安全接入认证可以有效阻断大部分非法链接。

2）对网络上各种病毒进行检测和防护，同时还包含了入侵防御的部署。

3）对各种网络资产进行有效识别、管理及对各种异常的网络设备接入进行检查和记录。

（2）精准的上网行为管理部署

1）通过对各种常用的网络应用和网址进行识别和审计，可以让网络管理员更加灵活地管理网络上的各种应用。

2）通过管理系统提供的各种审计日志，可以让网络管理员轻松管理用户的各种上网行为，如用户所访问的各种网址、每个用户所产生的流量数据以及各个用户终端的信息等。网络管理员可以通过对这些信息的管理实现对网络的精细化管理。

3）通过对管理日志的管理，以及将日志管理数据传送到其他综合管理平台，可以有效管理网络上用户的各种上网行为。

（3）精细的流量控制部署

1）借助五元组的特性，可以灵活差异化管理各个用户的数据流量。

2）通过对数据流量的动态管理，可以充分利用各个空闲流量，通过动态调整给有需要的用户，间接扩大网络的使用带宽，实现网络带宽的充分利用。

3）通过对网络时长和网络流量的综合管理，可以制定各种适合用户需要的上网套餐，满足各个用户的实际需求。

（4）简化的运维管理部署

1）可以将设备的配置文件灵活保存到各种移动存储设备，在需要恢复配置文件时可以快速使用移动存储的备份文件，简化系统管理员的运维管理操作。

2）通过专门的系统管理软件可以对各个上网行为管理设备进行集中管理和监控，同时实现对策略的集中管理和策略的统一下发操作。

3）通过IPSec VPN协议栈动态化技术的动态学习功能，可以将整个网络各个网络节点的设备配置进行集中调整，简化了网络管理的难度。

3. 无线分析系统部署

无线分析系统部署的配置。

（1）无线健康度检测

1）对无线系统的各种关键运行指标进行健康度检查和诊断，判断无线系统当前运行的状态是否正常，各个用户的接入情况是否运行良好。所检查的

关键运行指标有吞吐达标率、接入耗时和接入成功率等。

2）通过各种算法，对管辖网络进行健康度分析，判断各个区域的健康情况，便于运维人员识别出网络的问题，同时通过调整运维指标来调整网络状态，使各个网络区域都能达到最佳状态。

（2）无线拓扑展示

在无线分析系统的后台，控制器将区域、楼栋、楼层、障碍物、背景图、比例尺、真实AP及预部署AP的增量数据同步到WLAN拓扑系统，WLAN拓扑能根据同步过来的数据提供可视化拓扑展示能力。

（3）网络流量分析

网络运维人员可以利用Netstream技术对网络流量的指标进行分析和研究，从而灵活地对网络进行各种精细化管理，满足各个用户的网络需求。运维人员还可以利用Netstream技术将网络的流量信息提交给分析器进行分析，利用分析器的强大功能进一步得出统计分析结论，这样就可以更有效地管理网络。

（4）智能无线射频调优

基于AP的射频信号和邻居数据，评估射频得分和待提升AP数量，通过AI算法实时仿真优化效果，并给出信道调整建议。

结束语

随着全球数字化、智能化程度的日益提高，石油企业的网络安全问题日益受到关注。海洋石油是国家石油的关键领域，海洋石油工业系统的网络安全尤为重要。所以必须加强网络安全的管理，通过各种技术手段排除网络安全隐患，筑牢网络安全防线。

油气产业未来的发展将借道数字技术的深度应用来进一步实现行业的降本增效。而在此期间，以机器人为代表的数字技术将是石油企业实现生产降本、安全管理效能提升的有效工具。无论是巡检机器人还是人工智能、可穿戴设备等数字化应用设备，无线网络覆盖的安全性仍将是未来数年石油行业需要面对和解决的问题。通过对油气田陆岸终端巡检机器人无线网络安全的研究，给海上油气设施和陆岸油气设施的无线网络安全提供一种信息安全解决方案，帮助这些设施进一步提高网络安全管理能力。**EA**

（收稿日期：2022-04-11）

参考文献

[1] 姜虹．无线网络安全[J]．计算机光盘软件与应用，2014，17(8)：2．

[2] CHRIS HURLEY．无线网络安全[M]．北京：科学出版社，2009．

[3] 单光星，惠熠，周志强，等．无线网络安全问题初探[J]．网络安全技术与应用，2016(10)：2．

[4] 杨利彪．核电厂无线通信网络技术选择[J]．电气应用，2021，40(11)：77-83．

[5] 吴银伟，郭 璇，孙琦毓．核电厂无线通信网络电磁兼容性研究[J]．电气应用，2021，40(3)：29-34．

[6] 成健，胡力广，詹威鹏，等．电力监控系统网络安全态势感知研究[J]．电气应用，2020，39(7)：86-89．