DOI:10. 3969/j. issn. 1674-1951. 2021. 03. 004

基于SDN的边缘物联代理安全性风险及防御性技术综述

Security risk and defensive technology of Edge IoT agent based on SDN

韩坚[1],刘松[1],魏吟斌[2*],李彬[2],祁兵[2]
HAN Jian[1], LIU Song[1], WEI Yinwu[2*], LI Bin[2], QI Bing[2]

(1.国网江西省电力有限公司萍乡供电分公司,江西 萍乡 337000;2.华北电力大学 电气与电子工程学院,北京 102206)
(1.State Grid Jiangxi Electric Power Company limited, Pingxiang Power Supply Branch, Pingxiang 337000, China; 2.School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China)

摘 要:当今社会正在从互联网时代向物联网(IoT)时代发展,新兴的物联网正面临着巨大的可扩展性和安全性挑战。一方面,物联网设备存储计算能力有限,边缘云和边缘计算给物联网提供的外部援助有望增强物联网的可扩展性。另一方面,由于资源限制,物联网设备面对恶意攻击的抵御能力相对薄弱。针对这些挑战,研究了基于软件定义网络(SDN)的边缘物联代理安全性风险,比较了基于SDN网络进行网络入侵检测防御的最新研究成果。

关键词:边缘物联代理;软件定义网络;安全风险;防御技术;网络入侵检测;物联网;边缘计算
中图分类号:TK 01+8:TP 13 **文献标志码**:A **文章编号**:1674-1951(2021)03 - 0020 - 05

Abstract: During the development from the era of internet to the era of Internet of Things (IoT), the emerging IoT is challenged on its scalability and security. On the one hand, the storage and computing capacities of IoT devices are limited, while the external assistance provided by edge cloud and edge computing is expected to enhance the scalability of the IoT. On the other hand, constrained by current resources, IoT devices can hardly resist malicious attacks. Aiming at these challenges, the security risk of Edge IoT agent based on Software Defined Network (SDN) is studies, and the latest research results of network intrusion detection and defense based on SDN network are analyzed.

Keywords: agent of Edge IoT; Software Defined Network; security risk; defense technology; network intrusion detection; Internet of Things (IoT); edging computing

0 引言

2020年5月,国家电网有限公司互联网部、设备部、营销部、物资部共同牵头,组织开展并发布了《智慧物联体系总体设计(2020版)》。智慧物联体系总体架构遵循“精准感知,边缘智能,统一物联,开放共享”的技术原则,通过物联管理和边缘物联代理等平台以及设备、标准化接入各类采集终端,实现业务融合贯通。

物联网设备的计算能力有限,包括存储、处理和通信资源,无法有效地在本地执行计算量大而密集的任务。边缘计算通过使计算更接近物联网边缘来解决资源限制问题。在整个网络中提供分布式边缘节点可减少集中计算的压力,同时克服物联网中的数据传输延迟。软件定义网络(Software Defined Network,SDN)通过向运营商呈现网络的全局视角来实现有效的网络管理。它可为物联网集中处理繁杂信息提供动力,有助于物联网服务协调[1]。SDN通过收集、分类和分析移动边缘的物联网数据流,基于SDN架构建设边缘物联代理平台,与云平台形成一种协同关系,有助于提高物联网系统的可扩展性,构建智能、开放、安全、友好的弹性网络。

由于SDN架构存在安全风险,并且边缘物联代理对用户信息安全的隐私防护有很高要求,分析基于SDN的边缘物联代理存在的安全风险以及可采用的防御技术具有重要意义。

SDN架构的防御方案中,一种主动安全防御框架能够将控制器的业务逻辑和安全功能解耦,并将

收稿日期:2020-12-18;**修回日期**:2021-02-25
基金项目:国家电网有限公司科技项目(SGJXPX00FCJS1900269)

安全功能部署在数据转发层和控制层之间，实现为不同的控制器提供统一的安全防御框架的功能[2]。另外的防御思路聚焦于SDN架构中的OpenFlow协议，通过分析SDN可能遭受的攻击手段总结未来SDN安全的研究趋势[3]。基于数据备份和恢复（DBAR）技术，文献[4]提出了一种新的防御机制，有望在SDN架构中实现防御功能。随着机器学习在安全监测与防御领域不断发展，针对SDN架构受到分布式拒绝服务（Distributed Denial of Service，DDoS）攻击，文献[5]提出基于C4.5算法产生的决策树的检测方法。

1　基于SDN的边缘物联代理架构

由于物联网具有数据量大、交互速度快等特征，互联网的可扩展性和效率不足以处理物联网大数据。因此，在保证用户隐私的前提下，设计一个数据共享框架使用户能够获得物联网服务迫在眉睫。文献[6]提出一个高效灵活的边缘物联代理架构EdgeIoT，它利用雾计算和SDN来收集、分类和分析移动边缘的物联网数据流。而边缘物联代理装置是物联网感知层数据汇总、安全控制的核心设备，是区别于传统状态监测项目建设的关键所在。因此建议基于雾计算，面向泛在物联网连接需求，建设边缘物联代理平台，屏蔽底层网络差异性，实现全连接。平台具备模型适配、连接管理、数据存储和转发、边缘计算、安全代理及防护等功能，打破纵向封闭模式，实现网络边缘智能[7]。边缘代理平台将强大的计算存储能力与用户满意的业务服务能力向用户侧倾斜，向网络边缘迁移，与此同时大量应用、服务和相应计算分析内容可实现个性化、近距离和分布式的特点。边缘物联代理位于电力物联网的感知层，利用设备本地通信接口对各类传感器、终端等设备接入并统一管理，通过协议解析将业务数据提取、汇聚及存储，并按物模型要求进行标准化建模，利用边缘计算能力对业务数据处理后发送至平台层。边缘物联代理宜具备本地通信、远程通信、协议解析、数据存储及处理、设备信息建模、边缘计算、设备管理、安全防护等功能模块。边缘物联代理的功能如图1所示。

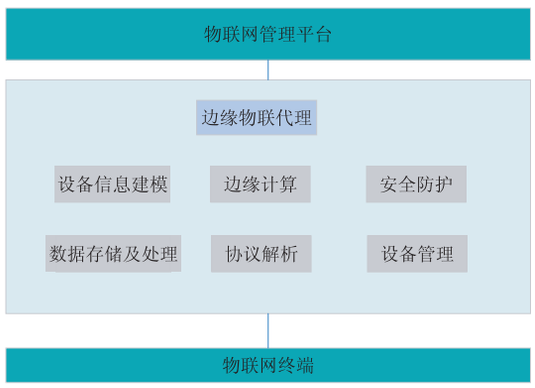

图1　边缘物联代理的功能

Fig. 1　Edge IoT agent function

2　基于SDN的边缘物联代理安全风险

2.1　SDN架构概述

利用分层的思想，SDN架构将数据与控制分开，从上到下分为应用程序层、控制层、数据转发层。控制层包括逻辑中心化和可编程的控制器，控制器可掌握全局网络信息；数据转发层包括“哑的”交换机（与传统的二层交换机不同，专指用于转发数据的设备）。交换机由于只提供简单的数据转发功能，实现快速匹配数据包并转发，可适应日益增长的大流量转发需求；在应用程序层，网络运营商被允许快速响应各种业务需求，构建出各种可在SDN控制器之上运行的应用程序软件[8]。因此，SDN技术不仅能够有效降低设备负载，协助网络运营商更好地控制基础设施，降低整体运营成本，还可应用于任何网络，通过引入可扩展的应用满足运营商不同需求。SDN基础架构如图2所示。

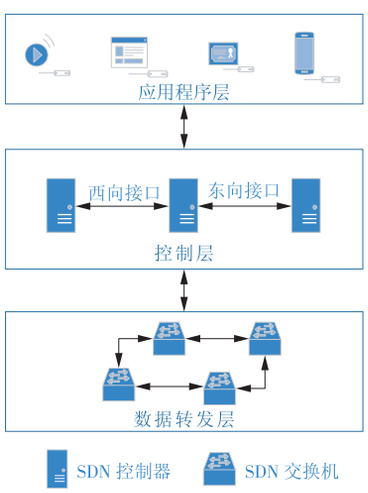

图2　SDN基础架构

Fig. 2　Architecture of SDN

2.2　SDN架构的安全风险

SDN虽然发展迅速，能够适用边缘物联代理，但也带来了一系列安全问题。首先，SDN的开放性使得攻击者更容易获得有关网络、服务和交互的相关信息。其次，对于集中式的SDN控制器，某些攻击，如拒绝服务（DoS），其影响可能比仅针对单个路由器的影响更大。最后，一些新的功能实体、协议和接口也会带来新的安全威胁，如OpenFlow协议、应用控制接口、资源控制接口等[9]。

2.2.1 应用程序层安全风险

攻击者通过操纵应用程序来实施网络攻击策略，对控制层造成严重影响。应用程序层安全风险见表1。

表1 应用程序层安全风险

Tab. 1 Application layer security risks

安全风险	描述
欺骗	攻击者通过伪装成SDN控制器来获取用户的数据或服务逻辑，并将其用于后续攻击
抵赖	用户可能会否认他实施过的恶意网络策略，例如复制特定流量并将其转发到恶意服务器
信息泄露	攻击者可伪装成合法用户，通过SDN应用程序向网络注入伪造的流量
应用程序漏洞	SDN应用程序漏洞（如代码缺陷和不安全代码）可被攻击者利用以访问资源[10]

2.2.2 控制层安全风险

SDN控制器是整个网络的核心，它必须达到最高的安全级别。一旦SDN控制器失效，将导致整个网络瘫痪[11]。控制层安全风险包括如下几项。

（1）流规则冲突：恶意流可以绕过安全检测，这与预配置的安全策略冲突，并对SDN控制器产生不利影响。

（2）虚假流规则插入：攻击者可通过劫持SDN应用程序发送一些伪造的转发规则。

（3）欺骗：攻击者可伪装成管理员或SDN应用程序，从SDN控制器中删除或修改敏感数据，或取得网络拓扑信息和路由信息，更有甚者能完全控制SDN控制器。

（4）DoS攻击：攻击者可以创建虚假信息流，对SDN控制器进行DoS攻击，使系统瘫痪。DoS攻击是对SDN的严重威胁。在SDN中，针对控制层的DoS攻击主要有2种方式：一种是使用多个流条目M-DoS进行DoS攻击，耗尽交换机的三态内容寻址存储器（TCAM）资源；另一种是DoS攻击使用一个精心设计的入口S-DoS来覆盖目标链路并进一步影响控制器[12]。

（5）操作系统漏洞：SDN控制器运行在某种形式的操作系统（OS）上，那么操作系统的漏洞就变成了SDN控制器的漏洞。攻击者利用操作系统的漏洞，如默认密码、后台账户，引导OpenFlow控制器服务或上层应用错误的访问，从而导致劫持、拒绝服务或者中间人攻击等恶意行为，严重影响SDN控制器正常工作[13]。

2.2.3 数据转发层安全风险

数据转发层主要包括路由器和交换机等转发设备。极易发生针对流表、流规则以及交换机的恶意攻击[14]。数据转发层安全风险包括如下几项。

（1）欺骗：攻击者可以伪装成管理员或SDN控制器，从SDN交换机中删除或修改敏感数据或获取敏感信息，如流表中的流条目[15]。

（2）窃听：攻击者可以窃听SDN交换机之间的流，以获取有关流、流量和设备的信息。比如链路层发现协议（LLDP）在SDN中被广泛应用于网络层拓扑发现，但它不能保证消息的完整性。攻击者可利用此漏洞制造LLDP数据包，以声明将2个远程交换机连接到控制器的虚假链接。这样控制器就会被误导到错误的链路上，从而导致进一步遭受DoS攻击、窃听甚至劫持攻击[16]。

（3）流量表溢出：潜在流量表导致流量表溢出。在实践中，基于流表特征引入一种双向流量概念，同时提出通过自适应改变监控流表粒度以定位潜在受害者的检测方案[17]。

3 智慧物联体系安全架构

遵循电力物联网总体防护要求，按照“可信互联、精准防护、安全互动、智能防御”的防护策略，建立覆盖物联管理平台、网络通信、边缘物联代理和采集终端等的整体防护架构，符合安全防护要求，智慧物联体系安全架构如图3所示。图中PKI（Public Key Infrastructure）即公开密钥基础设施，是证书制作和分发的一种机制，能给安全的网路通信提供保障[18]。

边缘物联代理模块在架构中向下主要实现终端的安全认证、安全监测、策略下发等，向上通过电力物联网安全接入网关接入物联管理平台，利用安全芯片、操作系统加固、可信计算等措施强化本体

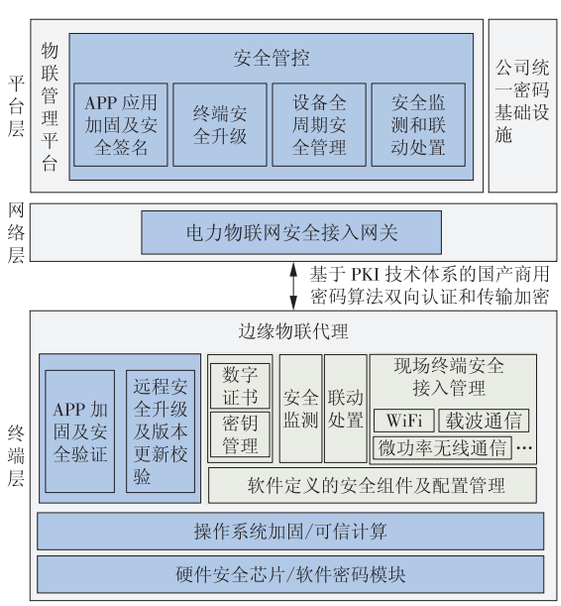

图3 智慧物联体系安全架构

Fig. 3 Security architecture of intelligent IoT system

安全防护及数据在本地存储及传输的安全性，主要包括APP加固及安全验证、终端远程升级安全、数字证书和密钥管理、安全接入等模块。

物联管理平台作为安全防护的关键，承担各类安全策略制定和下发、安全防护管理等核心功能，能够对物联网感知层的设备和应用等进行全面管控，主要具备以下安全能力。

（1）建立设备全周期安全管理模块，对接入边缘物联代理、采集终端等的设备进行全生命周期安全管理，重点实现设备初始化、注册、上线、离线和销毁等阶段的安全管理和异常状态监测。

（2）建立APP应用加固和安全签名模块，对研发厂商发布的终端APP应用进行安全认证，防止非法APP应用发布到物联管理平台。

（3）物联管理平台应能与边缘物联代理进行协同联动，实现安全策略的下发与更新，通过边缘物联代理实现安全措施落地。

（4）物联管理平台应通过数据加密、权限控制等措施做好存储数据的安全防护，并应加强数据业务应用之间的传输安全防护。同时采用可信计算技术，重点强化物联管理平台各类接口安全。

建立全面可靠的物联安全防护体系能够有效支撑边缘物联代理系统的高效运作，保障系统的安全可靠运行，对整个系统可能存在的潜在威胁和攻击采取防御措施。

4　基于SDN的边缘物联代理防御技术

（1）建立攻击表示模型进行攻击检测及有效防御。面对针对SDN的攻击和策略，一种威胁向量分层攻击表示模型TV-harm可捕获不同的威胁及其组合，从而对基于SDN的边缘物联代理网络进行安全风险评估。因为SDN控制器在SDN应用程序和通信协议中存在漏洞，攻击者可以执行窃听或权限提升攻击[18]。这类建立模型的方式为评估基于SDN架构的边缘物联代理受到的安全风险提供了一种较为直观、系统的方法。

（2）基于SDN控制器调度的防御DDoS攻击方法。为了帮助SDN架构中控制器抵御DDoS攻击，文献[19]提出了一种控制器调度方法，利用被攻击交换机的标准化等待时间、等待时长和位置范围来选择需要控制器处理的请求。

（3）基于移动目标进行防御。在SDN控制器的帮助下，边缘物联代理在可编程和可控方面有大幅提高。因此，许多安全行动已利用这种能力，以最佳方式部署在使用SDN功能的复杂网络中。文献[20]开发出一种基于层次化的攻击图模型的内存技术设备（MTD）技术，该技术根据主机的主次对主机的网络配置（如媒体访问控制（MAC）/互联网协议（IP）/端口地址）进行乱序排列[21]。基于移动目标防御，生成相应网络动态防御策略计划，可有效评估动态防御策略并选取最优防御策略。

（4）基于联合熵的安全防御方案。为了增强SDN的安全性，抵御边缘物联代理遭受DDoS攻击，文献[22]介绍了一个统计解决方案来检测和缓解安全风险。该文通过生成一个基于联合熵的统计模型，有效抵御已知的部分攻击，且对新兴的攻击类型也能有效防御。

（5）基于机器学习进行防御。文献[23]提出了一种基于SDN的、在云环境下解决DDoS攻击的有效方案。通过一种基于支持向量机和自组织映射算法的混合机器学习模型，生成一种改进的IP过滤方案，提高了攻击检测的速度和效率，以便迅速进行防御。为了解决SDN中监控模块负担重、检测准确率较低的问题，文献[24]提出一种多级分阶段混合检测方法，将机器学习算法结合其他数据预处理算法，耦合成一种有效的分类模型来检测系统的入侵流量。

5　结束语

边缘物联代理作为智慧物联系统中的重要模块，由于需要服务于数据量大的物联网终端设备，具有极其复杂的接入环境，容易受到网络攻击。因此，对安全访问和防御保护的需求很大，这就需要有效的安全风险评估和防御技术支持，以防受到恶意攻击，影响业务安全。

本文介绍了基于SDN的边缘物联代理架构，并论述了基于SDN的边缘物联代理安全风险及防御技术，为边缘物联代理将来的推广和安全防护提供最新研究成果，有望最终实现物联网云平台、边缘代理设备及智慧采集终端和监测终端之间信息交互的机密性、稳定性和可信性。

参考文献：

[1]RAFIQUE W，QI L Y，YAQOOB I，et al.Complementing IoT services through software defined networking and edge computing：A comprehensive survey [J]. IEEE Communications Surveys & Tutorials，2020，22（3）：1761-1804.

[2]MEI L，TONG H J，LIU T，et al. PSA：An architecture for proactively securing protocol-oblivious SDN networks [C]// IEEE International Conference on Electronics Information

and Emergency Communication, Beijing, 2019: 1-6.
[3]雷家星,胡洋.基于OpenFlow的SDN安全漏洞与防御的研究[J].内江科技,2020,41(8):30,33-34.
[4]YANG L X, HUANG K F, YANG X F, et al. Defense against advanced persistent threat through data backup and recovery [J]. IEEE Transactions on Network Science and Engineering, 2020. DOI: 10.1109/TNSE.2020.3040247.
[5]刘俊杰.SDN网络安全的研究与实现[D].南京:南京邮电大学,2019.
[6]SUN X, ANSARI N. EdgeIoT: Mobile edge computing for the Internet of Things [J]. IEEE Communications Magazine, 2016, 54, (12): 22-29.
[7]储轶钢.基于边缘智能的雾化物联网建设策略研究[J].电信技术,2018(12):8-11.
[8]黄颖祺,张宏斌,卢赓,等.软件定义网络的安全问题及对策研究[J].信息安全研究,2020,6(3):202-211.
HUANG Yingqi, ZHANG Hongbin, LU Geng, et al. Security problem and countermeasure research of SDN [J]. Journal of Information Security Research, 2020, 6(3): 202-211.
[9]石悦,李相龙,戴方芳.一种基于属性基加密的增强型软件定义网络安全框架[J].信息网络安全,2018(1):15-22.
SHI Yue, LI Xianglong, DAI Fangfang. An enhanced security framework of software defined network based on attribute-based encryption [J]. Netinfo Security, 2018(1): 15-22.
[10]朱梦迪.软件定义网络中控制信息一致性检测技术研究[D].合肥:安徽大学,2020.
[11]陈超,王帅,李智,等.SDN网络管理关键技术应用分析与改进思路[J].现代计算机,2020(24):34-41.
CHEN Chao, WANG Shuai, LI Zhi, et al. Application analysis and improvement of key technology of SDN network management [J]. Modern Computer, 2020 (24): 34-41.
[12]YUE M, WANG H Y, LIU L, et al. Detecting DoS attacks based on multi-features in SDN [J]. IEEE Access, 2020, 8: 104688-104700.
[13]王丽娜,王斐,刘维杰.面向SDN的安全威胁及其对抗技术研究[J].武汉大学学报(理学版),2019,65(2):153-164.
WANG Lina, WANG Fei, LIU Weijie. Researches on security threats and countermeasures of SDN [J]. Journal of Wuhan University (Natural Science Edition), 2019, 65(2): 153-164.
[14]DARGAHI T, CAPONI A, AMBROSIN M, et al. A survey on the security of stateful SDN data planes [J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1701-1725.
[15]邵喆丹.软件定义网络安全保障若干关键技术研究[D].南京:南京邮电大学,2019.
[16]HUA J Y, ZHOU Z D, ZHONG S. Flow misleading: Wormhole attack in software-defined networking via building in-band covert channel [J]. IEEE Transactions on Information Forensics and Security, 2020, 16: 1029-1043.
[17]陈超.SDN网络场景中的DDoS攻击检测方法与缓解机制的研究[D].南京:南京邮电大学,2018.
[18]谢宗晓,董坤祥,甄杰.公钥基础设施(PKI)的发展过程及其架构[J].中国质量与标准导报,2020(5):17-20.
XIE Zongxiao, DONG Kunxiang, ZHEN Jie. The development of public key infrastructure (PKI) and its architecture [J]. China Quality and Standards Review, 2020 (5): 17-20.
[19]EOM T, HONG J B, AN S, et al. A systematic approach to threat modeling and security analysis for software defined networking [J]. IEEE Access, 2019, 7: 137432-137445.
[20]LI S F, CUI Y H, NI Y F, et al. An effective SDN controller scheduling method to defence DDoS attacks [J]. Chinese Journal of Electronics, 2019, 28(2): 404-407.
[21]YOON S, CHO J H, KIM D S D, et al. Attack graph-based moving target defense in software-defined networks [J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1653-1668.
[22]刘江.网络动态防御策略及其有效性评估研究[D].郑州:解放军信息工程大学,2017.
[23]KALKAN K, ALTAY L, GÜR G, et al. JESS: Joint entropy-based DDoS defense scheme in SDN [J]. IEEE Journal on Selected Areas in Communications, 2018, 36(10): 2358-2372.
[24]尹胜.SDN网络中入侵行为识别与检测研究[D].西安:西安科技大学,2020.

(本文责编:张帆)

作者简介:

韩坚(1985—),男,江西萍乡人,高级工程师,从事电网运行可靠性方面的研究(E-mail:260031530@qq.com)。

刘松(1990—),男,江西萍乡人,工程师,工学硕士,从事电网运行可靠性方面的研究(E-mail:853495312@qq.com)。

魏吟斌*(1998—),女,江西南昌人,在读硕士研究生,从事能源互联网信息通信技术方面的研究(E-mail:wei_yinwu@163.com)。

李彬(1983—),男,北京人,副教授,工学博士,从事电气信息技术及电力系统通信方面的研究(E-mail:direfish@163.com)。

祁兵(1965—),男,辽宁铁岭人,教授,博士生导师,工学硕士,从事电力节能、自动需求响应方面的研究(E-mail:qbing@ncepu.edu.cn)。