浅析物联网安全防护技术

Analysis on IoT Security Technology

汪襄南[1]，王　冰[2]，霍纯敬[2]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联通北京分公司，北京 100061）
Wang Xiangnan[1], Wang Bing[2], Huo Chunjing[2]（1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. China Unicom Beijing Branch, Beijing 100061, China）

摘　要：
物联网已渗透到日常生活的方方面面，安全问题逐渐显现，安全防范的重要性不言而喻。首先简述了物联网发展的背景及运营商的物联网建设、部署和业务发展现状，结合近期物联网安全攻击事件及其影响，通过对物联网安全风险几个方面的研究，阐述分析了物联网安全现状及防范手段，最后对未来物联网安全防范技术进行展望和探讨。

关键词：
物联网；网络安全；分布式拒绝服务攻击；区块链
doi：10.12045/j.issn.1007-3043.2019.06.005
中图分类号：TN929.5
文献标识码：A
文章编号：1007-3043（2019）06-0019-05

Abstract：
IoT has been applied to all aspects of daily life, and security issues have gradually emerged. The importance of safety precautions is obvious. Firstly, the background of the development of IoT and the development status of operators' IoT construction, deployment and business are briefly described. Combined with recent IoT security attacks and their impacts, through the study of several aspects of IoT security risks, the security status and preventive measures of IoT are elaborated and analyzed. Finally, the future security prevention technology is prospected and discussed.

Keywords：
IoT; Network security; DDoS; Blockchain

引用格式：汪襄南，王冰，霍纯敬. 浅析物联网安全防护技术[J]. 邮电设计技术，2019(6)：19-23.

1 概述

物联网（IoT）已经成为一种日益复杂的生态系统，各类物联网终端日趋智能化和自动化。物联网相关业务的发展以及网络的演进速度已远远超前于安全防护能力。在此前提下，电信运营商如何在现有通信网络架构的模式下防范物联网安全风险，已经成为亟待研究和探讨的关键问题。

1.1 物联网背景及相关概念

物联网（IoT）引领着网络下一代的潮流，其发展必将对世界产生巨大的影响。据Gartner报告统计，到2025年全球物联网连接数将达到250亿，万物互联的蓝海即将到来，物联网的连接数量将呈现爆炸式增长。

互联网实现了全球点对点的信息传递，而正在以指数级进化的物联网设备，未来必将越过“奇点”，成为与人类一样的网络世界平等参与者。在通信领域，传统方式下的信息是通过点对点传输的，所以可通过追踪传输路径并拦截信息对网络的安全风险问题进行溯源。而在万物互联时代，电信运营商现有的通信网络架构难以承载亿级的物联网设备接入，而且物联网终端的多元性使用户对安全问题的感知度高低不

收稿日期：2019-04-10

一，所以必须探讨新的解决方案来保障基础网络设施及关键数据的安全。

根据国际电信联盟 ITU 的定义，物联网是指通过二维码识读设备、射频识别装置、红外感应器、全球定位系统和激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。物联网主要解决物与物、人与物、人与人之间的互连。从最初的机器通信（M2M——Machine to Machine）到物联网（IoT）再到万物互联（IoE——Internet of Everything），物联网超越了人口的限制，开拓了全新的市场蓝海，国际运营商已纷纷将物联网作为其新的业务增长点。

1.2 运营商物联网建设现状

目前运营商的物联网业务以发卡模式为主，尚未形成端到端的运营模式，应用服务层主要由服务提供商提供，终端感知层由用户自行管理。运营商主要负责网络能力层和连接管理层的建设与维护。在网络能力层建设物联网专用核心网，疏导物联网流量。在连接管理层建设物联网专用平台，提供 API 接口供企业用户调用，向用户提供批量发卡和集中管理卡的业务。物联网网络层级示意图如图 1 所示。

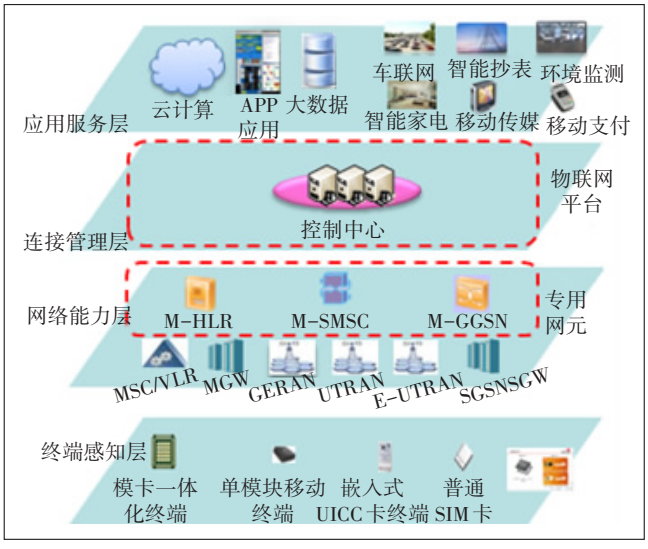

图 1　物联网网络层级示意图

2 物联网安全现状及案例

截至 2017 年，我国物联网连接数突破 1 亿，占全球总量 31%。我国运营商“云—管—端”的物联网体系已初步形成，业务呈现碎片化趋势。

2015 年起，越来越多的物联网智能设备出现在互联网上，大量涌现的物联网智能设备开始在分布式反射拒绝攻击（DRDoS 攻击）中扮演重要角色。由于物联网智能设备主要通过 SSDP 协议进行交互，物联网设备又具有高带宽、低监控水平、全天候在线等特点，因此其反射攻击具有比其他类攻击更为广泛的设备基础。

Gartner 的研究报告称在互联网终端中，27% 的控制系统已被攻破或被感染，80% 的设备采用简单密码，70% 的设备通信过程不加密，90% 的固件升级更新过程不进行签名验证，较易沦为攻击者发动 DRDoS 攻击的傀儡机。所以笔者认为物联网安全对物联网业务的重要性不言而喻。网络攻防趋势如图 2 所示。

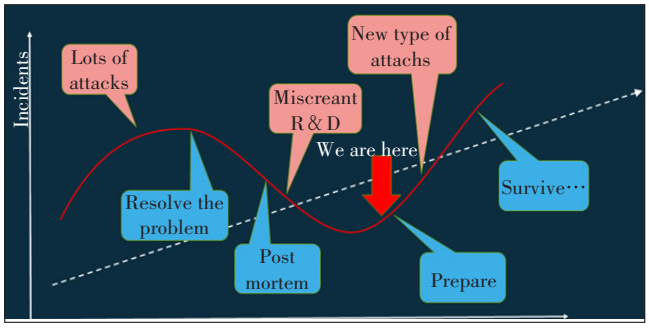

图 2　网络攻防趋势

与传统互联网网络安全防范相比，物联网的安全防范工作更加艰难。首先，物联网终端的智能化水平存在差异，而且终端资源（计算能力、存储空间）受限；其次，目前物联网缺乏通用的安全通信及安全检测协议；最后，与传统电脑终端、服务器相比，物联网设备自身安全防护能力较差。物联网终端更易受病毒、木马、蠕虫和恶意软件的攻击，导致设备无法使用、关键信息泄露、成为傀儡机甚至危及整个网络系统的安全，

下面介绍下过去发生的影响较为广泛的物联网安全案例。

2.1 Mirai 病毒

物联网僵尸网络病毒“Mirai”是新型的物联网病毒，可以发动大规模的分布式 DDOS 攻击。该病毒通过高效扫描物联网系统设备，感染采用出厂密码或者弱密码加密的物联网设备。

防火墙不能有效防范该病毒的入侵和传播，IoT 设备在不知不觉中被感染，成为僵尸网络中的一份子。攻击者就可以利用被感染的设备扩大传播范围，发起

大规模的外网攻击，同时监控内网，组织有规模的内网攻击。

2.2 IoT Reaper木马

IoT Reaper木马（也被称为IoT roop）是在2017年10月发现的一种新型物联网木马，其原型是Mirai，但比Mirai强大，它是利用漏洞实现跨平台的物联网设备访问，IoT Reaper攻击模型如图3所示。

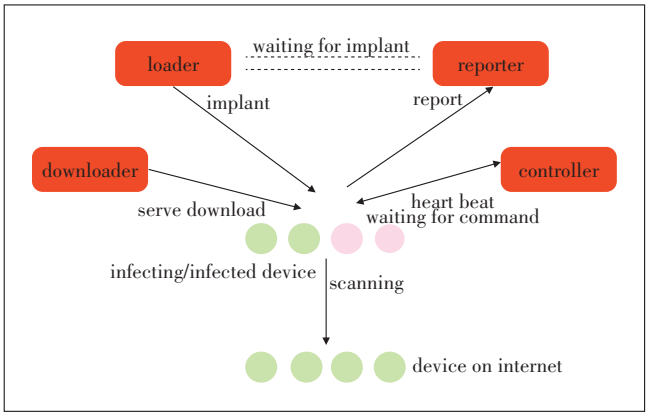

图3　IoT Reaper攻击模型

IoT Reaper放弃了Mirai中利用弱口令猜测的方式，转为利用IoT设备的漏洞进行植入。目前全球范围约有200万台物联网设备被感染，可以发动比Mirai规模更大的DDoS攻击，据监测，该类攻击的源IP地址分布中中国排名第1。

2.3 Memcached DDoS反射攻击

Memcached是一个高性能的开源分布式内存对象缓存系统，主要用于提高Web应用的扩展性，能够有效解决大数据缓存的问题，因为其结构简洁、部署简单，目前被广泛的应用于“云结构”和基础设施即服务（IaaS）网络中。

Memcached基于内存的key-value存储小块数据，并使用该数据完成数据库调用、API调用或页面渲染等，攻击者正是利用key-value这项功能构造了大流量的Memcached反射攻击。Memcached简单高效，但其在初始设计上没有过多考虑安全性及健壮性，留下了很多安全隐患，例如在默认状态下，它不做鉴权认证，而且TCP 11211及UDP 11211端口全部开放。

2018年2月，全球爆发了Memcached DDoS攻击，峰值流量高达1.7 Tbit/s，溯源结果表明，在这次攻击中分布在中国的被利用的Memcached服务器位列第2位，占比12.7%，中国位于北京的服务器排名第2，所以对此类攻击的防护也亟需重视。

3 近期物联网安全防范技术研究

从以上实际案例中可以看出，物联网安全问题的研究和安全部署时不我待。笔者认为电信基础运营商主要负责网络能力层和连接管理层的建设与维护，需要保证网络“管道”的可达性与安全性，其安全风险主要集中在3个方面：物联网终端安全问题、网络安全风险问题、物联网运营平台安全问题。

3.1 终端安全问题

物联网终端普遍成本低，智能程度低，但终端安全风险会威胁到整个物联网或者网络层的可用性，所以必须对此做一定防范。首先对设备进行强口令设置，并且建议安装防病毒软件，定期升级；其次建议在物联网中搭建恶意代码监测系统，通过采集Gn口流量，进行DPI深入包分析，通过抓包识别恶意代码特征并进行告警和拦截。例如针对Memcached DDoS反射攻击，通过执行以下代码，分析其主要特征。

```
from scapy.all import *
import binascii
payload=binascii. unhexlify ('000100000001000073
746174730d0a')
pkt=Ether ()/IP (src= "10.1.138.170", dst= "172.
17.10.103")/UDP(sport=666,dport=11211)/payload
sendp(pkt,iface="eth1",loop=0,verbose=False)
```

对Memcached DDoS的抓包分析如图4所示。

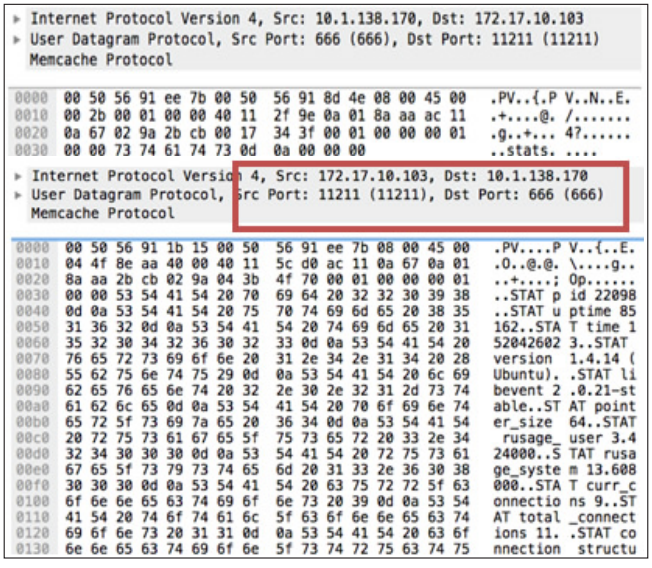

图4　Memcached DDoS抓包截图

3.2 网络安全风险问题

目前常见的物联网攻击与传统互联网攻击形式

相似，为保障网络性能，首先防范的仍然是巨型流量攻击造成的网络阻断与网络可用性降低。

以2018年发生的DDOS攻击规模来看，攻击峰值流量已达到Tbit/s级别，物联网海量设备接入后，其攻击流量规模呈几何级别增长，已经对网络基础运营造成了不可忽视的影响。

对于大流量反射攻击，需要进一步分析其包特征，网络边缘将异常流量数据包直接丢弃，并进行异常流量清洗等安全防护，物联网的安全部署如图5所示。

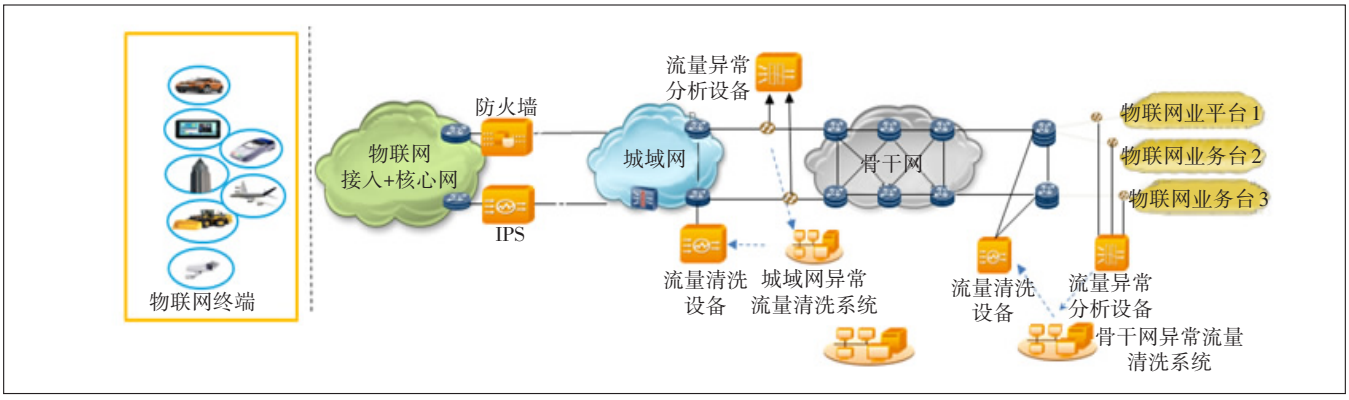

图5　近期物联网安全部署示意图

黑客只需要执行以下一段简短的代码执行程序就可以让设备发出巨大流量：

```
from scapy.all import *
import binascii
# cmd = "get a a a a a a a a a a a a a a a a… <729 times>"
payload=binascii. unhexlify ('000100000001000067
65742061206120612061206120612061206120612…')
pkt=Ether ()/IP (src= "10.1.138.170", dst= "172.
17.10.103")/UDP(sport=80,dport=11211)/payload
sendp(pkt,iface="eth1",loop=0,verbose=False)
```

可以通过抓包进一步分析反射DDoS攻击特征（见图6）。

3 0.002366	10.1.138.170	172.17.10.103	QUIC	1513 Payload (Encrypted), Seq: 1
4 0.075723	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
6 0.088618	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
7 0.088652	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
8 0.088658	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
9 0.088662	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
10 0.088678	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
11 0.088683	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
12 0.088692	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
13 0.088698	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
14 0.088704	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
15 0.088710	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
16 0.088715	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
17 0.088720	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1
18 0.088724	172.17.10.103	10.1.138.170	QUIC	1442 Payload (Encrypted), Seq: 1

图6　反射DDOS攻击特征抓取分析截图

从以上数据中可以看出，攻击者只需发送1个数据包，但反射器可发送50万个数据包，单一IP地址可产生高达6G的攻击流量。

面对如此巨大流量的攻击，运营商首先要在骨干网层面做好相应的安全预案模板，可通过设置白名单等手段做到快速响应和一键阻断。同时，各自治域需要对其对接的PEER进行安全流量控制，防范来自僵尸网络大量终端所带来的巨型流量风险。在核心网层面，可以在Gi出口位置部署防火墙、IPS等安全设备，定期进行核心网设备的漏洞扫描与弱口令验证，加强其健壮性并通过现有已部署的flow设备监控异常流量，完成近源清洗。具体的步骤应有：

a）首先分析判断受攻击的IP地址是否为物联网设备地址。

b）追踪新物联网僵尸网络感染设备的范围。

c）关联检测物联网地址的外发流量新指征以进

行进一步流量抑制。

4 物联网安全防范技术展望

网络安全领域的问题，目前已得到世界各国的重视，其重要性甚至可以上升到国家安全层面。未来的网络将是人与机器共舞的全新世界，需要一种不同于传统人为控制的、完全透明和公平执行的秩序。

中期来讲，物联网的安全运营业务将由传统的硬件交付转变为服务交付。虽然安全防护类设备不可或缺，但专业的安全服务、安全评估、安全培训以及安全运营服务（MSS）也将成为未来安全市场发展的重点。Gartner将MSS定义为：通过安全运营中心（SOC）的共享服务，实施IT安全功能的远程监控和管理。其服务可以包括防火墙服务、IPS/IDS、防DDoS攻击、基础设施日志收集与报告分析、故障与安全事件响应。

运营商首先要考虑建立可运营的SOC，提供安全运营服务，将物联网纳入管理和监控，从而建立信息广泛、统一预警的安全威胁情报中心。同时通过丰富的采集及监控手段，获取大量数据，增强风险预报的精度与效率，并且跟随网络演进的步伐同步升级监控及防护系统。

长期来看，物联网的智能设备将会呈现指数级增长态势，随之也会带来一系列问题。首先是成本问题，传统物联网需要部署中心化的云平台，这需要高昂的建设维护成本；其次是扩展性问题，海量的设备接入给网络带来扩容压力，而中心化的平台存在性能瓶颈；同时，大规模物联网终端接入将带来巨大的信息安全风险，而安全、隐私和信任是物联网发展的前提。

显然，只有去中心化、区域自治、扁平化的网络结构才能满足未来物联网业务发展的需求。

“区块链”技术是一种天然的去中心化的协议，它将分布式数据库作为载体，任意节点间的权利义务均等，没有权威服务器，系统中的所有数据块由整个系统中具有维护功能的节点来共同维护，每个节点分享权力和义务，通过广泛分布的节点进行验证，确保信息不可伪造和进行篡改。

成功的去中心化物联网不仅是点对点的，而且是无需信任的，也不存在中心化的单点故障。各物联网设备间可建立一种高度加密的轻量级通信机制。也许在不远的将来，这种无需信任的点对点通信协议，将演进成比TCP/IP协议更适合于物联网的传输层协议。

虽然区块链技术在物联网安全方面的应用市场前景广阔，但目前它在基础网络的应用还处在萌芽期，要达到规模商用还需克服重重挑战。首先，物联网终端需要具备加密和验证区块链交易的计算能力；其次，随着区块链的增长，节点存储空间的需求也越来越大；而且生成一个区块需要系统内多个节点参与记录并验证通过，会增加时延。

5 结束语

物联网安全模式需要IoT生态系统的每一部分进行合作、协调和连接。终端、网络、平台必须一起发力，相互整合。为了实现这种最佳的物联网安全模式，IoT生态系统的各组成部分均要考虑其安全性，从而建立稳固的底部和顶层结构。

海量接入的设备必将给网络带来更多的安全威胁，运营商需要主动出击，迎接物联网带来的机遇和挑战。

参考文献：

[1] Gartner：2017年物联网10大趋势分析研究报告[EB/OL].[2018-12-29]. https://www.sohu.com/a/127276007_526275.
[2] 信息安全技术信息系统安全等级保护基本要求第4部分物联网安全扩展[EB/OL].[2018-12-29]. https://max.book118.com/html/2018/0126/150703180.shtm
[3] IBM物联网白皮书[EB/OL].[2018-12-29]. https://www.8btc.com/article/32272.
[4] 于敏辉，刘波. 区块链与物联网解决方案分析[J]. 集成电路应用，2017(12)：87-88.
[5] 宋国栋. 基于区块链构建去中心化、自治、安全的物联网[J]. 中兴通讯技术(简讯)，2016(12).
[6] 杨光，耿贵宁，都婧，等. 物联网安全威胁与措施[J]. 清华大学学报(自然科学版)，2011(10)：1335-1340.
[7] 武传坤. 物联网安全关键技术与挑战[J]. 密码学报，2015，2(1)：40-53.
[8] 孙建华，陈昌祥. 物联网安全初探[J]. 通信技术，2012，45(7)：100-102.
[9] 赵阔，邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息网络安全，2017(5)：1-6.
[10] 姜威，姜泽睿. 以区块链技术为核心的物联网安全解决对策研究[J]. 通信技术，2018，51(6)：159-162.

作者简介：
汪襄南，高级工程师，学士，主要从事网络安全方面工作；王冰，高级工程师，硕士，主要从事网络分析、网络建设方面工作；霍纯敬，工程师，学士，主要从事网络运营维护方面工作。