2020【2】8　2卷8期 ISSN: 2661-3530(Print); 2661-3549(Online)

Universe Scientific Publishing

# 试论移动互联网时代信息安全新技术的展望

魏恒达

北华大学 吉林 吉林 132021

【摘要】移动互联网是人们生活中的必需品，其存在为人们带来巨大的便利，社会科学技术不断发展，随之而来的就是网络信息安全问题。移动互联网的信息安全问题能够给人们的财产和信息带来损失，进而也不利于互联网的发展。因此相关的学者要结合现有的网络信息安全防御措施，设计能够应对新型病毒入侵的防御，为人们提供更加安全的互联网服务。

【关键词】移动互联网；网络信息安全；网络安全技术；黑客

## 1 前言

移动互联网是现时代工作和生活的必需品，在人类的世界中得到广泛的使用。移动互联网在被使用过程中，往往会出现一切的安全问题，如木马和病毒的攻击，让人们正常使用网络的过程中存在安全隐患，对其财产和设备使用都会带来影响，进而降低人们使用移动互联网的积极性。故相关学者和专家要将此项问题作为目前最急需解决的课题，通过采用先进技术，提高移动互联网的使用安全性，确保人们能够正常使用，进而为人们的生活提供更加安全的便利条件。

## 2 移动互联网信息安全威胁分析

移动互联网信息面临的安全风险种类非常多，如勒索病毒、特洛伊木马等，这些病毒能够将自己藏身于各种数据文件中，伺机对移动互联网服务器进行破坏，导致移动终端的网络发生终端甚至崩溃，进而对用户产生严重损失。2018 年在微软、谷歌、中国移动、中联控股等世界名企中爆发一场勒索病毒，导致这些企业的移动网络瘫痪，造成大量用户无法开机进入系统，使得使用者不得不向勒索方缴纳赎金。移动互联网病毒或者木马能够向网络发起 DDoS 攻击，能够在短时间内形成无数的访问请求，占用宽带资源，给用户带来无法上网的影响，进一步影响移动互联网的正常访问，给政府部门和个人带来严重的损失。DDoS 攻击主要是带宽攻击和连通性攻击，其中带宽攻击能够在瞬间产生大量的非法数据包，占宽带资源，使得用户无法正常访问服务器，降低移动互联网运行效率。

信息技术不断更新和改进，木马病毒技术也随之优化，各种各样的新型技术被不法分子利用，将病毒和木马的潜伏期变得更长，可攻击设备越来越多，故目前来看，我国移动互联网信息安全防御方面面临着更加严峻的挑战。今年 3 月份，360 公司在季度总结报告中指出，我国移动设备的使用越来越广泛，导致各种各样的木马病毒也得到不同程度的发展，新型木马病毒将会流入移动互联网，如 PassCopy 和暗黑蜘蛛侠等典型的木马病毒，这些病毒侵入主要以盗取和篡改用户敏感信息，对大量信息数据进行更改。由此看来，移动互联网信息安全技术要及时更新，除了现有的防火墙技术、访问控制技术等，还需要引进新型的信息安全防御技术，如深度包过滤、人工智能算法、入侵检测技术等，对移动互联网中的访问信息进行收集，并对其分析检测是否含有入侵行为，尽早发现及时处理，防止入侵者破坏网络服务。

## 3 移动互联网信息安全的全新技术

### 3.1 密码技术

3.1.1 后量子密码技术

传统的密码技术没有利用到物理学知识，而新型的量子密码技术将密码学和物理学知识相结合，是一项全新的技术和学科，逐渐成为未来信息技术发展的方向。量子密码技术在目前技术中，无法进行破解，其基本原理就是利用光子之间的量子理论状态，单个量子可以独自计算，这样就算有病毒入侵，也能将其阻隔在外，防止移动互联网信息出现泄漏的问题，进而保障移动互联网的信息安全，为人们正常使用移动互联网提供有力保障。目前的量子密码技术不需要迁移，随着各项网络技术的发展，量子密码技术能够与企业网络相互兼容。虽然目前的量子密码技术不够成熟，但是就其作用和功能来看，在未来有很大的发展空间。

3.1.2 同态密码技术

移动互联网技术更新较快，随之而来的就是网络

信息安全的问题。密码锁是应对网络信息安全的重要保护方式之一。同态密码技术就是其中的一项技术，有足够的优势被应用在移动互联网信息安全防御中。云计算的运用范围比较广泛，是当今社会中的热点技术，其采用的密码技术就是通过对数据进行加密而实现的保护作用，确保用户信息不会受到盗取，免于外界的影响。同态密码技术与其他密码技术相比，有其独特的优势，能够被越来越多的人使用。同态密码技术能够通过自身实现对数据信息的加密，并对信息数据进行明文运算，之所以能够将其运用在不同领域的信息安全防御中，就是因为其防御功能强大。但是同态密码技术在运行时，不可避免会出现一些问题和漏洞。因此在日后的研究中，要加强对其优化和修复，力争做到完善防护，网络信息安全提供一定的作用。

### 3.2 深度包过滤技术

深度包过滤技术能够将软件和硬件互相结合的网络信息安全防御技术，能够深入分析移动互联网中每个数据包的内容，如包头、其他信息数据协议字段中包含的数据，多每一项数据包的内容进行分析，是需要通过软件和硬件共同完成的，能够有效提高入侵检测的效率和准确度。深度包过滤能够结合访问者对入侵过滤规则进行设置，通过启发式防御软件，对 IP 地址和 MAC 地址进行检测和判断，确定其是否符合设定额的规则，如果符合规则，就可以通过，如果不符合，就无法通过。深度包过滤还能够对数据包内的信息和数据进行分析，检查数据包内的每个数据是否含有不安全的字符和字段。经过多年的实践和运用，能够结合受保护对象和部署的位置自主进行不同的深度包过滤工具，如移动互联网 Web 服务器和网关服务器等，能够确保网络不受到破坏，并且这种技术的部署代价较低，在一定程度上能提高互联网的安全。在实际运用中，深度包过滤技术的运用能够使内部网络暴露在外部网络中，影响实际防御，因此在未来的技术中，要加强对这方面的研究和优化。

### 3.3 入侵检测技术

现阶段，移动互联网技术面临的信息安全威胁还是很多，这些危险因素能够通过网络入侵到服务器，并且连接服务器的设备也比较多，除了 PC 设备、笔记本终端，还有手机、平板和路由器等，这样就会造成入侵来源繁多，给入侵检测工作带来一定的难度。故为了满足实际需求，应该研究出更加高效、快速、准确的入侵检测技术，结合先进的网络信息技术和人工智能技术，通过新型算法实现入侵检测全覆盖，提高入侵检测的效率。入侵检测技术能够通过人工智能技术创建一个对网络信息异常、状态异常、特征异常检测的模型，弥补传统入侵检测的不足和缺陷，能够识别大规模的组合式和分布式入侵方式，还能够对移动互联网不同区域进行针对性检测，实现对骨干网、通信网和核心网的检测，不仅能大幅减少检测过程中对资源的占有率，还能使检测的范围更加广阔。

## 4 结语及展望

在未来对移动网络信息安全防御技术进行研究时，要结合以往的经验，在传统的防御技术基础上，采用新型技术对其扩展和优化，为人们提供安全性较高的网络服务。此外在未来的信息安全防御研究中，要完善相应的法律法规，提高每个人的网络信息安全意识，在网络中要加强信息认证管理工作，将高风险的数据消除掉，确保存在网络中的数据都是安全的。在移动终端设计中，要提升设备安全管理，注重应用程序的研发，要设计必要的安全防护软件，进而为人们正常使用提供有力保障。

## 【参考文献】

[1] 邓青殷，黄兆敏，洪真忠 . 移动互联网信息安全技术体系浅析 [J]. 无线互联科技 ,2014,000(006):3.
[2] 李子臣 . 移动互联网时代信息安全新技术展望 [J]. 信息通信技术 ,2012,000(006):75-80.
[3] 何桂荣 . 移动互联网信息安全威胁与漏洞分析 [J]. 电子技术与软件工程 ,2017,17(115):218.