无线网络通信协议中的安全问题及对策

汤慧

湖南省通信建设有限公司　湖南　长沙　410000

[摘　要]信息时代的到来使得无线网络通信技术在我国的广泛应用，大数据时代的逐步到来使得无线网络通信技术已经不可或缺，因此安全问题得到人们的重视。无线网络通信技术开放性、自由性、全球性的特点既是其优势，也给国家、社会、个人的安全带来了极大的隐患。因此，本文介绍新时期无线网络安全问题的出现类型并根据存在的问题提出相应的解决措施以保证网络用户始终体验安全有效率的网络服务。

[关键词]无线网络；通信协议；安全问题；对策

【DOI】10.12252/j.issn.2096-6288.2020.02.631

1 无线网络安全方法与技术概述

1.1无线网络安全技术分析

用户可以在无线网络应用过程中通过安全设置来有效提高无线网络安全性与稳定性，防范各种攻击的到来。加密处理无线网络数据可以有效降低无线网络运行风险，通过合理的加密方式可以有效拦截未被授权部分的数据攻击，防止因为攻击者的不断侵犯而导致出现数据丢失、数据损坏以及数据篡改等问题，当前应用更多的几种加密方式主要包括节点加密与链路加密。确保通信安全的重要措施就是安全认证，借助于实体认证或数据认证，能够避免伪装用户在网络当中进行非法访问，但是需要注意安全认证应用期间应当做好多种防范、双向认证的完善，从而防止安全认证过于单一。访问控制可以组织未被授权的用户对无线网络进行访问，并规范用户行为，使其只能够在权限以内进行活动。数据校验则能够有效确保无线网络数据的真实性与完整性，并利用保密协议避免出现数据被恶意截留的问题。

1.2无线网络安全必要性

近些年来，我国在不同区域部署的Wi-Fi无线网络数量逐渐增加，如表1所示。相较于传统网络，无线网络为用户提供了更高的自由度，进一步扩展了用户空间，更便利了人们的使用。在此期间，无线网络也带来了全新的安全性问题，严重限制无线网络的发展与完善。因为Internet本身就有着相对脆弱的安全机制，同时无线网络原本就具有一定的开放性与局限性，因此在无线网络运行期间，将会面对相较于传统网络更加复杂且严峻的安全威胁。无线网络借助于开放性的传输线路在针对高速数据进行传输过程中，往往会伴随着各种各样的安全问题，但是在传统网络当中所研究与掌握的防控策略，目前已经不再适用于无线网络的安全防护工作。由此可见，受无线网络开放性特点的影响，既为我们带来了较大便利，同时也是我们需要面对全新的挑战，所以研究无线网络安全方法与技术至关重要。

表1 无线网络部署区域及Wi-Fi热点数量

部署区域	Wi-Fi 热点数量
公共热点	650 万台
政府	20 万台
家庭	1 亿台
运营商 / 商业	9400 万台

2 无线应用协议的安全性

通常情况下，无线应用协议（简称WAP）一般是指无线数据、互联网和电话相结合的产物，其主要目标是定义一个联系紧密，但进行分层的可扩展网络模型。实际上，基于WAP构建的模型中各层具有相对比较集中的功能，这就使得各层均可以实现集中扩展和表述；同时各层与其相邻层又存在相辅相成、互相联系的关系，因此其整体的功能都能够发挥出来。WAP系统包括了WAP客户端、WAP应用服务器和WAP代理等实体部分，此外还包括了有线网络与无线网络间的连接。其中WAP代理即所谓的WAP网关，其一般是负责实现有线域和无线域的连接，同时也包括了用户代理结构管理、转化编译器功能、缓存代理和无线协议等。无线网络主要涵盖了WAP网关到基站的无线部分、基站到移动台的空中接口部分；有线网络通常是指互联网。

WAP系统对TCP/IP协议的分层思想进行了借鉴，并对各层中的安全通信的要求和每一层的功能、应用等给予综合考虑，并且随着技术的发展时期安全规范得到了有效拓展和增强。例如，已发布的WAP2.0技术涉及无线标记语言脚本密码、汇集（简称WMLSCrypto）、无线传输层安全（简称WTLS）、WAP身份模块（简称WJM）和WAP公钥基础设施（简称WPKI）等四个方面的安全规范。

3 无线通信网络安全态势识别技术分析

3.1网络安全事件的前期助理以及识别要素提取

针对网络安全态势进行感知的研究，往往医和防火墙以及入侵检测设备，而结合当前的无线通信网络运行状态来讲受到不同生产商以及不同生产标准的影响，这些设备在收集数据信息的过程中，格式往往不统一，因此在数据集中还存在着较多的无效数据，这会对最终的网络安全态势感知造成干扰，影响结果的有效性以及精准性。因此打造规定的格式和规则，统一的进行辅助设备以及系统的转化至关重要，在这个过程中涉及了数据预处理操作，也可以将其称为态势特征提取。通常来讲，大部分的网络数据都是以日志的形式呈现的，因此在数据预处理的过程中，要结合大量的数据日志提取具有功能性的特征数据，将其中的冗余信息抛弃。这其中网络安全态势感知模型的建立，往往需要依赖前期的特征提取，由于大规模的无线通信网络安全态势感知需求较高，需要综合大量的检测设备进行日志信息的处理，确保可以全面提升态势评估的精准性。

安全态势识别最主要的是要快速定位影响网络安全的要素，因此进行网络风险要素识别至关重要，而由于当前无线通信网络涉及的安全信息较多，为了确保其中的有用信息可以被精准提取，通常以数学方式进行数据预处理。

3.2感知要素的定位以及提取

在原始数据集处理的过程中，可以利用数学方法进行规定、融合、计算，然后才可以产生网络安全态势参数。本文建立在深度自编码网络前，向传播技术的基础上能够快速地提升识别的有效性，通过计算无线通信网络安全态势数值能够分析网络安全态势。

首先从技术角度来讲，深度自编码网络是建立在编码器、编码层、解码器这三个基础上打造的技术体系，这其中编码器主要提供信息的输入，而编码层以及解码器是提供信息的输出。在进行安全态势感知要素定位和提取的过程中，首先需要将网络通信数据从编码器的输入端口输入系统，自身附带的编程系统，会结合不同的网络输入信号进行训练，训练结束之后会在输出端口将安全态势感知要素输出。整体的技术体系属于一种镜面对称结构，能够将已知的编码信息整合到深度训练学习系统中。

但是由于常规的网络数据信息中含有大量的隐藏节点，这些隐藏节点以非线性映射的方式存在于输入端口系统中。这也就导致在网络数据输入的过程中，无法结合实际情况定位其具体的体量，一旦初始值过大，会导致最终的输出结果出现局部最优的情况，而初始值最小则会无法执行网络训练。为了解决这样的问题，可以直接通过受限玻尔兹曼机网络逐层训练机制，逐层的进行网络训练。该机制主要划分成可视层、编制单元以及隐藏层这三个结构，这其中可视层负责进行信息输入编制单元以及隐藏层，负责进行信息输出。

4 无线网络安全问题的解决措施

4.1信息安全认证技术

目前的信息安全认证技术主要是要求用户按照要求录入个人密码，或以邮件、手机验证码等方式来一对一的加密信息。该加密方式即所谓的完整性检测技术，如今在网络客户端信息防护中得到了广泛应用，具有操作简单、随机性强、安全性高、上手容易等优势，且密码不易被窃取或丢失。在信息发送过程中，即使不法分子窃取或截获该信息，也会由于该信息只能够被服务端和用户所知而得到应有的保护，不会被困扰到，能够最大程度上保护双方的隐私。

并且因为其是随时随地进行更换的，即使不法分子能够通过接口连接到用户的输入设备而操作用户的设备，但是也难以及时获取验证信息。虽然其具有一系列的优势，但是其还有一些弊端。例如，用户的验证信息被同时更新到其他设备中，不法分子提前或同时与用户进行操作，用户的操作就会无效。另外，用户的原有设备丢失，用户便难以证实自身的身份，会给用户带来更多的麻烦。

因此，无线网络通信技术服务商和相应的技术人员都要想办法解决信息安全技术的弊端，尽量保证其优势。

4.2身份认证技术

在互联网快速发展过程中，无线网络技术不仅可以为人们带来便利，而且还可以提高用户信息保护力度，多数的网络运营商会通过身份认证保护客户信息。现在广泛应用的有安保手机验证、安保信息认证、个人的问题验证等。身份认证技术主要是在相关法律法规的监管之下，通过对用户的信息和输入的信息进行验证来保护客户的信息，一旦出现差错，就会立即停止登录。进而能够避免用户的信息泄漏。

4.3VPN技术

所谓VPN技术，指的就是借助于公用网络构建起一个临时且十分安全的连接，这属于一条公用的网络隧道，具有安全且稳定穿越混乱网络环境的优势。利用VPN技术能够有效确保无线网络运行过程中的安全性。VPN技术借助于加密、用户认证、数据认证等，确保无线网络运行过程中的安全性。其中用户认证的主要目的就是确保用户在得到授权之后可以完成对无线网络当中数据的实时接收与发送；数据认证的主要目的就是保障数据传输过程中的完整性，同时能够确保数据的来源认证设备更加明确；加密的主要目的就是保障即便是数据被攻击者所拦截，也需要较长时间才能够完成解密。

4.4启用MAC

MAC指的就是介质访问具体的控制地址，属于无线网卡当中的地址，针对各个设备而言都属于唯一地址，这个地址既对计算机之间存在的网络连接有着一定的定义作用，还能够在网卡硬件电路当中将其记录。因为不同无线网卡所具备的物理地址是唯一的，所以可以借助于手动方式在AP当中设置一组访问权限更高的MAC地址列表，从而完成过滤物理地址的目的。通过这种方式，一般需要AP当中的MAC地址列表可以具备实时更新的功能，一旦没有较强的可扩展性，就会导致不同AP之间存在的漫游无法实现；MAC地址还可以有效防止黑客入侵无线网络，从而进一步确保网络安全，

4.5防止未授权服务的恶意捆绑

认可用户发送的对应用的使用申请之后，网页或客户端将会把相关内容面向有权限的客户开放，一般用户进行操作。但是，这种网页端或客户端认可与用户发送申请存在的时间差将会被不法分子所利用，并借助网络插件捆绑的方式来对网页内容进行更改，使得用户在点击网页信息时误点其他的信息，被恶意捆绑并使得用户个人信息流失，甚至有损用户与服务商双方的利益，进而获得非法收入。

除此之外，还有一些不法分子会通过不明的链接，并将链接伪装成邮件、游戏等其他正常的链接来迷惑用户，使得用户误以为错误链接为正确的链接并进入到非法的页面，造成用户的信息泄漏。

结论

网络的开放性和自由性极大地满足了大多数用户对网络服务提出的要求，然而在网络技术发展过程中，由于各方面因素的影响，导致无线网络通信技术出现一系列的问题，需要人们加以重视。针对无线网络的无限窃听技术、身份假冒攻击、服务交易后不予服务方应得的报酬等一系列问题，需要加强信息安全认证技术、身份认证技术、防止未授权服务的恶意捆绑等，同时用户自身也要提高自身的网络安全防范意识，并对无线网络通信技术给予合理、合规应用，避免由于自身操作不当而出现数据流失及信息泄漏现象。

参考文献

[1]盛仲飙.WIFI无线网络技术及安全性研究[J].电子设计工程.2012，（16）.1-3.

[2]贾海峰.无线网络通信协议中的安全问题及对策研究[J].中国管理信息化，2015（14）：184.

[3]邢劭谦，徐璐，原野.无线网络通信协议中的安全问题及对策探讨[J].中国新通信，2019，19（13）：29.