基于 NGN 的网络安全技术研究

刘 伟[1] 吴俊敏[2] 朱小东[2]
(中国科学技术大学苏州研究院软件学院 苏州 215123)[1]
(中国科学技术大学苏州研究院计算机学院 苏州 215123)[2]

摘 要 随着 IPv6 的部署和 5G 标准化的推进,下一代网络已成为业界关注的热点。通过分析下一代网络(Next Generation Network,NGN)的 4 层体系结构以及其关键技术,结合我国的网络特点,提出目前仍有必要更进一步进入下一代网络;同时给出了下一带网络发展过程中的实践部署经验,提出其需要突破的地方,并结合现有的技术给出下一代网络在安全方面存在的问题及其解决方案。

关键词 下一代网络,网络体系结构,网络安全
中图法分类号 TP301 **文献标识码** A

Research on Network Security Technologies Based on NGN

LIU Wei[1] WU Jun-min[2] ZHU Xiao-dong[2]
(School of Software Engineering,Suzhou Institution for Advanced Study of the University of Science and Technology of China,Suzhou 215123,China)[1]
(College of Computer and Technology,Suzhou Institution for Advanced Study of the University of Science and Technology of China,Suzhou 215123,China)[2]

Abstract With the deployment of IPv6 and the promotion of the 5G standardization,the next generation network has become the focus of attention of the industry. Through the analysis of next generation network (NGN) 4 layer system structure and its key technology,combined with the characteristics of our country network argues,there is still a need to go further into the next generation network. This paper gave the experience of the practice and deployment of the next generation network development,and put forward the place where it needs to break through. Combined with current technology,we gave the security problems of the next generation network and provided solutions.

Keywords Next generation network,Network architecture,Network security

随着国家提出“互联网+”战略以及 IPv6 的部署和 5G 标准化进程的逐步推进,下一代网络的发展将成为未来关注的焦点。现在国内很大部分消费以互联网为中心,其各项业务急剧增长,促进了以 IPv6 技术为基础的融合数据、图像、视频、实时监控等综合业务的 IP 网络向下一代网络(NGN)平滑演进。本文在研究 NGN 体系结构及其关键技术的基础上,针对现在网络发展以及下一代网络中可能存在的安全问题,提出一些解决问题的方案。

1 下一代网络研究

1.1 下一代网络概述

下一代网络是未来网络融合的一种趋势,它是基于 IP 技术实现语音、网络视频和流媒体的网络[1]。ITU-T 对下一代互联网的定义是:它是一个分组网,不仅可以提供电信业务,而且可以提供数字广播电视业务等多种业务,通过使用各种带宽形式和 QoS 服务能力的传输技术完成服务业务与数据传输的分离,并且它对用户所需的各种业务的接入是不受限的,实现了用户对业务使用的一致性和统一性。NGN 将传统交换机的功能模块分离为独立的网络部件,各个部件可以各自独立发展,协议接口遵守相应的标准[2]。NGN 具有 4 层架构,网络分层架构如图 1 所示。

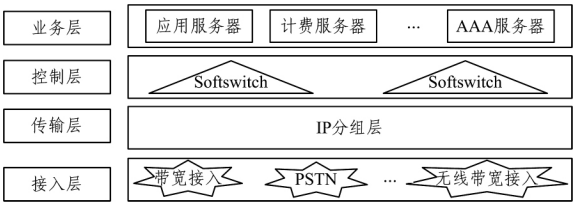

图 1 NGN 网络分层架构

图 1 中,接入层由各类接入网关、中继网关和智能终端等组成,其作用是实现数据格式转换和转发,并完成数据在 IP 分组网的传输。传输层帮助完成 IP 包转发的各类承载网功能,实现数据能在网络上正确送达,目前仍然是通过 MPLS IPv6 技术的下一代 IP 网和自动交换光传送网实现传输层的数据传送。根据现实情况,基于 IPv6 的网络目前不能全部进

刘 伟(1991-),男,硕士,主要研究方向为网络技术、深度学习,E-mail:liuwei_ustc@sina.com;吴俊敏(1973-),男,博士,副教授,主要研究方向为并行与分布式系统、深度学习、无线传感网络;朱小东(1980-),男,博士,讲师,主要研究方向为计算机系统性能分析、并行与分布式仿真系统等。

行部署，使用 MPLS 技术是下一代网络最好的承载技术。控制层是下一代网络的核心层，它能够完成各类控制呼叫功能以及业务信息的发送功能，另外它还控制着路由判断和转发数据的功能，并实现端-端的通信过程，此层包含有软交换设备、signal 网关等。业务层是一个开放的、综合的业务接入平台，由一系列应用服务器组成，提供各种增值服务，通过提供标准接口，可接入海量的服务而不必考虑其下层的兼容[3]。

1.2 下一代网络体系结构研究

1.2.1 应高度重视网络体系结构研究

网络体系结构（Network Architecture）[4]就是行业内所说的网络顶层设计，即网络系统的总体设计框架，包含从物理层到应用层的整个体系结构的描述协议和通信机制的设计原则两大部分。通俗地讲，网络体系结构是通过对网络各类应用的深刻理解而最终抽象出来的设计原则[5]。目前国内软件行业高速发展，但是在大型项目中往往忽略了体系结构设计，并且网络建设也难以逃脱这一弊病。为了解决这些问题，在建设网络的过程中更需要有前瞻性的结构设计原则。现在网络建设出现的很多问题都是由于没有注意体系结构设计而导致的，因此在研究 NGN 时一定要注重网络体系结构的研究。

1.2.2 基于 Internet 体系结构的下一代网络体系结构的借鉴

Internet 体系结构是 20 世纪 70 年代由 IETF 确定的，而对 Internet 起着监管作用的 ITB（Internet Architecture Board）机构指出，Internet 的设计原则 50 年来没有大的改变。这是由于在因特网发展初期主要针对的需求[6]是使得网络互相连通，保证网络的健壮性，实现网络设备异构性和分布式的管理，降低上网成本等。这样就确定了以无连接的分组交换结构为基础的因特网体系结构，高层的功能都集中于网络边缘末端[6]，采用路由机制和尽力服务（Best Effort）原则。

目前 Internet 已经进入高速发展的阶段，全世界已有超 32 亿人[7]上网，这也对下一代网络体系结构的发展提出了新的要求，例如移动性、语音、视频、网络安全等。新的应用需求迫使我们必须重新审视下一代网络的设计结构，甚者可能会进行根本的体系结构变革。实际上，下一代网络的体系结构不但要考虑技术的需要，而且还得考量很多非技术上的因素，包含企业的发展方式、经济投入等，这就促使我们不能一蹴而就地采用自顶向下的方式进行，而应该采用更加合理的方式，如迭代方式。复杂的网络需求导致我们在设计新的体系结构时并不能面面俱到，但是我们可以抽象出最基本的需求，根据这些需求定义整个下一代网络机制的最小部分，再定义满足不同需求的子体系结构，这样层层递进就可以实现最后的下一代网络体系结构方案。

1.2.3 光通信与分组交换技术的融合

20 世纪，MIT 教授 David Clark 提出了边缘论——“一种应用功能只有当其知识和帮助置于通信系统的边缘才能完全和正确地实现，因此将提出这种应用功能作为通信系统本身的性质是不可能的”[8]，随着网络技术的发展，后来他发表了一篇要重新思考 Internet 设计原则的重要论文[9]推翻了过去的观点。加之网络用户数量快速增加导致对音频、视频的需求量持续走高，这样就使得基于光通信和分组交换的融合技术成为一种趋势。

基于光技术的线路交换（Circuit Switch）和基于电子技术的分组交换（Packet Switch）是目前网络通信的基础，而且研究表明下一代网络的融合也是集中于光与电的融合[10]。现在线路交换的软肋仍是光电转换，若是在 THz 领域创造一种新的技术，则能够实现分组交换。目前的线路交换是由路由器完成的，但是它的带宽利用率很低，不超过 50%，而且路由器解决阻塞问题总喜欢进行丢包处理，同时路由器并不智能，它不能识别语音、图像和文字流，这就阻碍了下一代网络在网络广播电视领域的发展。

随着应用增强，人们在使用路由器时不仅仅要增大路由器的速度，还要提高它的智能效果。用全光技术实现交换和路由是很多人想要的，但是目前 OXC 仅仅比电分组交换快 2～3 倍，竞争力优势依然不足。今后如果光子交叉互联能够在更大粒度上实现交换、传输光波的延迟和存储技术进一步发展，那么下一代网络的融合将不再受带宽限制。

2 下一代网络演进实践

目前国内向下一代网络演进的实践很多，这里最为典型的是中国电信，其如今的网络试点和一系列试验都将为对未来下一代网络的发展提供宝贵的经验。研究表明[11]，通过对实际网络的正确部署以及对业务的升级运营，就能够发现并解决下一代网络在推行过程中遇到的问题，同时也必然会收获意想不到的经验。

事实上，自从 2013 以来，以中国电信北京研究院为主要技术支持和部署指导的江苏电信公司就通过与华为技术有限公司进行战略合作，在整个向下一代网络推进的实践过程中，对技术研究和设备部署过程中进行的预想布置和安排均进行了试验和验证，最终的结果表明，整个网络的部署工作达到了预期的效果。电信实践中的收获，对于未来下一代网络的发展有极大的推动作用。

（1）升级业务平台

研发人员通过升级 IDC 平台，实现承载网络的接入；对网络中的汇聚设备和出口设备也进行升级；同时对 ICP 核心服务器和应用系统也实现软件升级达到双协议栈的承载功能。对于其他运营商的业务平台，可以对运营服务器和承载网络进行升级，从而实现双协议栈功能。

（2）支撑体系

现在越来越多的宽带接入部分已经实现了 IPv6 化，这样也就存在双协议栈（IPv6/IPv4）用户、IPv4 用户、IPv6 用户等不同的用户类型。这种用户类型的产生也就要求电信对应的 IT 系统、网络管理系统、DNS 系统、认证系统、计费系统等进行相应的改造。对于 OSS 系统、DNS 系统、认证系统、计费系统等则是通过增加相应的字段属性或者升级软件系统来支持双协议栈，不仅如此，运营商的部分 Firewall 也进行升级以支持双协议栈。然而现实问题阻碍了进一步发展，这也是未来下一代网络需要克服的问题。

1）国家还没有完成 IPv6 安全监管和系统建设，而且 IPv6 的访问也仅仅是在国内，大部分用户访问还不能普及。

2）实行双协议栈虽然可以很快地引入 IPv6，但是对于解决 IPv4 的根本问题仍然是徒劳的，因此必须研究过渡技术，支持大范围的用户使用，这样也就阻碍了下一代网络的推进。

3）现在市场决定设备发展，没有大范围地使用 IPv6，就

不会使设备都具有 IPv6 的功能；并且 IPv4 设备与 IPv6 设备同步使用也会出现不兼容问题，造成进一步的设备问题。

4）现在毕竟基于 IPv6 的应用市场中不是很多，不具有带动作用，很多研发单位也不会投入很多资金去进行这样的研究。

（3）实现网络承载功能

整个骨干网将主要的节点升级为双协议栈，将基于 CN2 的 PE 设备升级到 6PE/6VPE，这样就可以实现承载 IPv6 流量，进而就形成了骨干网的双协议栈结构。对于城域网，接入设备就实现开启 IPv6 的功能，这样做可以减少对 BRAS 的升级，节省成本开支，也实现了双协议栈带宽接入能力，对于那些不具备升级能力的 BRAS，可以使用 L2TP 方式进行带宽接入，这些可以在一定程度上减少下一代网络实际部署难题。

上述需要克服的问题，都不是某一个运营商能单独进行解决的，而是需要国家的支持、产业链的努力、技术的不断发展，而最根本的是下一代网络技术发展方向的问题。

3 下一代网络未来亟待克服的问题

对江苏电信下一代网络实践经验的研究以及对下一代网络整个体系结构的研究，明确说明了下一代网络的整体发展[12]需要一个比较长的实践过程才能完善，并需要在整体上加以突破和发展。根据实际情况，下一代网络研究重点应该集中于以下几个方向。

（1）网络承载方面

现在世界网络的 IP 地址已经处于枯竭状态，最为迫切的是怎么解决 IPv4 地址短缺的问题，IPv6 自然将是其重点过渡技术。虽然目前有很多公私网络的地址翻译技术，比如 NAT 技术和 NAT444 技术，但是从发展下一代网络方面来讲，这些技术本质上还是原来 IPv4 NAT 技术向网络发展衍生出来的缓解 IPv4 地址压力的部署方案而已，并不算是一种新的技术。因此，未来发展过渡技术的重点仍是如何利用 IPv6 地址给用户提供接入服务，并要接受今天 IPv4 大量存在的现实。因此基于双协议栈、翻译技术原理的新型 IPv6 过渡技术将可能是解决问题的首选方法[13]。

（2）业务平台方面

在现在的网络环境下，大部分是 IPv4 业务平台，无论是运营商自己的业务平台还是其他开放的业务平台，都存在从 IPv4 到 IPv6 逐步过渡的情况，因此很好地实现这些平台的合理过渡将是一个重要的待解决的方向。然后需要考虑不同的业务提供商的不同能力，同时不可能只使用一种技术，而是需要引入一些应用迁移技术。另外，现在的大数据技术、物联网技术、移动互联网技术的应用是直接使用 IPv6 的好机会，但是也要考虑与其他 IPv4 业务平台间的互联互通问题。

（3）支撑系统

下一代网络发展过程中，如 AAA/DNS、MBOSS 等相关的支撑系统都具有 IPv6 特性，然而现在 IPv6 的发展支持力度不够，从而这些系统的软件层面在支持 IPv6 时就显得相对较弱。这就告诉我们推进 IPv6 时，系统升级也是需要注意的问题，并且使用过渡技术将是不可避免的。所以就需要将这些系统和过渡技术配合好、利用好，做到让业务具有可用性、可控性、可管性等特征；在计费、流量监控等方面必须有一个好的解决方案。

4 NGN 网络安全技术解决方案的研究

4.1 安全现状

当前“十三五”计划加强网络安全建设，加之“互联网＋”和 5G 技术在业界被大力提倡，因此下一代网络的安全问题更是整个网络的重中之重。现在网络上对视频和语音等的截取以及解密行为对网民的隐私和信息造成了极坏影响，并且网络攻击事件时常发生，所以网络泄密严重威胁到了下一代网络安全[14]。IPv6 技术、云计算技术、物联网技术等将产生更为复杂的网络安全攻击问题；现在运营商网络的规模很大，这会导致更多的安全弱点出现，而且现在运营商的安全体系建设各不相同，复杂程度高，最终导致运营商的骨干网和信息系统更受到各类的攻击，进而盗取用户信息和其他重要信息的事件不易被发现，这样就不得不需要新的安全体系来维护并保证运营商的信息安全。

4.2 早期 P2DR 安全模型安全防护体系

最开始的安全体系是比较原始的体系，基于 P2DR，主要是由策略、防护、检测和响应这 4 个部分组成。

（1）策略（Policy）：开始对运营商的整个安全策略体系进行分析，然后根据这个安全风险分析得出所需的安全策略，这个安全策略将要描述需要保护的资源以及实现保护的方法。策略是网络安全模型的核心部分，并且各种防护、检测和相应响应都是根据这个安全策略进行的。安全策略制定的正确与否直接影响到整体系统的安全。

（2）防护（Protection）：不断修复系统漏洞、修正设计开发并安装系统来预防安全事件的产生；然后设定固定时间来发现系统存在的漏洞；通过培训手段使用户和管理员正确地应用系统，阻止意外的威胁；最后使用访问控制技术和网络监控手段来阻止恶意威胁。防护技术包括数据加密、身份认证、访问控制技术、授权和 VPN 技术、防火墙等，这就是防护的基本方法。

（3）检测（Detection）：不断地检测和监控网络系统，以动态响应和加强防护为依据，寻找出系统新的威胁以及弱点，然后不断循环反馈来及时做出有效的响应。这样做使得在攻击者攻击防护系统时，检查功能皆可以发现威胁并及时对威胁进行处理。

（4）响应（Response）：响应是由于检测到网络入侵而进行的事件处理，包含紧急响应和处理，处理可以有系统恢复和信息恢复。这种处理安全的方式的好处是通过风险评估理论把安全当作动态的系统进行处理。

对于以上的安全体系，网络安全领域开始产生很多的设备，如防火墙、入侵检测系统等，其实现在很多公司依然将入侵检测系统作为主要的处理网络入侵的技术。

4.3 近期木桶原理安全防护体系

网络的发展不断地加深了人们对网络安全的理解，并促使人们对网络安全的本质进行探索，最后形成了基于木桶原理的安全防护系统的思想。这个安全防护原理是说，整个网络系统的安全并不是整体决定的，而是由其中最弱的一部分决定的；即整个安全体系的建设要求去找出整个网络所有的安全边界，通过这些安全边界，做到每一点都能够得到很好的

防护，这样做就可以实现网络的整体安全。然而实践证明，依靠这种思想去指导安全体系建设，使用网关防护设备确定网络的入口边界，使用第三方专业的网络版防病毒系统等方法做到安全保护，虽然效果很好，但是成本上升，不能很好地利用设备资源，增加了资金成本。

传统的安全防护系统就是基于这种木桶原理进行的，但是缺点也是显而易见的，即只要其中的一点被攻击破，则其他的部分也就很容易被攻击，最后的结果可能是整个安全系统崩溃。因此，现在基于传统的安全防护体系已经不能满足网络发展的需要。

4.4 使用大数据技术建设下一代网络安全防护体系

安全防御体系主要基于主动威胁防御和被动威胁防御两种思想。过去基于木桶理论的安全防护体系属于被动威胁防御思想。现在的安全防护体系则是主动发现威胁，且不论威胁怎么变化，其总是可以被感知的，遵守图 2 模型。威胁仅仅有两种入侵途径：从外部网络向内部网络入侵的威胁途径及从内部网络向外部网络扩散入侵的威胁途径。从外部网络向内部网络攻击的方式主要是黑客攻击等，而反向攻击的最常见的事件就是 U 盘病毒。如图 2 所示，如果能够将这两种关键性的路径进行检测和控制，就可以杜绝威胁产生的途径，以最小的安全成本解决下一代网络的安全问题。随着大数据技术的发展，基于大数据技术的“安全云、端、边界”的安全架构可以很好地解决现在突发式的安全问题，其模型架构如图 3 所示。

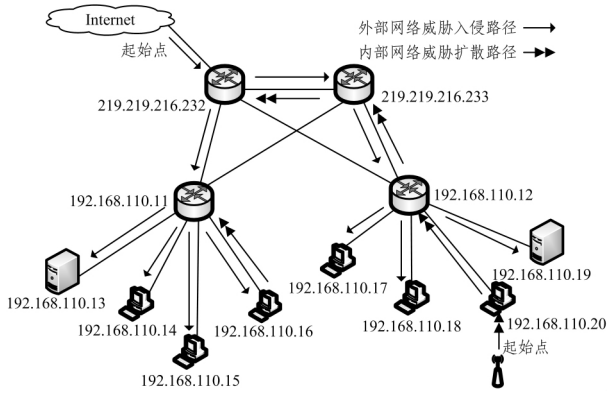

图 2 威胁入侵模型

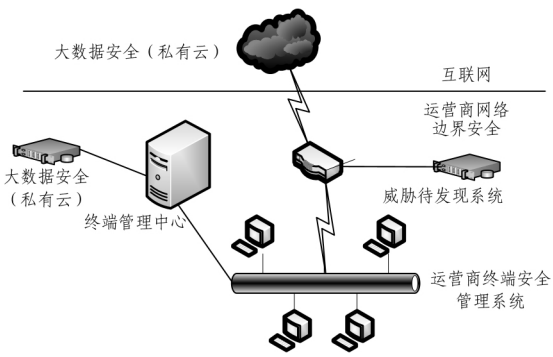

图 3 基于大数据技术的“安全云、端、边界”的安全架构

基于大数据技术的“安全云、端、边界”的安全架构是用于解决新的网络威胁问题而出现的下一代网络智能防护系统架构，整个系统架构包含大数据安全、运营商网络边界安全和运营商终端安全等 3 个主要的关键部分。基于大数据安全的平台就是以大数据技术为核心建立的捕获安全威胁的系统，分为公有云和私有云两部分。在整个互联网大环境下，则使用公有云进行安全威胁捕获；在隔离网络环境下，则是使用私有云进行安全威胁捕获。对于边界安全，可以通过大数据安全技术发现未知威胁，端安全能够使用大数据技术来实现终端安全管理和防护。大数据安全就是我们常说的云安全体系，一般的云安全模型如图 4 所示。

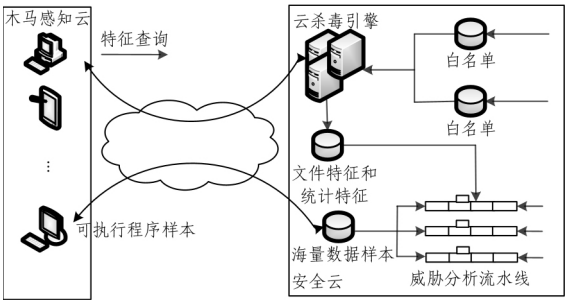

图 4 大数据安全分析模型

通过使用终端服务器的木马感知云，可以将很多的可疑威胁数据收集到安全云中，先是从海量数据中分拣数据，然后把分拣好的数据样本输入到恶意软件分析流水线进行处理，接着将分析得到的样本数据进行黑白名单的分类，最后将产生的大数据安全数据提供给云端的杀毒系统使用。这样的一个系统是自循环系统，所以可以在很短的时间内发现网络上存在的新的威胁，然后将这些威胁分析整理后用于边界防御和终端防御，这样能够很好地实现对下一代网络的安全防御。

4.5 使用深度神经网络感知网络安全态势

目前深度神经网络算法对数据学习、预测和分类都表现出了很好的效果，如果将神经网络应用到下一代网络的网络安全预测中，将能够及时发现网络中存在的安全问题，降低网络安全问题出现后解决问题的成本。基于深度神经网络的网络安全预测通过对网络中安全相关的元素进行提取分析，理解网络数据状态，预测网络安全的发展态势并及时提出解决方案。Srihari R K[15] 提出的用于获取预测信息的要素提取方法，并没有考虑数据的多元化，更没有对安全的发展趋势和结果进行过多研究，因此并不能很好地解决安全预测问题；国内的谢丽霞等[16] 通过使用神经网络实现安全态势预测，但是其预测方法还是由人工完成，比如数据采集、元素提取等。因此这些方法都不适合在整个下一代网络的大环境中实践应用，所以自动收集数据、将预测的结果进行可视化、增大网路的范围和复杂程度等可以是未来研究的对象。

4.6 下一代网络的安全预测和基于大数据的防护技术共同解决下一代网络安全问题

根据 4.4 节对基于大数据的安全防护体系的研究，在云感知部分，现在还没有研究通过使用深度神经网络进行网络威胁检测和预知。通过网络数据的搜集，使用神经网络天生的强学习功能，就可以对下一代网络中未知威胁进行感知，其神经网络算法如图 5 所示。正如 4.4 节和 4.5 节中所述，如果将这两个技术接合在一起，将可能实现网络无威胁的状态，但是现在还需进一步的研究和实验。

（下转第 376 页）

[8] Tuyls P, et al. Read-proof hardware from protective coatings[C]// 8th International Workshop, Vokohama, Janpan. October 10-13, 2006:369-383

[9] Cao Yuan, Zhang Le, et al. A low-power hybrid RO PUF with improved thermal stability for lightweight applications[J]. IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems, 2015, 34(7):1143-1147

[10] Masato T G C, Mitsuru S, et al. A stable key generation from PUF responses with a fuzzy extractor for cryptographic authentications[C]// IEEE Global Conference on Consumer Electronics. 2013:525-527

[11] Guajardo J, Kumar S S, Schrijen G J, et al. FPGA Intrinsic PUFs and Their Use for IP Protection[M]. Cryptographic Hardware and Embedded Systems-CHES 2007. Springer Berlin Heidelberg, 2007:63-80

[12] 李晖,夏伟,邓冠阳,等. PUF-HB#:轻量级 RFID 双向认证协议[J]. 北京邮电大学学报,2013,36(6):13-17

[13] Majzoobi M, Rostami M, et al. Devadsa S. Slender PUF protocol: A light weight, robust, and secure authentication by substring matching[J]. IEEE Symposium on Security and Privacy Workshops, 2012:33-44

[14] 向学哲,马昌社. 基于 PPUF 的高效 RFID 隐私认证协议[J]. 华南师范大学学报,2013,45(1):42-46

[15] Canteaut A, Chaband F. A New Algorithm for Finding Minimun-weight Words in a Linear Code: Application to McEliece's Cryptosystem and to BCH codes of length 511[J]. IEEE Transactions on Information Theory, 2010, 44(1):367-378

[16] Hori Y, Yoshida T, et al. Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs[C]// 2010 International Conference on Reconfigurable Computing and FPGAS, Cancun, Quintana Roo, Mexico, 13-15 December 2010:115-120

(上接第 361 页)

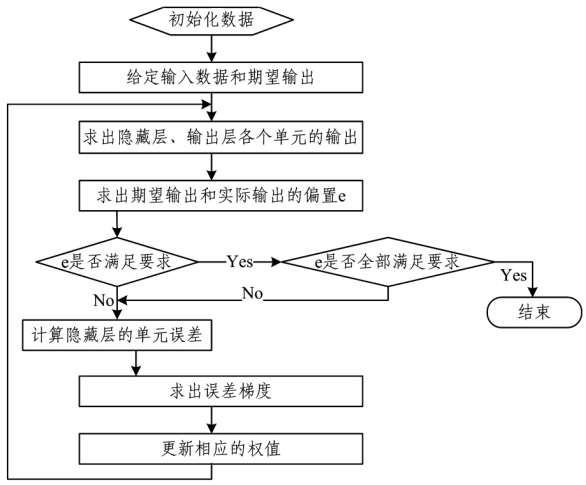

图 5 神经网络算法

结束语 综上所述,可以确定的是网络的体系架构对未来下一代网络的发展方向起着关键性的作用。基于电的分组交换网络和基于光的光交换网之间的紧密联系和数据交换是下一代网络将要研究的对象。我国应该注重组织新的示范网工程,使之达到局部验证成功到大面积推广的效果,这样不仅可以实现更宽的带宽,而且可以在实践中发现问题并可以方便连接各个网络。另外,网络安全是未来下一代网络不可逾越的问题,再加上未来网络速度更快、带宽更宽、运营商的网络规模庞大且结构复杂,网络容易受到攻击的部分也会越来越多,如果采用过去的基于"木桶理论"的安全边界防护体系,这个任务必定是难以完成的。然而使用大数据技术建设下一代网络安全防护体系,就可以利用丰富的检测分析数据迅速发现新的威胁内容;同时深度神经网络的学习也可以预测危险,及时高效地发现网络的安全问题并加以解决。因此未来下一代网络安全的发展将是基于深度神经网络和大数据安全防护的下一代网络安全体系。

参 考 文 献

[1] 程海燕,董见. 下一代网络技术在移动通信网络中的应用[J]. 信息通信,2014(7):210-210

[2] 赵慧玲. 软交换下一代网络的核心[J]. 中国电信业,2001(4):47-49

[3] 于伟. NGN 网络 QoS 的分析和保障[D]. 青岛:山东大学,2009:1-3

[4] 肖勇. 基于服务元网络体系结构的实时通信系统的设计与实现[D]. 成都:电子科技大学,2008

[5] 李国杰. 关于下一代网络的体系结构[J]. 中国工程科学,2002(8):40-43

[6] 樊秀梅,林闯,王忠民. 网边缘可控的 IP QoS 体系结构及其算法[J]. 电子学报,2002,30(12A):2027-2031

[7] ITU. ITU releases annual global ICT data and ICT Development Index country ranking[R]. Geneva, Switzerland, ITU, 2015

[8] Saltzer, et al. End-to-End Arguments in System Design [J]. ACM Transactions in Computer System, 1984, 11(3):277-288

[9] Clark D D, Blumenthal M S. Rethinking the design of the Internet: The end to end arguments vs. the brave new world[J]. ACM Transactions on Internet Technology — TOIT, 2001, 11(1):70-109

[10] 李国杰,徐志伟. 关于下一代网络体系结构和应用模式的思考[J]. 武汉理工大学学报(信息与管理工程版),2002,10(4):1-6

[11] 史凡,姚建锋,陈运清. 下一代互联网络体系架构与现网络演进实践[J]. 电信技术,2011,5(15):67-70

[12] 王璐. 移动互联网用户行为分析[D]. 北京:北京邮电大学,2011

[13] 乐红文. 典型 IPv6 过渡技术的仿真与组网设计[D]. 南昌:南昌大学,2011

[14] 张晓兵. 下一代网络安全解决方案[J]. 电信工程技术与标准化,2014,6(13):59-61

[15] Srihari R K. Situation awareness through concept—based information extraction [EB/OL]. (2012-05-20). http://www.dawnbreaker.com/vas05

[16] Xie Li-xia, Wang Ya-chao, Yu Jin-bo. Network Security Situation Awareness based on Neural Network [J]. Journal of Tsinghua University(Science and Technology), 2013, 53(12):1750-1760