一种基于 IPv6 的物联网分布式源地址验证方案

胡光武[1)] 陈文龙[2)] 徐 恪[1)]
[1)](清华大学计算机科学与技术系 北京 100084)
[2)](首都师范大学信息工程学院 北京 100048)

摘 要 作者在融合物联网的新一代互联网网络环境下,提出了基于 IPv6 的源地址验证整体架构.基于该架构,考虑物联网节点资源受限特点,并结合物联网末梢网络的拓扑形态及其路由方式上的特征,设计了基于 IPv6 的物联网末梢网络分布式源地址验证方案.分别讨论了静态指定、SLAAC(Stateless Address AutoConfiguration)、DHCPv6(Dynamic Host Configuration Protocol Version 6)以及 DHCPv6 与 SLAAC 混合情况下的物联网节点 IP 地址分配及其验证机制.模拟实验表明,该方案仅以微小的代价实现了物联网节点 IP 地址的分配,同时还保证了物联网节点之间、物联网节点与互联网端系统之间端到端通信时双方 IP 地址的真实可靠性,从而整体上增强了物联网的安全性.

关键词 物联网;IPv6;源地址验证;DHCPv6;SLAAC
中图法分类号 TP393 **DOI 号**:10.3724/SP.J.1016.2012.00518

An IPv6-Based Distributed Source Address Validation Scheme in Internet of Things

HU Guang-Wu[1)] CHEN Wen-Long[2)] XU Ke[1)]
[1)](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)
[2)](*Information Engineering College, Capital Normal University, Beijing* 100048)

Abstract Under the background of Next-Generation of Internet based on the Internet of Things (IoT), an architecture of IP source address validation is proposed in this paper. Considering the resource-restraint of IoT nodes, the distributed IPv6 source address validation scheme is designed according to this architecture as well as the topology and routing manner in end-edge network of IoT. Meanwhile, IPv6 address allocation methods for IoT nodes and their authentication mechanisms are respectively discussed under the scenarios of static assignation, DHCPv6, SLAAC and DHCPv6-SLAAC mixed. The simulation has proved that our scheme can not only implement IP address allocation, but also keep the IP address authenticity with slight cost among IoT nodes, as well as between IoT nodes and Internet end-host. As a result, the whole security in IoT is enhanced.

Keywords Internet of Things; IPv6; source address validation; DHCPv6; SLAAC

1 引 言

物联网(Internet of Things,IoT)是在无线传感器网络(Wireless Sensor Networks,WSNs)基础上发展形成的一种融合无线射频识别(RFID)系统、传统有线和无线互联网、移动通信网络以及其它通信技术的新兴泛在网络.我国对物联网的定义是指

收稿日期:2011-08-31;最终修改稿收到日期:2011-12-28.本课题得到国家"九七三"重点基础研究发展规划项目基金(2009CB320501)、国家"八六三"高技术研究发展计划项目基金(2008AA01A323,2008AA01A326,2009AA01A334)、"新一代宽带无线移动通信网"国家科技重大专项项目基金(2012ZX03005001-001)资助.**胡光武**,男,1980 年生,博士研究生,主要研究方向为计算机网络体系结构、高性能路由器、物联网.E-mail:hgw09@mails.tsinghua.edu.cn.**陈文龙**,男,1976 年生,博士,讲师,主要研究方向为计算机网络体系结构.**徐 恪**,男,1974 年生,博士,教授,博士生导师,主要研究领域为新一代互联网体系结构、高性能路由器体系结构、P2P 与应用层网络、物联网等.

“通过信息传感设备，按照约定的协议，把任何物品与互联网连接起来，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，它是在互联网基础上延伸和扩展的网络”①. 尽管国际电信联盟(ITU)②、欧盟③④以及我国对物联网的定义稍有不同，但其共识是：物联网中的任何物体能在任何时间、任何地点都能够与其它任何物体进行连接，具有在时间、地点、物体三个维度下的任意连接性.

物联网在仓储物流、智能交通、环境保护、工业监测、智能家居、远程医疗、公共安全以及环境保护等各方面显示出极大的应用前景，许多发达国家已将物联网列为国家战略予以扶持和研发. 2005 年国际电信联盟 ITU 发布了《ITU Internet Reports 2005：The Internet of Things》②，2008 年 IBM 提出了“智慧地球”⑤的概念，2009 年 6 月欧盟委员会提出了物联网行动方案[1]，而我国在 2009 年也提出了“感知中国”的物联网发展概念，并将物联网技术及发展规划列入 2010 年政府工作报告以及“十二五”重点开发计划. 由此可见，物联网应用前景广阔，世界主要国家正对其展开积极的研究.

物联网与传感器网除了体系架构不同之外，最大的区别在于物联网具有“感知”功能. 物联网中的物品节点能与遵循协议的其它物品联接，交换数据，并能与互联网设备及端系统通信，上传数据并进行智能分析和判别，可以说物联网是在互联网基础上，无限延伸的智能化一体化网络.

近年来，随着物联网研究的深入，已取得一些重要成果. 2000 年 12 月 IEEE 标准委员会成立了 802.15.4 协议工作组，目标是开发一个低速率的无线个域网 LR-WPAN(Low Rate-Wireless Personal Area Network)标准；2004 年 11 月 IETF 成立了 6LoWPAN(IPv6 over Low power WPAN)工作组，其目的是制订基于 IPv6、以 IEEE 802.15.4 协议作为底层标准的低速无线个域网标准[2-4]；2008 年 2 月 IETF 成立了 ROLL(Routing Over Low-Power and Lossy Networks)工作组，目标是使得公共的、可互操作的第 3 层路由能够穿越任何数量的基本链路层协议和物理媒体；2010 年 3 月 IETF 成立了 CoRE (Constrained Restful Environments)工作组，旨在研究资源受限物体的应用层协议；2011 年 3 月 IETF 又成立了 LwIP(Light-weight IP)工作组，其目的是在资源受限的设备上实现轻量级 IP 协议栈.

物联网中的节点具有与互联网节点一致的 IP 地址后，物联网节点之间、物联网节点与互联网节点之间就具有了端到端的通信能力. 给每个物联网节点赋予 IPv6 地址，运行简化的 IPv6 协议，不仅能解决物联网末梢网络间、物联网末梢网络与 Internet 间的互连互通问题，同时还克服了无线传感器网络的内在缺点，如需数量巨大的地址资源、缺乏有效的地址管理及安全机制等问题.

物联网节点被赋与了与互联网终端一致的 IP 地址后，尽管在寻址、路由、通信等方面带了巨大便利，然而传统互联网中所存在的一些安全问题也随之而来. 其中，最重要的就是物联网节点的认证及节点 IP 源地址的可靠性问题. 互联网发展之初，基于网络的简单性和用户的可信性，在其协议设计中，路由器并不对 IP 数据分组中的源地址进行检查，而只根据目的地址进行路由转发. 这种缺陷直接造成了 DoS[5]/DDoS[6]、Smurf⑥、SYN flood[7] 等一系列攻击及病毒侵袭行为发生. 攻击者为了隐藏其身份，往往使用假冒的 IP 地址以躲避追查. 与此同时，随着互联网规模急骤增大和用户规模不断增长，这一现象也更加突出. 据国际电信联盟和中国互联网信息中心的报告，截止到 2010 年底，全球互联网用户数达 20 亿⑦，而中国的网民规模已超 4.57 亿⑧. 而与此同时，据美国麻省理工学院的 IP Spoofer 项目组统计，截至到 2011 年 7 月 6 日，全球可被假冒的地址块、IP 地址及自治系统的比例分别达到了 10.4%、29.8%和 19.8%⑨.

由于 IP 地址具有身份和位置的双重语义，如果

① 温家宝. 2010 年政府工作报告. http://www.gov.on/2010lh/conent_1555767.htm

② International Telecommunication Union. Internet Reports 2005：The Internet of Things. http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

③ European Research Projects on the Internet of Things (CERP-IoT) Strategic Research Agenda (SRA). Internet of things-strategic research roadmap. http://ec.europa.eu/information_society/policy/rf id/documents/in_cerp.pdf

④ Commission of the European Communities. Internet of Things in 2020. http://www.umic.pt/images/stories/publicacoes2/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf

⑤ IBM. Smarter Planet. http://www.ibm.com/smarter-planet

⑥ Computer Emergency Response Team. CERT Advisory Smurf IP Denial-of-Service Attacks. http://www/cert.org/advisories/CA-1998-01.html

⑦ International Telecommunications Union. ICT Facts and Figures. http://www.itu.int/ITU-D/ict/material/Facts-Figures2010.pdf

⑧ 中国互联网络信息中心. 第 27 次中国互联网络发展状况统计报告. http://www.cnnic.net.cn/dtygg/dtgg/201101/P020110119328960 192287.pdf

⑨ MIT. Spoofer Project. http://spoofer.csail.mit.edu/summary.php

物联网节点的源地址一旦被冒用,那么节点传感器传回数据的真实性将难以保证,这就使该应用场景的安全性大打折扣,甚至可能危及整个系统.目前,这个问题的严重性还没有引起研究人员的足够重视和注意.

基于以上现状,本文提出了一种基于 IPv6 的分布式物联网节点源地址验证机制.其贡献在于:(1)在融合物联网的新一代互联网网络环境中,提出了基于 IPv6 的源地址验证方案整体架构;(2)针对静态指定、DHCPv6、SLAAC 和 DHCPv6 与 SLAAC 混合等地址分配方式,详细描述了物联网节点地址获取、绑定等过程的场景交互,以及地址分配过程中的时序及状态变迁细节;(3)根据物联网末梢网络中节点规模和地址分配场景,设计了基于 IPv6 的物联网末梢网络分布式源地址验证方案.

本文在第 2 节中将概括介绍源地址验证课题上已有的相关工作研究,以便让读者对本研究方向有一个全面的了解;第 3 节是本文的重点,该节详细介绍了本方案的设计思路和实现细节.作者将首先提出融合物联网的新一代互联网源地址验证框架,然后对物联网节点的地址获取方式予以说明,最后对不同地址分配方式下的分布式物联网节点源地址验证方案进行详细阐述.此外,与方案相关的问题也在本节进行了讨论;方案的实验模拟及性能评估将在第 4 节中给出,最后一节我们将对全文进行总结,并说明进一步需要深入研究的工作.

2 相关工作

源地址验证是指对终端节点发出的 IP 数据包中的源地址字段数据进行检查和验证,以保证其发送者 IP 地址的真实性和有效性.为了达到源地址验证及丢弃假冒数据包的目的,目前已有许多方案,我们简单总结如下:

(1)入口过滤. Ingress Filtering[8]是一种用于识别和丢弃假冒数据包最常用最直接的办法. uRPF① (Unicast Reverse Path Forwarding)就是思科公司提出的一种在数据包入口上进行单播反向路由查找以验证和过滤数据包的办法,其主要思想是根据数据包的源地址反查路由表,判断转发端口是否与数据包的入端口一致,从而确定数据包源地址的合法性.其缺点是无法防止同方向上的地址假冒,同时路由的非对称性也可能导致假阳性的误判. SAVI② (Source Address Validation Improvements)技术采用在用户接入交换机上嗅探接入主机地址分配协议的方法,实现了主机 IP 和 MAC,交换机端口,甚至用户名及登录时间等多元信息的绑定,达到了在用户接入交换机中进行假冒数据包过滤的目的,保证了用户身份的可靠性.现在已有多家国内厂商开发出其商用产品,但目前仅适用于 IPv6 以太网,并且尚未大规模应用.

(2)协议重设计. SAVE[9]方案对路由器及用户主机协议栈进行重新设计,研究出了一整套数据包验证及其路由机制,但该协议过于复杂并且需要修改用户主机协议栈,因此目前无法应用于实际.而 SPM[10]、Passport[11]、StackPi[12]、Base[13]等方案在 IP 包头中的 ToS 或其它较少使用的选项字段加入用户身份鉴别标签,当数据包出自治域或管理范围时使用专用设备进行验证并去标签,其缺点是假冒者可以学习标签的添加方法,从而逃避验证.另外对数据包包头字段的修改可能会影响自治域内包括 QoS 在内的其它特殊应用. HIP[14]方案则是修改用户终端主机协议栈,在 IP 和传输层之间添加"主机标识层",通过分离主机 IP 地址身份和位置语义,从而达到了源地址验证、加密和扩展性的目的,但端系统的修改、应用还存在着实际困难.

(3)源地址加密和跳数推测. TrueIP[15]、CGA[16]、AIP[17]等方案将数据包中的源地址用加密后的地址信息取代,以达到识别、验证和防止篡改的目的,但其缺点是需要引入密钥管理服务器,对源地址与对应加密后的地址进行映射和查询,因此引入了额外的开销,甚至有可能成为网络瓶颈点.还有方案[18]对数据包中的 TTL 值进行 Hop 推测,通过逐步学习建立起正常数据包跳数范围取值区间,对于 TTL 值明显偏离取值范围的数据包则判定为假冒源地址数据包.这一方法存在着明显的假阳性或假阴性的可能,从而会造成误判或漏判.

(4)整体方案.清华大学吴建平教授等人提出了 SAVA[19](Source Address Validation Architecture)源地址验证整体方案框架(RFC5210),该方案将互联网整个源地址验证级别分为三部分:接入子网验证、域内验证和域间验证.不同的级别达到不同

① Cisco. Unicast reverse path forwarding. http://www.cisco.com

② Wu J, Bi J. Source Address Validation Improvement Framework. http://datatracker.ietf.org/doc/draft-ietf-savi-framework

的验证粒度：接入子网达到了端系统用户主机的验证；域内验证达到了域内子网 IP 前缀粒度验证；域间验证达到了 AS 粒度的验证. SAVA 在每个别级均有相应的子方案. 目前，该方案正逐步部署到我国最大的纯 IPv6 网络 CNGI-CERNET2.

由于物联网是一种新兴的网络形态，并且物联网节点在引入 IP 地址后，如何防止源地址假冒的问题还并未得到研究和重视. 因此，到目前为止，还没有适用于物联网环境的源地址验证研究文献. 本方案是一种基于 SAVA，适应于融合物联网的新一代互联网环境下的源地址验证整体方案.

3　基于 IPv6 融合物联网的新一代互联网源地址验证方案

根据物联网是“按照约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的目的，是在互联网基础上延伸和扩展的网络”[20] 的定义，我们对物联网及其源地址验证方案有如下认识：

(1) 与互联网的概念类似，物联网也是唯一的，任何物品能连接到以 IPv6 为核心的互联网上，形成的一种智能网络；

(2) 物联网节点应具有 IPv6 地址；

(3) 物联网的核心应是以 IPv6 为基础的互联网，但不排除物联网节点能通过互联网的双向翻译网关或隧道机制与传统的 IPv4 终端主机通信；

(4) 由物联网节点组成的局部网络接入在互联网的边缘，我们称之为物联网接入子网或物联网末梢网络. 由互联网及全部物联网接入子网所组成的网络，对物而言，我们称之为物联网，对 IPv6 为核心的互联网，我们称之为融合物联网的新一代互联网；

(5) 在物联网节点中，有一部分节点自身具备一个或多个传感器，并将传感器采集的数据上报给互联网的终端主机，并与之进行端到端的通信，我们称这些节点为物联网传感器节点；而还有一部分节点本身并不具有传感器，也不进行环境数据的收集，但它们的 CPU、内存以及电力等资源较传感器节点相对充足. 它们运行物联网路由协议，对传感器节点收发的数据进行中继传输，从而保证传感器节点能与互联网上终端主机进行通信，我们称之为物联网可路由节点；

(6) 因 6LowPAN 标准规定物联网物理层最大只能支持 127 字节的数据包，因此物联网节点只能运行轻量级 IPv6 协议，而互联网以太网上 IPv6 的最大传输单元(MTU)为 1500 字节，因此物联网接入子网连接到互联网、并与互联网主机进行端到端数据通信过程中，必须在其互联的位置使用专门的设备进行协议的翻译转换，我们称这种设备为多协议网关. 它与末梢网络通过无线方式进行通信，通过有线或无线的方式与接入互联网进行连接. 另外，在本文中，物联网节点在末梢网络中均使用 64 位 IP 地址. 因此多协议网关除了要完成协议的双向翻译外，还必须完成 IP 地址补齐和去前缀的工作.

(7) 依据物联网接入子网的规模大小以及物联网可路由节点与物联网传感器节点间的位置关系，我们将物联网接入子网又分为 3 种：单跳网络、层级网络和多跳网络. 单跳网络是指所有的传感器节点数据只需经过至多一个可路由节点就能到达多协议网关(如图 1 所示)；多跳网络是指一部分传感器节点无法直接与可路由节点进行通信，必须通过传感器节点间中继传输，在一个或多个可路由节点的转发下与互联网节点进行通信(如图 2 所示)；层级网

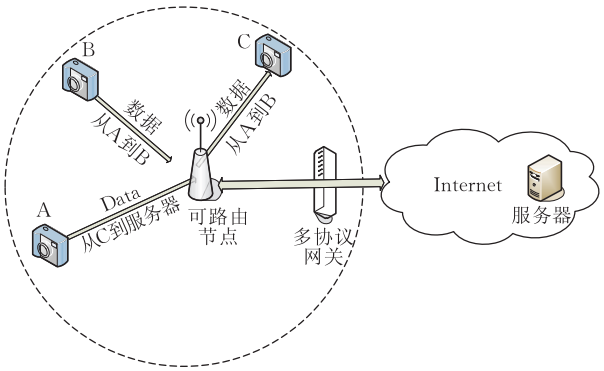


图 1　物联网末梢网络形态：单跳网络

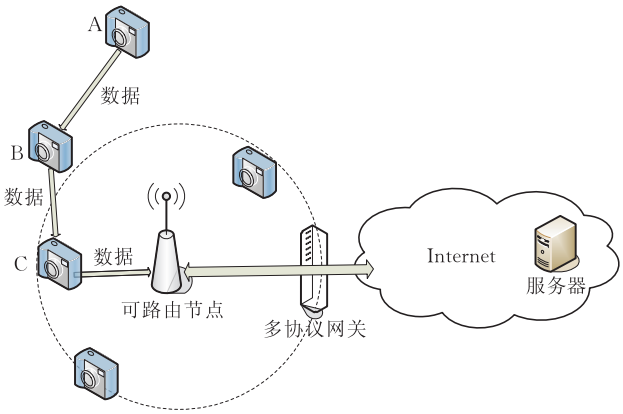


图 2　物联网末梢网络形态：多跳网络

络是单跳网络的扩展，是指所有的传感器节点都能直接与自己所覆盖的可路由节点进行通信，但数据至少需要一个以上的可路由器节点进行中继传输才能到达多协议网关(如图 3 所示).

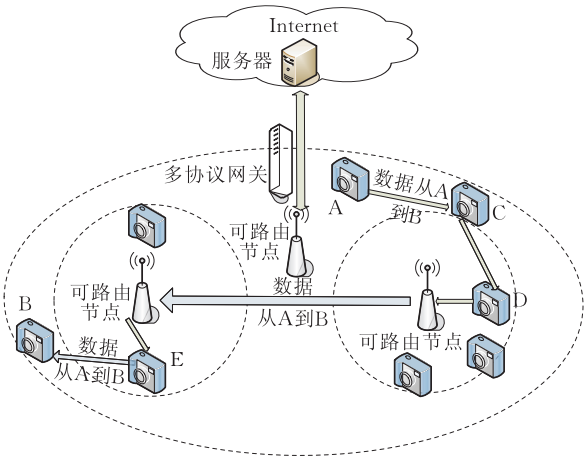


图 3 物联网末梢网络形态:层级网络

物联网与互联网的主要对比如表 1 所示.

表 1 物联网与下一代互联网主要对比

对比点	物联网	下一代互联网
主要目标	物物相连，数据交换	主机互连，高速通信
主要组成	传感器节点、可路由节点	主机、交换机、路由器
地址格式	IPv6 或轻量级 IPv6	IPv6
体系架构	6LoWPAN，ZigBee	TCP/IP
路由协议	RPL 等	OSPF/RIP/BGP 等
物理层	RFID，Bluetooth，802.11，802.15.4，ZigBee	Ethernet，Token-Ring，FDDI，ATM，WLAN
MTU	127 B	1500 B
子网形式	单跳、层级、多跳网络	星形、环形、总线型等
地址验证	末梢网络分布式验证	接入、域内、域间验证

3.1 融合物联网的下一代互联网源地址验证框架

基于以上认识，结合 SAVA 框架，我们提出了如图 4 所示的融合物联网的新一代互联网源地址验证架构，该方案具有 4 个层次：

(1) 在自治域间，运行 BGP 路由协议的 IPv6 骨干网络采用域间源地址验证方案，保证从自治域发出的数据分组中的源地址具有真实可靠性，达到自治域粒度的验证级别，具体的方案有 SMA[21] 等.

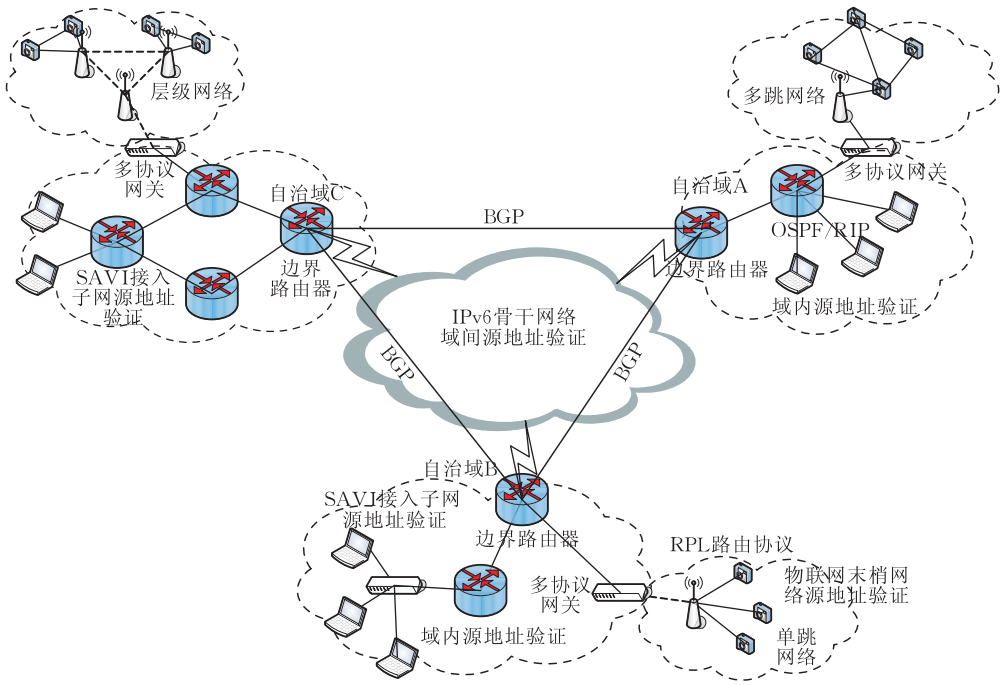


图 4 融合物联网的新一代互联网源地址验证架构方案

(2) 在自治域内，网络运行 OSFP、RIP、IS-IS 等路由协议，采用域内源地址验证方案，保证域内子网间主机无法互相假冒，具体的方案有 SAVT[22] 等.

(3) 在用户接入子网内，采用 SAVI 交换机技术，保证用户身份及主机真实可靠，达到主机粒度的验证级别.

(4) 在物联网接入子网内，可路由节点运行 RPL① 等路由协议，采用本文所提出的分布式源地址验证方案，保证物联网传感器节点 IP 地址的真实可靠性，达到传感器节点粒度的验证级别.

3.2 物联网 IPv6 接入子网分布式源地址验证方案

由于源地址验证方案是与 IP 地址分配方式密切相关的，因此在介绍物联网接入子网分布式源地

① Winter T et al. RPL: IPv6 Routing Protocol for Low Power and Lossy Networks. http://tools.ietf.org/html/draft-ietf-roll-rpl-19

址方案之前，我们必须对物联网节点地址的分配方式及其验证方式同时进行分析.

在地址分配方式上，目前在 IPv6 互联网中，有静态地址分配、无状态的地址配置(Stateless Address AutoConfiguration，SLAAC[23])、有状态的地址配置(Dynamic Host Configuration Protocol Version 6，DHCPv6[24])和 DHCPv6 与 SLAAC 混合的 4 种地址分配方式.

而在验证方式上，有集中式和分布式两种方案. 集中式是指在物联网接入子网连接的互联网管理网络内增加一台物联网节点源地址管理服务器，管理员将传感器节点的 EPC(Electronic Product Code 节点对象的唯一标识)编码、MAC 地址以及 IP 地址等提前输入到服务器的绑定表中，而传感器节点网络接口地址在启用前，必须向服务器发送数据包进行自身 IP 地址验证，而多协议网关将监听该过程并记录验证返回的结果，进而放行或阻止携带该 IP 的数据分组通过(当然，多协议网关也可充当源地址管理服务器的角色). 集中式方案的优点是对节点资源没有影响，但其缺点是只能保证该接入子网 IP 前缀级的真实性，而不能防止子网内部的互相仿冒，而这并不符合我们的设计目标. 由于每一个物联网可路由节点覆盖一定的区域，并承载对该区域内传感器节点数据中继传输的功能，因此分布式方案是利用可路由节点，验证选择其作为第一跳接入路由节点的传感器节点的 IP 地址的有效性.

在物联网可路由节点中，在控制层面上存在一个绑定状态表 BST(Binding Status Table)，用于监听和维护传感器节点地址绑定状态，主要字段有〈Index，EPC，IP，MAC，State，Lifetime，Other〉，其中 Index 为序号，长度为 8 位，范围为 1～256；EPC 编码是节点对象的唯一标识，由 64，96 或 256 位组成；IP 为节点网络层的地址，类型为 link-local 或 global，省去网络前缀，长度为 64 位；MAC 为节点在数据链路层的地址，长度为 48 位；State 为地址的绑定状态，长度为 1 个字节，可表达 256 种状态，其值可为手动静态绑定：Sta_Bound(0)，SLAAC 监听：SLA_SNP(1)，SLAAC 绑定：SLA_Bound(2)，DHCP 监听：DHCP_ SNP(3)，DHCP 绑定：DHCP_Bound(4)等；Lifetime 是每个状态下的生存时间，如 DHCP 地址续存时间等，长度为 2 个字节；Other 为保留字段. 同时，可路由节点在数据层面上还存在一个过滤表 FT(Filtering Table)，用来对转发的数据包进行过滤，只有匹配过滤表中登记的 IP 地址的数据包才予以转发，字段有〈Index，IP〉，其中 Index 为序号，其值与绑定表中的序号一致；IP 为绑定表中状态为绑定成功的网络层地址. 我们将具体讨论物联网传感器节点的四种地址分配方式及其分布式验证方式.

3.2.1　静态地址分配及验证方式

节点静态地址分配适用于物联网接入子网规模不是很大，管理员能将每个节点的地址预先配置后再进行部署. 在这种情况下，有两种方法支持节点的源地址验证.

(1)与集中式验证类似，管理网络内需增加一台地址管理服务器，管理员将传感器节点的 EPC 编码、MAC 地址以及 IP 地址事先配置到服务器的绑定表中. 传感器节点网络接口地址启用前，首先需要发送重复地址检测的邻居请求 DAD(Duplicate Address Detection)-NS(Neighbor Solicitation)报文，以验证自身 IP 地址的合法性，覆盖该节点的可路由节点充当 DAD-Proxy，将 DAD-NS 报文转发至多协议网关，由多协议网关翻译并将报文转交给验证服务器，得到验证服务器的确认回复后，可路由节点建立该节点的绑定关系和过滤表条目，之后匹配过滤表中的 IP 地址均可以直接发送数据分组. 其节点地址验证场景如图 5 所示.

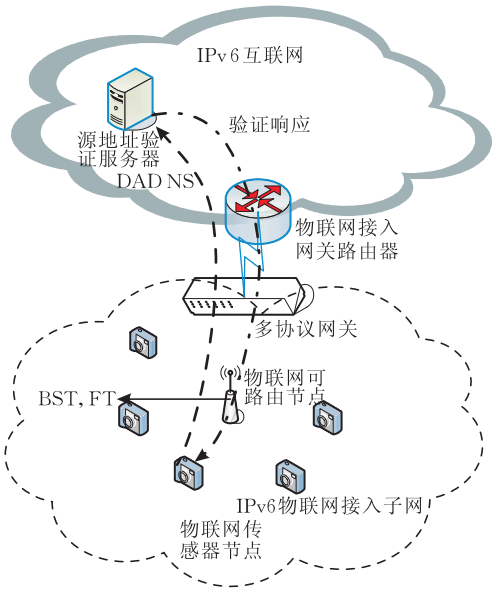


图 5　物联网节点静态方式源地址验证场景示意图

(2)管理员事先在可路由节点中建立传感器节点的绑定属性关系并生成过滤表，匹配的 IP 数据包可以直接转发，不匹配或不存在于过滤表项的 IP 地址将被过滤.

3.2.2 SLAAC 地址分配及验证方式

SLAAC 无状态地址分配是一种无状态、采用 ICMPv6 进行的地址配置方式，在传统互联网中主要经历 3 个过程.

(1)终端发起 NS 报文以请求网络配置参数，终端接入路由器回复 NA(Neighbor Advertisement)报文，将长度为 64 位的网络前缀等参数返回.

(2)终端再将自己 48 位的 MAC 地址映射为 64 位的 IEEE EUI-64 地址后[25]，与网络前缀一起形成 128 位的 IP 地址并进行配置.

(3)使用该地址前，终端还需要发出 DAD-NS 报文进行重复地址检测，若一段时间内无响应，则地址可用.

为了节省带宽、减少资源消耗，针对物联网特点，我们对 SLAAC 协议进行了简化，具体做法是省去以上过程的第一个步骤，即传感器节点在形成 64 位的 EUI 地址后，直接发出 DAD-NS 报文，之后与静态地址验证场景方式(1)类似，可路由节点充当 DAD-Proxy，向源地址验证服务器中继请求，并由源地址验证服务器返回正确的验证后，覆盖该传感器节点的可路由节点建立对该传感节点的绑定和过滤表项，不再赘述.

3.2.3 DHCPv6 地址分配及验证方式

DHCPv6 是一种有状态、采用 C/S 模式和 UDP 报文交互的地址分配方式. 在传统互联网中，通过 DHCPv6 获取地址一般要经过 5 个过程.

(1)客户端首先发送一个 DHCP Solicit 消息到一个特定多播地址(FF02::1:2，UDP 端口 547)，查找可用的 DHCP 服务器. 若 DHCP 服务器和客户端并不在一个接入子网内，则由路由器进行报文中继. 整个过程中，中继代理对于客户端是透明的.

(2)所有符合客户端要求的 DHCP 服务器以 DHCP Advertise 消息进行单播应答，返回给客户端.

(3)客户端从所有应答的服务器中选择一个(通常是最先到达报文所指向的服务器)，并向它发送 DHCP Request 消息来获取地址和其它配置信息.

(4)被选择的服务器以携带了被请求的配置信息(IP 地址、DNS、子网掩码等)的 DHCP Reply 消息进行应答.

(5)客户端根据返回的参数配置网络接口，并进行重复地址请求 DAD-NS，如果在一段时间内无任何响应，则该地址可用. 同时所获取的 IP 地址都存在由服务器指定的更新时间和有效时间. 当时钟到达更新时间，客户端必须向服务器发送一个 DHCP Renew 消息来续租该地址，服务器再向客户端返回一个带有新的更新时间的 DHCP Reply 消息. 如此反复，客户端就可以一直使用该地址. 如果客户端过了有效时间，服务器仍未收到客户端的 Renew 报文，那么客户端的地址就予以作废，而需要重做以上过程申请新的地址.

根据物联网的特点，我们对 DHCPv6 过程进行了简化，省去第一和第二步并做出改进，具体过程是：

(1)传感器节点发出 DHCP Request 到多播地址 FF02::1:2，UDP 端口 547；可路由节点中继该请求，并直接将该报文发送至多协议网关；之后，多协议网关再将该报文翻译后，单播发送至 DHCPv6 服务器.

(2)DHCPv6 服务器将配置信息以 DHCP Reply 消息进行应答给多协议网关；多协议网关翻译后单播发送至请求的传感器节点.

(3)传感器节点收到配置信息后，发出 DAD-NS 报文进行重复地址恳请，在一段时间内无响应即可使用该地址.

发出请求的传感器节点的第一跳可路由节点将监听传感器节点 DHCP 获取地址的整个过程，在最后 DAD-NS 超时无回复情况下建立绑定关系并生成过滤表项. 此外，需要指出的是，在绑定关系建立后，可路由节点还应向绑定的节点定期发送探测(Probe)报文，其主要作用有两点：(1)对节点有效性探测，以防止节点的移动或不可达造成地址浪费. 探测可通过发送 NUD(Neighbor Unreachability Detection)报文完成；(2)保持绑定关系，以防止因为某些节点长期不进行数据发送而造成地址错误回收的现象，可以通过 NA 报文完成. 其场景示意如图 6 所示，时序图和状态变迁如图 7、图 8 所示. 其中状态变迁图中存在的 6 个状态分别是

--：初态.

START：客户端发出 DHCP Request，即将触发绑定.

LIVE：DHCP 地址被 DHCP Server 告知.

DETECTION：可路由节点收到或者主动发送地址对应的 DAD NS.

BOUND：客户端的地址通过了冲突检测，建立了绑定.

QUERY：可路由节点询问绑定的无状态地址是否依然在使用.

3.2.4 DHCPv6 与 SLAAC 的混合地址分配方式

还有一种是将 DHCPv6 和 SLAAC 结合的混

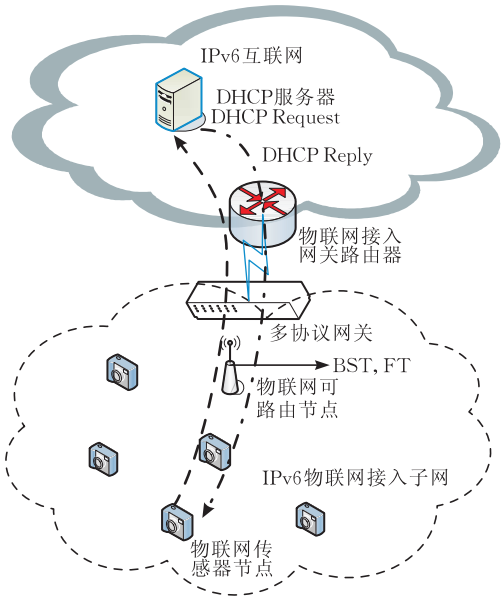


图 6　物联网节点 DHCPv6 方式源地址验证场景示意图

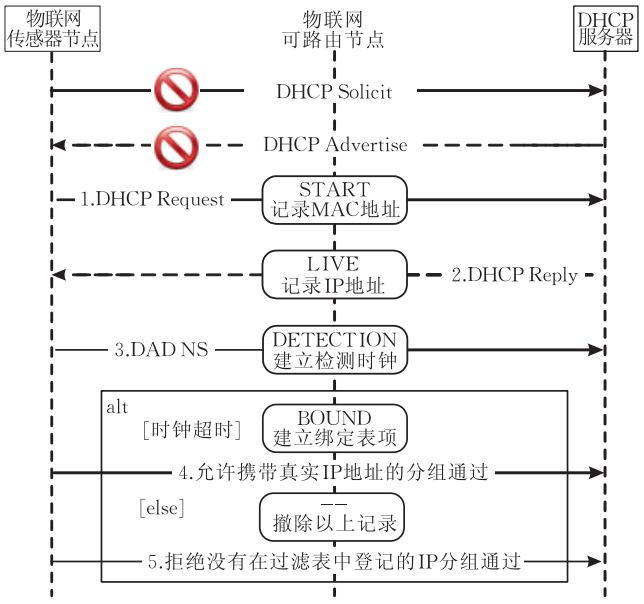


图 7　物联网节点 DHCPv6 方式源地址验证过程时序图

合地址分配方式，这是一种介于有状态和无状态之间的地址管理方式，即主机首先通过 SLAAC 方式获取 IPv6 地址，然后使用 DHCPv6 获取除地址以外的其它网络配置参数，如 DNS、域名后缀等.

就本文而言，我们重点关注的是 IP 地址的真实有效性，而在这种混合模式下，节点获取地址的方式仍是依托于 SLAAC，故这种混合方式下的源地址验证我们仍归于 SLAAC 方式验证.

3.2.5　小　结

物联网接入子网有单跳网络、层级网络和多跳网络 3 种形态；而物联网节点地址分配方式有静态

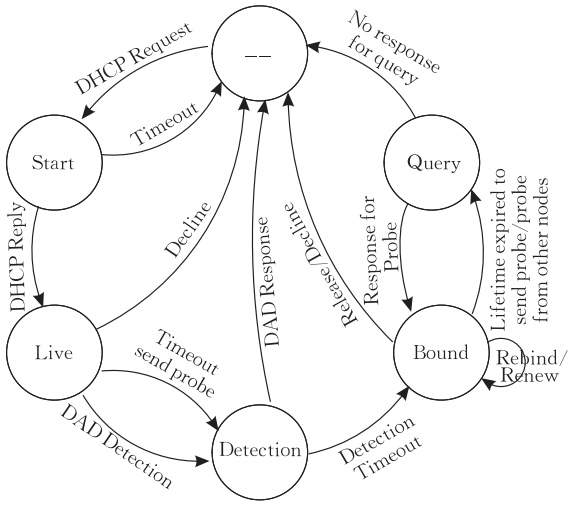


图 8　物联网节点 DHCPv6 方式源地址验证状态变迁图

指定、SLAAC、DHCPv6 以及 DHCPv6 与 SLAAC 混合的 4 种方案，在相应的验证方式中，验证对象均为传感器节点，验证主体为验证对象被覆盖范围内、所选择的第一跳可路由节点；总体上，节点 IP 地址验证方式又有集中式和分布式两种，集中式的优点在于对节点的资源无影响，但无法保证细粒度的地址验证，并且有可能造成瓶颈点；分布式方法的缺点在于对可路由节点的资源有所消耗. 我们就物联网源地址验证场景及方案进行了总结，如表 2 所示.

表 2　物联网接入子网源地址验证场景及方案总结

分配方式	网络形态			
	集中式	分布式		
		单跳网络	多跳网络	层级网络
Manual	(1) 建立地址验证服务器(可由网关代替) (2) 在验证服务器上进行实时验证	第一跳可路由节点事先绑定、实时验证		
SLAAC		第一跳可路由节点监听传感器节点 SLAAC 过程、绑定属性关系并验证		
DHCPv6		第一跳可路由节点监听传感器节点 DHCPv6 过程、绑定属性关系并验证		
Mixed		同 SLAAC 方式		

3.3　讨　论

在本小节中，我们就方案的相关问题予以讨论.

(1) 如何保证可路由节点源地址的真实有效性？

在本文中，我们并没有考虑物联网可路由节点 IP 源地址的有效性，原因在于，如同互联网路由器、交换机较互联网端系统主机信任度要高一样，可路由节点 IP 地址仿冒的可能性远没有传感器节点高，所以我们重点关注传感器节点源地址验证. 事实上，由于可路由节点的数量较传感器节点要少得多，因此，我们也可以采用集中验证方式对每个可路由节点单独验证.

(2) 如果没有可路由节点，如何对传感器节点

的 IP 地址进行验证?

物联网接入子网中如果没有可路由节点,那么传感器节点本身将充当可路由节点的角色,运行路由协议,进行数据的转发.这样就加重了节点资源的消耗,这也是不太现实的,否则就形成了类似于 ad-hoc 自组织网络形态,那么节点间的数据传输将并不依托于网络层地址,因此 IP 地址的功能将会大大被弱化.但是为了保证能与互联网端系统靠 IP 地址进行端到端的通信,我们可以采用被验证节点的邻居节点作为验证主体,监听其地址的获取过程并建立绑定关系表.由于邻居节点可能存在着多个,因此可以采用所有邻居投票累计或加权的方式进行验证.当然,其详细的机理还需进一步的研究.

4 方案评估

我们采用了 UC Berkeley 大学推出的针对物联网基于 TinyOS 的 TOSSIM① 模拟器进行了本方案的仿真,主要评估了可路由节点绑定表和过滤表所消耗内存容量以及端到端的时延、丢包率等指标.

我们首先评估可路由节点绑定表和过滤表所占用的内存比例.绑定表项的字段及长度为〈Index(1B),EPC(0B,暂时未用),IP(8B),MAC(8B),State(1B),Lifetime(2B),Other(0B,暂时未用)〉.因此,每条记录所占用的内存为 20B.过滤表的字段及长度为〈Index(1B),IP(8B)〉,绑定成功的记录同时会生成一条过滤表项.因此,每个 IP 成功绑定生成绑定表及过滤表记录所占用的内存为 29B.在绑定 20 个节点的情况下为 580B.假如可路由节点的内存为 64KB,则所消耗内存的比例为 0.885%.

我们还考察了节点在不进行源地址验证、进行源地址验证、节点移动并进行源地址验证 3 种情况下的端到端的平均时延及丢包率.具体的做法是,采用 SLAAC 地址分配协议,用 50 个节点模拟物联网节点,其中 10 个可路由节点,40 个传感器节点.可路由节点都实现了 TinyRPL 路由协议和 BLIP② 所代表的 6LoWPAN 协议(图 9 为节点架构的示意图),同时还实现了 SLAAC 协议的监听、绑定以及验证的功能.传感器节点不需要 TinyRPL 及地址验证模块.我们用 1 个位置固定的传感器节点模拟互联网 PC 端用于接收数据,用 1 个传感器节点每隔 2s 向该节点发送一个固定报文."PC"节点收到该消息后,会在 TOSSIM 调试窗口显示相关记录.表 3 列出了模拟实验相关参数设置.我们针对 3 种状态、每组 10 个数据包进行实验结果平均的方法,得到如图 10、图 11 所示的平均时延及丢包率对比结果.

表 3 实验模拟参数设置

参数	值
面积	250Grid×250Grid
节点数量	50
可路由节点数量	10
传感器节点数量	40
节点位置	随机
地址分配方式	SLAAC
Tossim 加载插件	Send Radio Packets, Radio Link, Radio Model, Debug Message 等
布局	gridrandom
每次执行时间	20s
数据发送间隔	2s
发送数据包大小	127B
天线范围	Radioscaling=5Grid
移动速率	2.5Grid/s
节点移动路线	随机

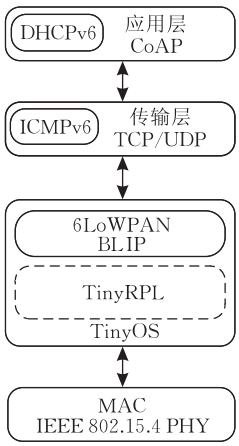


图 9 物联网模拟节点操作系统架构图

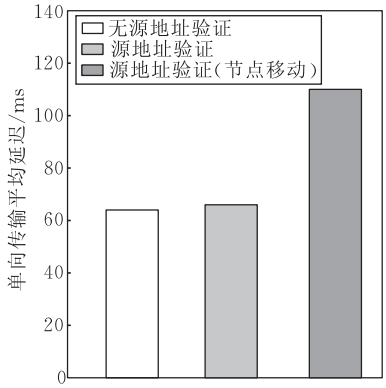


图 10 单向数据传输时的平均传输时延

① UC Berkeley. TOSSIM: A Simulator for TinyOS Networks. http://www.cs.berkeley.edu/~pal/research/tossim.html

② University of California at Berkeley. BLIP. http://smote.cs.Berkeley.edu:8000/tracenv/wiki/blip

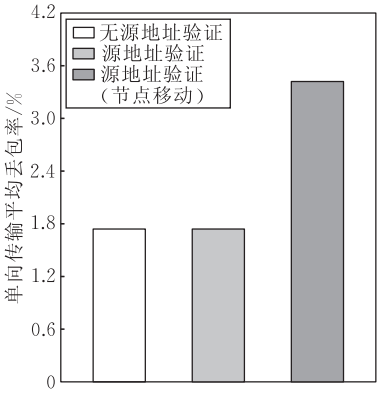


图 11　单向数据传输时的平均丢包率

从图 10、图 11 中我们可以看出，节点在没有移动的情况下，进行源地址验证对节点数据的传输几乎不产生任何影响. 而在节点移动情况下，节点的传输时延及丢包率都会显著增长，分别增长近 60% 和 100%，分析其主要原因应该在于节点移动，造成重新获取地址带来时延所致.

5　结论及进一步的研究工作

物联网是在传感器网络基础上融合了互联网的新一代智能感知网络，也是近年来世界各国大力研究和发展的重点. 目前，研究大多聚焦在物联网的体系结构、路由机理、协议简化以及与互联网互联互通的机制等方面. 物联网的安全问题还未引起大家的重视，特别是物联网节点采用了 IPv6 地址，能够与互联网端系统进行点对点通信之后，物联网节点的 IP 地址真实性有效性就变得尤为重要，否则现有互联网（包括地址欺骗，数据篡改在内）的众多安全问题将会在物联网中继续出现.

本文首先从 IP 地址真实可靠的必要性出发，论述了物联网 IP 源地址验证的重要性. 然后调研了现有互联网源地址验证的已有研究成果，并结合对物联网的基本共识，提出了融合物联网的下一代互联网源地址验证框架，同时根据物联网的特点指出了分布式验证方法优于集中式验证方法的思路，并分别讨论了静态指定、SLAAC、DHCPv6 和 DHCPv6 与 SLAAC 混合四种地址分配情况下的场景交互、过程时序以及状态变迁的细节. 通过在可路由节点上建立自己所覆盖的传感器节点的绑定表和过滤表，建立了分布式源地址验证机制. 最后的模拟实验也证明了该方案的合理性和有效性.

需要指出的是，仍有许多研究工作还有待进一步研究.

（1）地址分配过程的报文交互安全性有待加强

SLAAC，DHCP 地址分配方式本身也存在安全漏洞，比如 IPv6 网络中的 MAC 欺骗、虚假 RA 公告地址前缀等. 因此我们在强调 IP 地址本身有效性的同时，还应关注几种地址分配方式的安全性. 通过 IPSec 及 MD5 消息签名等方法可以强化地址获取过程中交互报文的有效性，但具体的机理和手段还需进一步的研究.

（2）多协议网关翻译机制需要进一步研究

由于物联网节点物理层允许的最大数据长度为 127 字节，地址分配以及重复地址检测过程，必然会涉及到节点数据分片和协议网关数据包重组. 数据包翻译机制会对包括源地址验证在内的所有物联网节点与互联网节点互联互通工作起到推动作用. 因此需要进一步研究.

参　考　文　献

[1] Commission of the European Communities. Internet of Things-An action plan for Europe. 2009

[2] Kushalnagar N, Montenegro G, Schumacher C. IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919, 2007

[3] Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, 2007

[4] Hui J W, Culler D E. Extending IP to low-power, wireless personal area networks. IEEE Internet Computing, 2008, 12(4): 37-45

[5] Garber L. Denial-of-service attacks rip the Internet. IEEE Computer, 2000, 33(4): 12-17

[6] Elliott John. Distributed denial of service attack and the zombie ant effect. IT Professional, 2000, 2: 55-57

[7] Eddy W. Defenses against TCP SYN flooding attacks. The Internet Protocol Journal, 2006, 9(4): 2-16

[8] Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827, 2000

[9] Li J, Mirkovic J, Wang M, Reiher P, Zhang L. SAVE: Source address validity enforcement protocol//Proceedings of the INFOCOM. New York, USA, 2002: 1557-1566

[10] Bremler-Barr A, Levy H. Spoofing prevention method//Proceedings of INFOCOM. Miami, USA, 2005: 536-547

[11] Liu X, Li A, Yang X, Wetherall D. Passport: Secure and adoptable source authentication//Proceedings of the 5th USENIX NSDI. Berkeley, USA, 2008: 365-378

[12] Perrig A, Song D, Yaar A. StackPi: A new defense mechanism against IP spoofing and DDoS attacks. Carnegie Mellon University: Technical Report CMU-CS-02-208, 2003

[13] Lee H, Kwon M, Hasker G, Perrig A. BASE: An incrementally deployable mechanism for viable IP spoofing prevention//Proceedings of the ACM Symposium on Information, Computer, and Communication Security. New York, USA, 2007: 20-31

[14] Moskowitz R, Nikander P. Host identity protocol (HIP) architecture. RFC 4423, 2006

[15] Schridde C, Smith M, Freisleben B. TrueIP: Prevention of IP spoofing attacks using identity-based cryptography//Proceedings of the 2nd International Conference on Security of Information and Networks. Famagusta, Cyprus, 2009: 128-137

[16] Aura T. Cryptographically generated addresses (CGA). RFC 3972, 2005

[17] Andersen D, Balakrishnan H, Feamster N et al. Accountable internet protocol (AIP)//Proceedings of ACM SIGCOMM on Data Communication. Seattle, USA, 2008: 339-350

[18] Jin C, Wang H, Shin K G. Hop-count filtering: An effective defense against spoofed DDOS traffic//Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington, USA, 2003: 30-41

[19] Wu J, Bi J, Li X et al. A source address validation architecture (SAVA) testbed and deployment experience. RFC 5210, 2008

[20] Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks, 2010, 54: 2787-2805

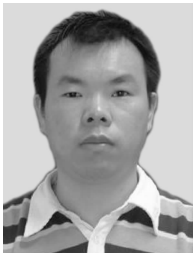
[21] Bi Jun, Liu Bingyang, Wu Jianping et al. Preventing IP source address spoofing: A two-level, state machine-based method. Tsinghua Science and Technology, 2009, 14(4): 413-422

[22] Wu Guangwu, Wu Jian-Ping, Xu Ke et al. SAVT: A practical scheme for source address validation and traceback in campus network//Proceedings of the 20th IEEE ICCCN Conference. Hawaii, USA, 2011: 1-8

[23] Thomson S et al. IPv6 stateless address auto-configuration. RFC 4862, 2007

[24] Droms R et al. Dynamic host configuration protocol for IPv6 (DHCPv6). RFC 3315, 2003

[25] Hinden R et al. IP version 6 addressing architecture. RFC 4291,2006



HU Guang-Wu, born in 1980, Ph.D. candidate. His main research interests include computer network architecture, high performance router, and Internet of Things.

CHEN Wen-Long, born in 1976, Ph. D., lecturer. His main research interest is computer network architecture.

XU Ke, born in 1974, Ph. D., professor, Ph. D. supervisor. His main research interests include architecture of next-generation of Internet, high performance router, P2P and overlay network, Internet of Things.

Background

This work is supported by the National Basic Research Program (973 Program) of China (No. 2009CB320501), the National High Technology Research and Development Program (863 Program) of China (Nos. 2008AA01A323, 2008AA01A326, 2009AA01A334), "Network Protocol, Research and Verification of IPv6-based Wireless Sensor Network" in National Science and Technology Major Project "New Generation Broadband Wireless Mobile Communication Network" (No. 2012ZX03005001-001).

Internet of Things (IoT) is an emerging network form which is developed on the basis of the Wireless Sensor Networks and combines RFID, traditional wire/wireless Internet, mobile communication network and other technologies. Since its application scenario is very extensive, it has become one of the prime research subjects all around the world.

One of hot topics in IoT is how to apply IPv6 technology into its networks and nodes. Once IoT nodes deploy the same IP addresses as that of traditional Internet end-hosts, bilateral correspondence could be achieved among IoT nodes, and between IoT nodes and Internet end-hosts, which can not only resolve the stubborn problem of inter-communication between the end edge networks of IoT and the Internet, but also overcome such intrinsic defects of address-consuming, as well as the lack of IP address management mechanisms.

However, there are dual-semantemes of identity and location on the body of IP address. Thus, once the IP address of IoT node is spoofed, the data collected from nodes will be unreliable. What's worse, this will jeopardize the security of whole system. As research on IoT is still in its beginning stage, this issue has not drawn much attention yet.

Till now, there has not been any study on the subject of source address validation in IoT. Authors have made a lot of fruitful progress on the subject of the architecture of Next-Generation of Internet(NGI) and its source address validation framework. And several papers and Internet standards have been published, one of them is about the SAVA(Source Address Validation Architecture) framework. After fully investigating the relative studies and technologies about IoT, in this article, we propose the scheme of source address validation for NGI which involves IoT on the basis of SAVA.