

一种面向物联网的 M2M 通信解决方案

王 群^{1,2}, 钱焕延¹

(1 南京理工大学 计算机科学与技术学院, 江苏 南京 210094; 2 江苏警官学院 公安科技系, 江苏 南京 210012)

摘 要: 在分析了 M2M 系统体系结构和工作原理的基础上, 利用 NAT 穿越技术在物联网中的应用优势, 提出了一种基于 STUN 和 STUNT 协议的、具有用户身份认证功能的 M2M 通信方案. 经过实验测试, 该方案不需要改变原有网络结构, 只需要在 M2M 设备中嵌入 STUN Client 和 STUNT Client 模块, 就能够实现物联网中不同 M2M 节点之间的通信与管理.

关键词: M2M 系统; 网络地址转换(NAT); NAT 穿越; STUN; STUNT; 通信

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)11-0013-05

A M2M Communication Solution for the Internet of Things

WANG Qun^{1,2}, QIAN Huan-yan¹

(1 School of Computer Science & Technology, Nanjing University of Science and Technology, Nanjing 210094, China;

2 Department of Science & Technology, Jiangsu Police Institute, Nanjing 210012, China)

Abstract: On the basis of analysis of the M2M system architecture and working principle, using the advantages of NAT traversal technology for IoT, this paper proposed a M2M communication solution with user authentication function based on STUN and STUNT agreement. The experiments showed that communication and management between M2M nodes in the IoT could be achieved simply by embedding the STUN Client and the STUNT Client module into M2M devices without changing the original network structure.

Key words: M2M system; network address translation (NAT); NAT traversal; STUN; STUNT; communication

1 引言

被人们期望成为第三次信息产业浪潮和后互联网时代的物联网正在受到业界的普遍关注, 与之相关的技术研究和标准制订工作正在广泛展开. 从广义上讲, 物联网就是一个 M2M 系统, 分别代表机器之间(Machine to Machine)、人机交互(Man to Machine, Machine to Man)和人与人之间(Man to Man)的通信. 由于人与人之间的通信以及人机交互通信方式已经在互联网时代得到了广泛应用, 所以真正能够体现物联网泛在化特点的是机器之间的通信, 为此也将实现机器与机器之间通信的 M2M 系统称为机器类型的通信(Machine Type Communication, MTC)^[1].

物联网涉及现有和演进中的各种组网方式和通信网络类型, 其中以 Internet 为核心网络、以固定和移动 IP 为接入网络、实现 IP 终端互联的全 IP 网络结构是一种最直接、高效的 M2M 通信方式. 然而, 在现有的 IPv4 网络环境中, 当人与人之间的通信受到地址数量限制和网络安全威胁时, 如何将其成功地应用到人与物以及物与物之间的通信就显得极为重要. 本文在充分考虑物联网中 M2M 通信所具有的低功耗、低带宽、小内存等特点的基础上, 对 STUN 和 STUNT 协议的应用进行了有效精简与改进, 充分利用 NAT 穿越技术实现了物联网中 M2M 设备之间以及 M2M 设备与 M2M 应用服务之间的通信, 为目前正在发展中的物联网技术提供了一种有效的 M2M 通信解决方案.

2 M2M 系统的结构及通信特点

2.1 M2M 系统结构

本文中所强调的 M2M 通信是一种以物为主体,不需要人为干涉和与人交互的数据通信方式.根据功能域(Domain)的不同,将 M2M 系统分为设备域、网络域和应用域共 3 个组成部分,系统结构如图 1 所示^[2].

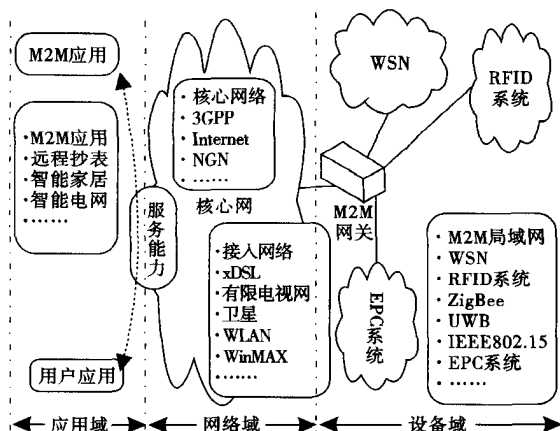


图 1 M2M 系统结构

图 1 中:① 设备域(M2M Device Domain)由 WSN、RFID 系统、ZigBee、IEEE 802.15 等具有不同应用功能的 M2M 局域网组成,每个 M2M 局域网由具有相同或相近功能的 M2M 终端组成,采用通用或特定的协议实现不同 M2M 设备之间的通信. M2M 设备是系统的神经末梢,提供了智能感知和通信功能.感知功能实现对物体自身或周围环境信息的采集,而通信功能负责对采集到的信息的转换和转发.不同的 M2M 局域网通过通用或专用的 M2M 网关接入网络域;② 网络域(Network Domain)实现 M2M 应用与 M2M 局域网之间的数据传输,包括接入网和核心网两部分.接入网通过各类有线或无线接入方式,将 M2M 网关接入核心网.核心网是数据交换的主通道,由现有的电信网、互联网、广电网及演进中的 NGN 等网络组成;③ 应用域(Application Domain)主要完成数据的分析、处理、管理和控制功能,同时根据不同行业的需求提供相应的智能化应用和服务.各类 M2M 应用通过服务能力(Service Capabilities)获得相应的 M2M 设备注册和智能信息服务.

2.2 M2M 通信特点

M2M 局域网、接入网和核心网分别是逻辑上相对独立且具有成熟技术和通信标准的网络,由于

M2M 系统具有边界明晰的功能域划分,所以其通信特点主要反映在不同域的界面处,具体表现在连接设备域与网络域的 M2M 网关处以及连接应用域与网络域的服务能力处.

M2M 网关是一个通信分界点,它既属于网络域的最边缘节点,也属于设备域的最高层节点. M2M 应用可以通过 M2M 网关实现与位于设备域中的原本“看不见”的传感器、RFID 读写器等智能终端之间的交互,反之亦然.在 M2M 分布式系统中,不同域中的数据在 M2M 网关处进行转换,如果是异构系统则需要在 M2M 网关处进行通信协议的映射.

服务能力是界于应用域和网络域之间起着承上启下作用的中间件层,它通过隐藏网络的异构性来简化和优化应用开发与部署,通过开放的接口为不同应用程序提供可共享的 M2M 功能,并充分发挥核心网的功能.

3 基于 STUN 和 STUNT 协议的 NAT 穿越原理

3.1 NAT 穿越原理与 M2M 通信的有机结合

NAT(Network Address Translation,网络地址转换)是 IP 网络在应用过程中为解决地址匮乏并隐藏企业网络内部结构而出现的一项技术^[3],随着 IP 网络应用的迅速扩张,NAT 技术也得到不断完善.将 NAT 功能应用到 M2M 通信是一种最直接、高效的解决方案,尤其当 M2M 局域网是 EPC 系统、WPAN 等直接支持 IP 协议的网络时,可将 NAT 功能直接整合到 M2M 网关中,实现 NAT 与 M2M 系统在体系结构上的融合.当 M2M 局域网为非 IP 网络时,需要将协议转换功能整合到 M2M 网关中.

NAT 将网络逻辑地划分为公网(Public Network)和私网(Private Network)两个应用域,传统的 NAT 环境中位于不同私网中的主机之间无法直接通信,位于公网中的主机也无法直接发起与位于私网中主机之间的通信.为克服传统 NAT 应用中存在的局限性,提出了各种 NAT 穿越技术,主要有 ALG、Middlebox Communication、UPnP、STUN/STUNT、TURN 等.其中,根据 NAT 穿越方式的不同,将 NAT 分为完全锥形(Full Cone)、受限锥形(Restricted Cone)、端口受限锥形(Port Restricted Cone)和对称(Symmetric)共 4 种类型,具体在文献[4-6]中进行了详细的描述.

3.2 STUN 协议

STUN (Simple Traversal of UDP Through Network Address Translators, UDP 在 NAT 上的简单穿越方式) 是 IETF 提出的一个基于 C/S 结构的互联网通信协议^[4]. 利用该协议, 位于私网中的客户端 (STUN Client) 便可以通过位于公网中的服务器 (STUN Server) 获得在 NAT 出口处的公网地址 (IP 地址和端口), 并将该公网地址直接写入到要发送报文净载荷 (payload) 的地址信息中, 这样当报文到达 NAT 出口处时, 只需要对报文头部的 IP 地址进行转换, 并保持与净载荷中地址的一致性. 通过该机制, 便可以实现不同私网中主机之间以及公网主机与私网主机之间的通信.

如图 2 所示, STUN 协议的工作原理为: ① 在所有 STUN Client 客户端已经向 STUN Server 进行了注册的前提下, 含有 STUN Client 的应用程序向 STUN Server 发送一个请求报文; ② STUN Server 在收到该报文后向 STUN Client 返回一个包含 NAT 出口处公网 IP 地址和对应端口号的响应报文, STUN Client 从该响应报文中得到 NAT 出口处的 IP 地址和端口绑定, 并协商确定 NAT 类型, 因为对进入私网的 UDP 数据报的处理方式会根据 NAT 类型的不同而不同. 目前 STUN 只能实现 Cone (包括 Full Cone、Restricted Cone 和 Port Restricted Cone) NAT 穿越, 而不支持 Symmetric NAT 穿越; ③ 根据所获得的 NAT 出口处绑定的 IP 地址和端口以及协商确定的 Cone NAT 类型, 位于不同私网中的 STUN Client 之间便可以进行相互间的通信.

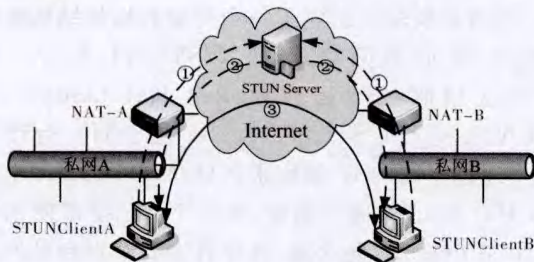


图 2 STUN 协议的工作原理

3.3 STUNT 协议

M2M 系统中大量的通信是由终端发起, 如智能终端定期以 UDP 数据报的方式向应用系统发送收集到的信息或向控制中心发送报警信息, 以及终端之间定期交换报文等, STUN 很好地满足了这一应用需求. 但是, 在一些特殊的情况下, 控制中心需

要穿越 M2M 网关对位于 NAT 后端的终端进行远程管理, 或应用系统需要主动向指定的终端发送请求报文^[1-2], 这时只能处理 UDP 数据报的 STUN 协议就无能为力, 可以采用支持 TCP 报文段的 STUNT 协议来解决这一问题^[7-9].

开发 STUNT (Simple Traversal of UDP through NATs and TCP) 协议的最初目的是让不同架构下的节点之间实现端到端的通信, 而不会因为 NAT 的存在受影响^[9]. 目前, 有关 STUNT 协议的实现方法较多, 应用效果之间也存在一定的差异, 比较典型的是康奈尔大学 NUTSS 项目组提出的一种针对 STUN 的改进协议 STUNT (STUN with TCP)^[10].

如图 3 所示, NUTSS 提出的 STUNT 协议的工作原理为:

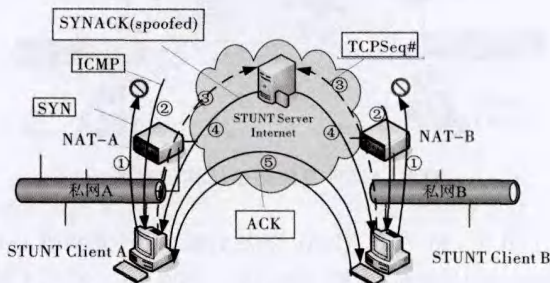


图 3 STUNT 协议的工作原理

① 运行有 STUNT Client 模块的客户端分别发送对 TTL 有严格限制的 SYN 报文:

$$\begin{cases} RA_i \leq TTL_A < RA_{other} \\ RB_i \leq TTL_B < RB_{other} \end{cases}$$

其中, TTL_A 和 TTL_B 分别代表客户端在到达公网前穿越所有 NATs 的 TTL 值, RA_i 和 RB_i 分别代表 SYN 报文分别到达 NAT-A 和 NAT-B 时所经过的路由器数量, 即 SYN 报文在穿越位于最后一个 NAT 的路由器 (从私网进入公网) 时将被丢弃. RA_{other} 和 RB_{other} 分别代表到其他 NAT 所经过的路由器数量, 即离开所在 NAT 后的 SYN 报文不能到达其他的 NAT; ② NAT-A 和 NAT-B 分别返回一个 ICMP 报文, 客户端通过监听经过 RAW-socket 或 PCAP 返回的 ICMP 报文, 从中分别得知 TCP 的初始序号; ③ 客户端分别将各自的 TCP 序号 (TCP Seq #) 发给 STUNT Server; ④ STUNT Server 根据已获得的客户端信息进而通过设置匹配的序号分别构造一个 SYNACK 欺骗报文给各个客户端; ⑤ 客户端之间分别发送 ACK 报文完成三次握手, 之后客户端进入正常的 TCP 传输.

4 基于 STUN 和 STUNT 协议的 M2M 通信方案

4.1 方案设计

如图 4 所示,为了体现本方案的实用性和可扩展性,除 STUN、STUNT 服务器和 M2M 应用服务器需要位于公网外,M2M 终端全部置于 NAT 后端的私网中.M2M 设备具有与互联网节点在结构上一致但应用功能上不同的 IPv4 地址,借助 NAT 穿越方式可实现 M2M 设备之间以及 M2M 设备与应用服务器之间点对点的通信,解决了 M2M 设备的地址分配与管理问题.

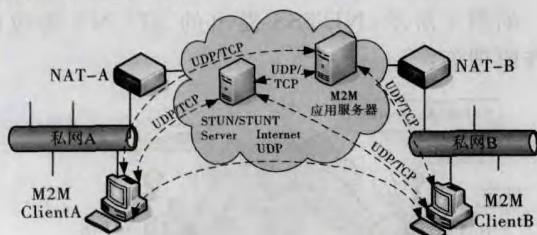


图 4 M2M 系统通信结构示意图

其中,每一个 M2M 设备分配一个全网唯一的 ID(如 64 位或 96 位的 EPC 等),并嵌入一个 STUN/STUNT Client 模块. STUN/STUNT Server 分别负责响应 STUN Client 和 STUNT Client 的请求,并判断 M2M 设备端的 NAT 类型. 集成了用户注册和认证功能的 M2M 应用服务器负责对 M2M 设备 ID 的管理,并记录 M2M 设备的 IP 地址、端口号、NAT 类型等信息. 下面分 3 种情况对主要节点之间的通信方式进行讨论.

(1) M2M 设备向 M2M 应用服务器发起通信

物联网的主要应用是实时采集各智能终端的感知信息,位于私网中的 M2M 设备可以将检测到的数据定期向位于公网中的 M2M 应用服务器发送. 由于通信的发起方是位于 NAT 后端的 M2M 设备, NAT 允许其建立 UDP 和 TCP 连接请求.

(2) M2M 设备之间的通信

M2M 设备之间的通信采用支持 UDP 的 STUN 协议方式. M2M 设备全部位于 NAT 后端的私网中,位于同一私网中的 M2M 设备之间可以利用其私有 IP 地址直接进行通信,而位于不同私网中的 M2M 设备之间通信时需要进行 NAT 穿越. 本方案中,经过改进的位于不同 NAT 后端私网中的 M2M 设备之间通信的建立过程如图 5 所示,该改进方案确保 M2M 设备所获得的是 Cone NAT 类

型,避免了 Symmetric NAT 类型的存在. 另外,为便于 M2M 应用服务器对 M2M 设备的注册和管理并避免频繁地运行 STUN 协议,经注册的 M2M 设备可定期向 M2M 应用服务器发送 keepalive 报文,以确保 M2M 设备在 M2M 应用服务器上注册信息的有效性,或及时更新 M2M 设备的注册信息.

(3) M2M 应用服务器向 M2M 设备发起通信

一般情况下,当 M2M 应用服务器需要对 M2M 设备进行远程控制和管理时可采用支持 TCP 的 STUNT 协议. 当位于公网上的 M2M 应用服务器发起对 NAT 后端私网中 M2M 设备的 TCP 连接时,需要借助于 STUNT 协议. 基于 STUNT 协议的 TCP 连接建立过程类似于图 5,在 M2M 设备已经注册的情况下,M2M 应用服务器首先把通信建立请求发给 STUNT Server,STUNT Server 可以将请求直接转给 M2M 设备,M2M 设备在收到请求报文后将与 M2M 应用服务器建立 TCP 连接,实现从公网到私网的穿越.



图 5 位于不同 NAT 后的 M2M 设备之间通信的建立过程

4.2 方案实现及验证

作者在实验室组建了一个功能和拓扑结构类似于图 4 所示的网络, STUN/STUNT Server 和 M2M 应用服务器运行在 Red Hat Linux9 上, STUN Server 和 STUNT Server 位于同一台计算机上,通过不同的 IP 地址来区分,M2M Client 也用 Red Hat Linux9 进行模拟,两台 NAT 设备使用的是 Cisco PIX 525 防火墙. 其中各主要节点和私网段的地址分配为:

STUN Server:210.1.1.10

STUNT Server:210.1.1.11

M2M 应用服务器:210.1.1.12

私网 A:192.168.1.0/24

NAT-A:210.1.1.13

私网 B:192.168.2.0/24

NAT-B:210.1.1.14

验证方式和结果见表 1。其中,为了加大通信的并发数,实验中在进行从 M2M 设备到 M2M 应用服务器以及 M2M 设备之间的测试时,分别由多个节点同时发送多个连接请求。

表 1 验证方式和结果

验证方式	通信方式	连接次数	成功次数	失败次数	成功率 (%)
M2M 设备到 M2M 应用服务器之间	UDP	200	200	0	100
位于同一私网的 M2M 设备之间	UDP	200	200	0	100
位于不同私网的 M2M 设备之间	UDP	200	198	2	99
M2M 应用服务器到 M2M 设备之间	TCP	200	196	4	98
M2M 设备到 STUN/STUNT Server 之间	TCP	200	200	0	100

实验结果表明:① 从 M2M 设备到 M2M 应用服务器以及从 M2M 设备到 STUN/STUNT Server 通信的成功率都达到 100%,确保了 M2M 设备的成功注册及定时向应用服务器发送数据,完全能够满足对 M2M 设备进行实时信息采集的需求;② 从 M2M 应用服务器到 M2M 设备通信的成功率达到 98%,但因这一方式主要用于对 M2M 设备的远程控制与管理,其通信失败率不会对实际应用产生较大影响;③ 位于不同私网中的 M2M 设备之间通信的成功率达到 99%,能够满足对 M2M 设备进行定位或计算路由时的通信要求;④ M2M 设备的内存和 CPU 占用率较小,满足物联网中对 M2M 设备低功耗、小内存的要求。

5 结束语

现阶段,将 NAT 穿越技术融入 M2M 通信成为适应物联网快速发展的一种可行的通信解决方案。通过本研究,当 M2M 节点与互联网节点具有一致的 IPv4 编址方式后,便可以实现 M2M 节点之间、M2M 节点与互联网节点之间点对点的通信,避免了在 M2M 网关处进行协议转换带来的效率和管理上的不足。通过有效改进 STUN 和 STUNT 协议的工作方式,并将两者在应用中进行结合,将能够实现点对点的通信与控制、兼容多种物理层协议的功能,同时由于 NAT 后端使用的是不受应用限制的私有 IP 地址,丰富的地址资源适合大规模高密度 M2M 节点的部署需要。

参考文献:

- [1] 3GPP. Service requirements for machine-type communications, TS 22.368 V10.0.0 [R]. Sophia Antipolis Valbonne; 3DPP,2010-03.
- [2] ETSI. Machine-to-machine communications, TS 102 690 V1.1.1 [R]. Sophia Antipolis Cedex;ETSI,2011-10.
- [3] Internet Engineering Task Force. RFC 2663. IP network address translator (NAT) terminology and considerations[S]. USA;ISOC,1999-08.
- [4] Internet Engineering Task Force. RFC 3489. STUN-simple traversal of user datagram protocol (UDP) through network address translators (NATs) [S]. USA;ISOC,2003-03.
- [5] Midcom WG,Takeda Y. Symmetric NAT traversal using STUN[EB/OL]. USA;Internet Engineering Task Force[2003-06-15]. <http://tools.ietf.org/id/draft-takeda-symmetric-nat-traversal-00.txt>.
- [6] Yuan Wei,Daisuke Yamada,Suguru Yoshida,et al. A new method for symmetric NAT traversal in UDP and TCP[C]// Proceedings of Asia Pacific Advanced Network 2008. New Zealand; 2008-08.
- [7] Internet Engineering Task Force. RFC 5382. NAT behavioral requirements for TCP [S]. USA; ISOC, 2008-10.
- [8] Jeffrey L Eppinger. TCP connections for P2P apps: a software approach to solving the NAT problem,CMU-ISRI-05-104[R]. Pittsburgh; Carnegie Mellon University,2005-01.
- [9] Saikat Guha,Paul Francis. Characterization and measurement of TCP traversal through NATs and firewalls [C]//Proceedings of the 2005 USENIX Annual Technical Conference. Anaheim;2005-04.
- [10] Saikat Guha,Yutaka Takeda,Paul Francis. NUTSS: a SIP based approach to UDP and TCP network connectivity[C]// Proceedings of SIGCOMM'04Workshops. Portland;2004-08.

作者简介:



王 群 男,(1971—),博士研究生,副教授。研究方向为网络安全管理、物联网。

钱焕延 男,(1950—),博士生导师,教授。研究方向为下一代网络协议与通信模型、计算机网络应用等。