文章编号:1671-4598(2019)10-0171-05 DOI:10.16526/j.cnki.11—4762/tp.2019.10.035 中图分类号:TP393 文献标识码:A

基于软件定义网络的实验室防火墙架构设计

刘 帅
(商丘职业技术学院,河南 商丘 476100)

摘要:针对高校网络实验室安全性较弱的问题,提出了一种基于软件定义网络的防火墙系统建设方案;该防火墙系统采用高性能软硬件系统和相结合的设计思路,以信息处理过程与数据交互过程中的安全防护为研究对象,在高校教师团队与专业技术公司的协同合作下,打造提升校园网络安全性,同时具备教学与科研功能的防火墙系统创新实验平台;在该平台上进行了实验,实验结果表明,开发的防火墙不仅可以抑制因控制器系统的引入而导致的网络攻击,而且能够成功地监控所有网络连接。

关键词:防火墙;软件定义网络;网络安全;创新实验平台

Design of Laboratory Firewall Architecture Based on Software Definition Network

Liu Shuai
(Shangqiu Vocational and Technical College, Shangqiu 476100, China)

Abstract: In order to deal with the problem of weak cyber security in high school laboratory, a software defined networking-based firewall system construction project is proposed. By combining high performance software and hardware systems, the protection for information processing and dada exchanging is investigated. With the help of cooperation between college teacher team and professional technology company, the campus network security is enhanced, and the innovation experiment platform for teaching and research is established. Simulation results on this platform verifies the proposed firewall system can not only suppress the network attack incurred by the control system, but can also monitor all network links.

Keywords: firewalls; software defined networking; cyber security; innovation experiment platform

0 引言

随着国家对“互联网+”思想的大力推广以及互联网技术的广泛应用,在极大地促进高技术公司和科研院所在数字化、信息化领域的研究热潮的同时,也对高校实验室教学工作提出了新的要求[1-2]。在互联网技术中,网络安全[3-4]作为维护互联网系统安全稳定运行的重要保证,已经成为了国内外的研究热点。为了紧跟时代步伐,保证互联网教学质量,全面提升学生的互联网能力,迫切需要建立完善的互联网网络安全教学实验室。

在网络安全技术体系中,防火墙[5]系统用于构造内部网和外部网之间的保护屏障,在硬件和软件相结合的基础上,保护内部网免受非法用户的入侵和网络攻击的破坏。作为网络安全的关键技术,防火墙系统的教学与实验平台需要为学生提供完备的学习与操作功能,从而让学生形成完整的网络安全知识体系,实现“教”与“学”的紧密连接,提高学生解决实际问题的能力。

以防火墙系统为核心的网络安全实验室与以往的教学平台建设相比,由于涉及到安全性这一敏感与重要的问题,因此具有更大的建设难度,需要借助先进的硬件设备、软件平台、安全算法等,针对网络攻击与网络连接的实验问题,从而为学生提供完善的实验环境。防火墙在实际系统中的大量应用使得其平台的建设可以充分利用社会上高科技公司的先进技术,同时在高校教师团队的主导下,建立适应高校教学、实验与科研的综合平台。

为了达到上述目标,提出一种基于软件定义网络(software defined networking, SDN)的防火墙系统设计方案,从而建立可以在控制器端实现的防火墙逻辑。网络安全的发展趋势表明,下一代防火墙在策略执行方面更有活力,并有能力保护内部网络。SDN技术通过集中式防火墙逻辑和分布式防火墙操作,可以实现可疑信息的准确隔离。实验结果表明所提的防火墙建设方案可以大幅度提升网络安全性能,从而证明构建的教学平台具备高网络安全性。

1 防火墙系统架构

在整合学校实验室现有资源的前提下,提出图1所示的高校网络实验室防火墙系统。自下而上,数据服务器群主要用于为实验过程及防火墙工作过程中产生的大量数据集进行存储;实时通信服务器群不仅保证防火墙内外网的实时通信,还能够对通信中的异常情况进行记录和分析;认证系统与网络服务器保证了信息通信功能的高可靠性,并为不同用户的访问提供了安全路径;控制器通过与底层

收稿日期:2019-03-04; **修回日期**:2019-03-23。
基金项目:河南省科技厅软科学研究计划项目(142400411213)。
作者简介:刘 帅(1984-),男,河南商丘人,硕士,讲师,主要从事计算机网络、云计算等方向的研究。

交换机之间的信息交互实现网络状态的实时监控；防火墙监控服务器中的先进算法可以大幅度提高整个校内网络系统的安全性能；贯穿于整个系统的高速宽带通信网络环境实现了数据在系统内的快速流动。

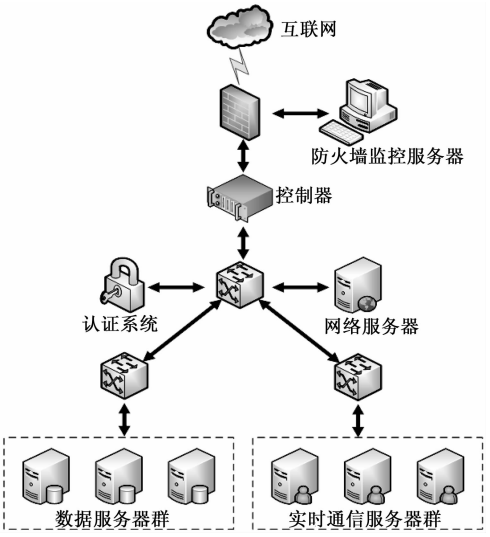

图 1 防火墙系统架构

2 提出的基于 SDN 的防火墙建设方案

2.1 连接跟踪系统

软件定义网络（software defined network，SDN）是一种基于 Open Flow 技术的新型网络架构[6-7]，其通过将网络设备的控制与数据分开，既可以实现网络流量灵活控制，又为应用创新提供了良好的平台。连接跟踪系统柜作为控制器和交换机之间信息交互的核心监控设备，需要借助 SDN 技术实现网络连接状态的高效防护。图 2 为连接跟踪系统的结构图。

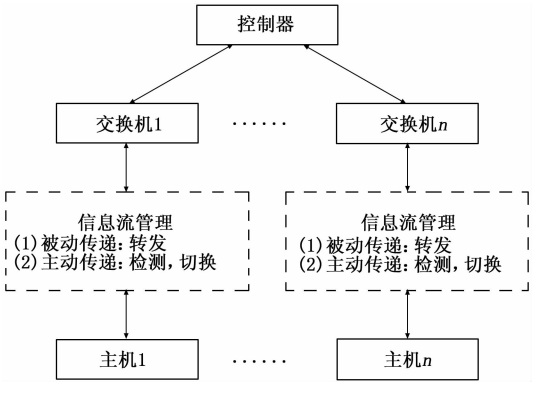

图 2 连接跟踪系统软硬件结构

图 2 说明了跟踪连接系统的三层结构。每一层被定义为具有类似属性和状态的流组条目。第一层由控制器及相应的流程规则组成，并以最高优先级处理数据状态交互；中间层用于检测新的状态连接；最下层用于广义交换机的流量转发规则。进入跟踪连接系统的数据将按照从第一到第三流的顺序进行比较和分析。

连接跟踪系统主要用于跟踪启动和停止两个通信连接状态[8]。对于连接启动跟踪，数据包只有在与任何现有的监控连接不匹配时才被转发给控制器，连接跟踪系统只需确保首个发起连接的数据包被报告即可。对于连接终止跟踪，使用不同的方法来处理 TCP 和 UDP 连接：在 UDP 连接中，使用超时参数来检测流量，因此不存在 UDP 的连接跟踪开销；在 TCP 连接中，交换机必须连续发送数据包到控制器以检查 TCP FIN 标记，此时存在通信开销。

连接跟踪系统由专业技术公司设计并提供，将其输出的数据包头进行比较，如果不匹配，数据包被分类为新的连接发起数据包。对于 TCP 协议，连接跟踪系统通过检测 FIN 标志来判断连接是否终止，同时将数据包发送到目的地；对于 UDP 协议，没有明确的标志来检测连接拆除，因此需要在流条目中会设置好截至时间，在特定的时间之后，如果没有 UDP 分组被发送，则数据流将被移除并且结束连接。

为了提高 SDN 解决方案的效率，设计了基于拓扑数据的交换机流量表简化方法：通过在每台交换机上选择性地安装控制流入口，可以达到简化防火墙的设置，实现连接交换机的快速检查[9]。

为了实现连接跟踪系统三层架构的可靠信息交互，提出了一种新型的入站流量高效分类方法：通过将反应流和主动流进行混合使用，可以预先将重要的防火墙控制流部署到相应的交换机中，从而保证在连接检测之后，跟踪连接得到稳定保持且不会有任何额外的延迟。

2.2 防火墙构建的软件实现

防火墙构建过程包括通过编程实现一些特定的防火墙配置功能。运行于防火墙监控服务器上，如图 3 所示。

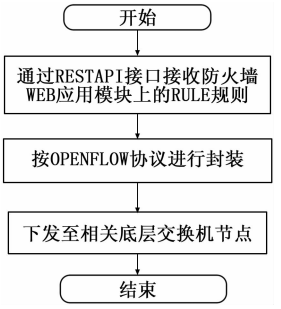

图 3 防火墙构建的软件实现流程

1）通过 REST API 接口接收防火墙 WEB 应用模块上系统管理员下发的 RULE 规则。

2）将流匹配规则以底层 OPENFLOW 软交换机能够理解的流表形式按 OPENFLOW 协议进行封装。

3）通过安全通道将上述包含新流表信息的控制信息下发至相关底层交换机节点。

采用在 GITHUB 上获取最新的 RYU 的源码，在 UBUNTU 4.15.1－13 环境下进行二次开发和实验。

源码结构如图 4 所示。

其中 CMD 目录下的代码是 RYU 框架的入口程序，它

```
xl@ubuntu:~/ryu/ryu$ ls
app     cmd          exception.py  hooks.py     log.py    tests
base    contrib      flags.py      __init__.py  ofproto   topology
cfg.py  controller   gui           lib          services  utils.py
xl@ubuntu:~/ryu/ryu$
```

图 4　源码结构图

会调用 RYU 核心组件的初始化程序，而组件的初始化是在 BASE 目录下进行的，TOPOLOGY 目录是有关拓扑的组件，控制也作为一个组件存在于 CONTROLLER 目录中。

2.3　DoS 攻击的检测

拒绝服务（denial of service，DoS）攻击通过瘫痪计算机或网络提供的正常服务来达到入侵损害系统的目的，是防火墙系统中需要重点防护的攻击形式[10-11]。为了减轻控制器 DoS 的损害，提出一种优先级分类与维护的多消息队列检测方法：实时监视每个特定主机正在进行的连接的峰值数目，同时借助以前时间段的累计峰值历史记录，估算每个主机的峰值连接；如果来自主机的连接请求的数量超过了某个预定义值，那么它将被识别为攻击者，其请求将被放入优先级较低的“警告队列”中，并在处理完“正常队列”中的所有请求后在对其进行处理[12]。

DoS 攻击的消息队列处理过程如图 5 所示。通信网络中由 MAC 地址标识的主机可以根据其行为分配一个队列线程。MAC 地址散列使防火墙能够对来自不同主机的入站数据进行分类，这样可令控制器在不需要逐个检查数据包的情况下立即丢弃恶意数据包。具有不同优先级的消息队列确保优先处理来自没有攻击历史的主机的合法请求，来自可疑主机的具有被攻击历史或当前正在增加连接数量的可疑主机的请求仅在普通队列完全为空之后才被处理。如果没有优先级队列机制，等待上线的合法数据包就会因为有许多恶意数据包填满了队列而被丢弃。

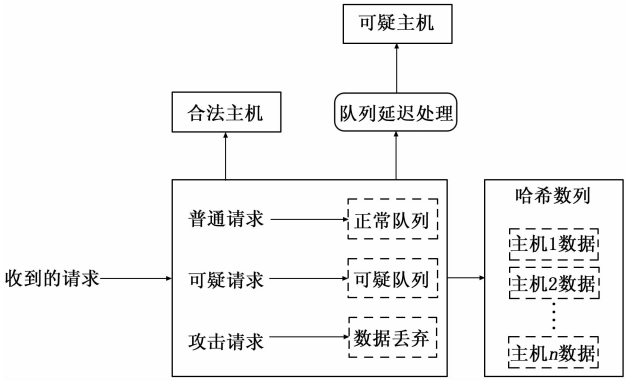

图 5　DoS 攻击的防火墙处理方法

2.4　防火墙状态线程

设计的防火墙状态线程包括：状态防火墙系统，REST API 服务系统，包过滤系统，二次转发系统，DoS 缓解系统。

1）状态防火墙系统：通过控制层来获取网络的状态信息，可用于状态的跟踪和监测。例如，当底层交换机收到的数据包中含有恶意数据，或者网络中的链路失效时，该系统能及时检测网络的状态，通过调整对当前网络检测查询频率，利用控制器发出一系列包过滤规则以确保网络安全。

2）REST API 服务系统：该系统处在控制层中，其功能是实现控制层与应用层的连接，实现与状态防火墙模块的通信交互。REST API 服务系统包含许多可编程接口，它们遵循 HTTP 系列的协议规定。

3）包过滤系统：规定了关于数据包的一系列过滤操作规则，对接收到的数据包执行通过或者舍弃决策。包头中有源和目标的 IP 地址、源和目标的 MAC 地址以及通信协议号等信息，设置过滤规则的主要目的是为了匹配包头中的参数信息。

4）二次转发系统：该与数据转发层中的信息交互，将有关数据包的信息转发到数据转发层中。它可以统计数据转发层中的流表项等信息，并将该信息发送至控制器。

5）DoS 缓解系统：用于识别网络攻击，并激活 DoS 检测与损害缓解功能。

3　平台建设与实验测试

3.1　防火墙系统平台建设

同各国充分整合学校实验室现有的硬件资源，建立基于校内云存储、控制器阵列和高速通信网络的防火墙系统。

云存储系统如图 6 所示。云存储服务器选用 10 台 WD/西部数据 My Cloud Pro PR4100 32TB，如图 7 所示。并与校内现有的分散计算与存储服务器进行整合，其功能包括：支持硬盘寄送，海量数据快速上传；基于 CIFS 协议配合存储网关，像读写本地数据存储磁盘；支持 Bucket 镜像，第三方数据无缝迁移；支持多用户访问控制、STS 临时授权；支持 HTTPS 加密传输和加密存储。

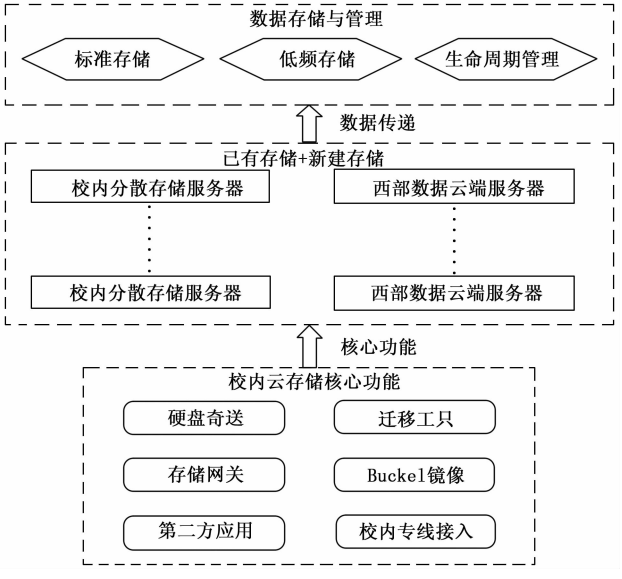

图 6　云存储系统

控制器阵列（连接跟踪系统）由专业公司设计研发，主要由 Intel/英特尔 8 核 CPU 处理器及其外部电路组成，用于控制防火墙系统运行过程中的数据交换过程，并对工

图 7 WD/西部数据 My Cloud Pro PR4100 32TB

程中产生的网络攻击、异常数据注入等问题进行实时监控，从而实现基于软件定义网络的防火墙核心安全防护。

高速通信网络由实验室网络升级改造而来。实验室现原有网络为典型的环形网，采用以太网接口设备及通信线缆，传输速度仅为 1 Gbit/s，不仅不利于数据的快速传递，也会产生通信延时并降低防火墙安全防护处理的功能。通过将实验室现有网络改造为星形网，并采用光纤通信技术，使得数据通信速度提升至 10 Gbit/s，不仅保障了数据的高速传输，而且降低了功耗，加大了通信距离。此外，借助交换机将实验室通信网络与校园高速宽带网络进行连接，可以实现数据在实验室和校园内的快速共享。

3.2 DoS 攻击缓解实验

DoS 攻击是一种非常常见的网络攻击，为了验证实验室建设的防火墙系统对于网络攻击的坚强性，并为学生进行相关实验做好准备，本文给出了实验室防火墙系统的实验结果与分析。

第一步：模拟 DoS 攻击。在正常情况下，主机每个时隙的请求数量在所有时隙都是静态的，通过突然增加和减少攻击者的时隙请求数量，用来以模拟 TCP SYN 洪泛攻击。攻击是以脉冲模式进行的，重复 10 个正常时隙，然后是 10 个攻击时隙，Singe 攻击波时长为 5 个时隙，数据包到达率为 10000packets/s，这种攻击模式如图 8 所示，这个实验的参数在表 3 中列出。

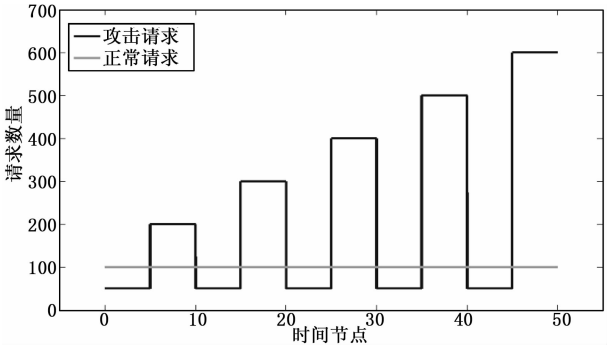

图 8 攻击模式

第二部：实验与分析。连接跟踪的 DoS 缓解功能利用多个具有不同优先级的哈希队列来快速丢弃恶意包，并减少合法用户的处理延迟。为了测试这个功能，本文将运行多个散列消息队列的连接跟踪与单个消息队列进行比较。缓解时间被定义为从检测到 DoS 到控制器队列中所有恶意数据包被丢弃的时间。记录所有攻击波的缓解时间。

对于多个哈希队列，连接跟踪只需在正常和警告列表中检查攻击者的 MAC 地址对应的队列，并将其全部删除即可。当使用单个队列时，连接跟踪必须检查每个单独的数据包以匹配攻击者信息。这些不需要的请求在队列中出现的时间越长，控制器占用的内存资源越多。此外，这些恶意数据包的数量过多会对合法数据包产生负面影响，如额外的延迟以及由于溢出队列而导致丢弃的机会增加。如图 8 所示，使用多个哈希队列的缓解时间范围仅为 0.3～0.85 毫秒。对于单个队列来说，缓解时间是使用多个哈希队列缓解时间的 10～25 倍，使用多个哈希队列比使用单个消息队列更能有效缓解 DoS 攻击。

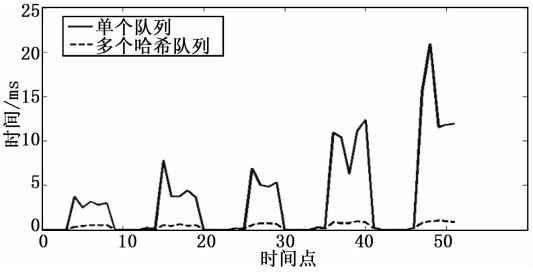

图 9 缓解时间对比

图 9 为在发生 DoS 攻击的情况下，不同优先级队列对处理合法请求的影响。整个处理时间为来自正常主机请求的总处理时间，总处理时间标志着连接跟踪在每个时隙处理来自普通主机的所有请求的持续时间。从图 10 中可以看出，使用单个队列的普通用户的处理时间大部分是稳定的，只是随着请求总数的增加而略微增加。可以注意到，传入的数据包以块形式到达，并且来自一个主机的所有请求数据包同时来到，随后是其他主机的数据包。这与本文推测两个主机之间数据包的混合到达不同，这是因为数据包在产生以及链路传输方面有延迟，单个队列的连接跟踪本身将处理从一个主机到另一个主机的所有请求。

相反，使用循环队列查找的多个哈希队列允许连接跟踪依次处理来自两个主机的请求。因此，在没有攻击的时隙内正常用户的处理时间是单个队列的两倍。另外，从攻击期的第二时隙到冷却期的第一时隙为重复模式。普通用户的处理持续时间大大减少，与单个队列的持续时间相匹配。在第二个攻击时隙（6，16，26，36，46）期间，攻击者在第一个攻击时隙被识别并标记为可疑主机，并且所有来自攻击者的请求包被放入警告队列。因此，正常队列中的普通主机的请求首先被处理，这导致处理持续时间减半。另一方面，在正常时间的第一个时隙（11，21，31，41），由于攻击者主机仍然有可疑的信誉，请求的数据包仍然具有较低的优先级，所以正常请求的处理持续时间不会被接收。在下一个时隙中，攻击者信誉由于没有违规而在下一

个时隙正常重置，因此处理持续时间随着分组查找而加倍。由以上分析可以得出结论，连接跟踪能够降低违反主机的处理优先级，以减少合法请求的延迟和丢弃概率。

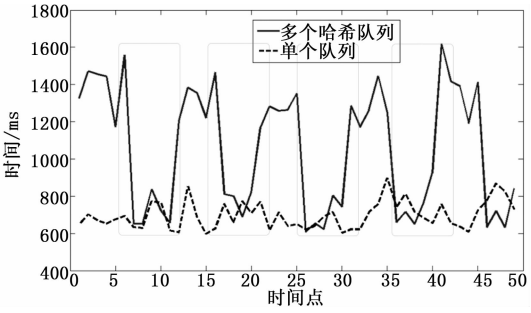

图 10　正常主机的处理时间

4　结语

在网络信息安全知识体系中，防火墙实验室系统的建设有利于培养学生系统的网络安全知识，激发学习热情和动手能力，提升软硬件使用能力。通过整合校内已有的计算资源，同时充分利用校企联合研发模式，建立了基于分散式云存储、控制器阵列和高速通信网络的集成化防火墙系统，解决了现有系统计算资源不足，通信控制性能较弱，数据传输速度较慢的问题。此外，提出了极有软件定义网络的新型防火墙安全防防护技术，通过实验分析了所提技术的优越性，该技术可以大幅度提高校内网络安全实验室的科研水平，在保障学生完成高质量实验的同时，也可以微笑内的教师和科研团队的进一步创新提供保证。

参考文献：

[1] 李　薇，杨庆华，赵玉萍. 基于物联网技术的智慧实验室近远程测控系统 [J]. 计算机测量与控制，2018，26 (11)：58－63，68.

[2] 孙会儒. 计算机硬件虚拟仿真实验教学系统设计 [J]. 微型电脑应用，2018，34 (4)：59－62.

[3] 韩　帅，矫文成. 基于信誉系统对 GRID 网格 Leader 选择协议的安全性研究 [J]. 计算机测量与控制，2018，26 (08)：249－252，257.

[4] 孙卫喜. SVM－PSO 在网络安全态势预测中的应用研究 [J]. 信息技术，2019 (2)：58－61.

[5] 孟祥成. 基于 eNSP 的防火墙仿真实验 [J]. 实验室研究与探索，2016 (4)：95－99.

[6] 毛健彪，卞洪飞，韩　彪，等. PiBuffer：面向数据中心的 OpenFlow 流缓存管理模型 [J]. 计算机学报，2016 (6)：1092－1104.

[7] Akyildiz I F，Lee A，Wang P，et al. A roadmap for traffic engineering in SDN－OpenFlow networks [J]. Computer Networks the International Journal of Computer & Telecommunications Networking，2014 (3)：1－30.

[8] Khattak Z K，Awais M，Iqbal A. Performance evaluation of OpenDaylight SDN controller [A]. IEEE International Conference on Parallel and Distributed Systems [C]. 2014：671－676.

[9] Trois C，Fabro M D D，Bona L C E D，et al. A Survey on SDN Programming Languages：Toward a Taxonomy [J]. IEEE Communications Surveys & Tutorials，2016，18 (4)：2687－2712.

[10] Gunasekaran M，Periakaruppan S. A hybrid protection approaches for denial of service (DoS) attacks in wireless sensor networks [J]. International Journal of Electronics，2017，104 (6)：993－1007.

[11] Ahmed M. Thwarting DoS Attacks：A Framework for Detection based on Collective Anomalies and Clustering [J]. Computer，2017，50 (9)：76－82.

[12] 吴志军，张景安，岳　猛，等. 基于联合特征的 LDoS 攻击检测方法 [J]. 通信学报，2017，38 (5)：19－30.

(上接第 166 页)

参考文献：

[1] 季晨雪，胡圣波. 3D 打印机的定位模糊控制 [J]. 贵州师范大学学报 (自然科学版)，2017 (1)：81－86.

[2] 彭宇林，覃贵礼，安轲，等. 基于 LV8731V 的步进电机细分驱动器设计 [J]. 通信电源技术，2018，(35) 01：3－5.

[3] 高伟康. 基于单片机的两相步进电机细分控制 [J]. 黑龙江科技信息，2017 (3)：59.

[4] 唐　立. 步进电机细分驱动系统设计 [J]. 机电信息，2017 (27)：90－91.

[5] 孙　星，吴　杏. 基于单片机的步进电机细分驱动系统设计 [J]. 山东工业技术，2017 (6)：157－158.

[6] 贾伟强，王德兴，李　静. 基于单片机的步进电机细分控制系统 [J]. 电脑开发与应用. 2010 (3)：69－71.

[7] 周永明，许进亮，李向阳，等. 基于 DSP 的两相步进电机细分驱动器设计 [J]. 电力电子，2017 (4)：87－89.

[8] Erdman J M，Kerkman R J，Schlegel D W，et al. Effect of PWM inverters on AC motor bearing currents and shaft voltages [J]. IEEE Transactions on Industry Applications，1996，32 (2)：250－259.

[9] 袁　帅，甘　靖. 基于 FPGA 的步进电机细分驱动技术研究 [J]. 湖南理工学院学报 (自然科学版)，2010 (1)：62－64.

[10] 时念科，吴美莲. 脉宽调制 _ PWM _ 实现步进电机的细分驱动技术 [J]. 硅谷，2011 (17)：39.

[11] 刘成淦，王　直. 基于 STM32 的一种步进电机系统的设计 [J]. 电子设计工程，2018 (1)：131－134.

[12] 张爱良，朱旭东，范　雪. 基于 STM8S 微控制器步进驱动器的设计 [J]. 电子设计工程，2018，(26) 01：180－183.

[13] 陈永军，刘　湃，基于微控制器的汽车空调步进电机控制系统设计与实现 [J]. 仪器仪表与分析监测，2017 (2)：1－6.

[14] 付家翰. 基于单片机的高精度步进电机控制研究 [J]. 中国新通信，2017 (5)：150.

[15] 曹丽娟，基于 STC89C51 单片机的脉冲喷吹控制仪设计 [J]. 自动化技术与应用，2017，(36) 01：104－107.

[16] THB6128 Development Specification Proposal，SANYO，stepping Motor Driver，Data Sheet [Z].

[17] 晋兆琼，夏超英，张　建. 基于单片机的步进电机细分驱动的实现 [J]. 电气自动化，2000，6 (01)：8－13.