摘 要

由于信息化网络流量的增多和网络需求的多样化，软件定义网络（SDN）体系架构逐渐成为研究热点，采用 OpenFlow 协议将转发和控制分离，通过控制器实现对网络的集中控制。在大规模网络中采用多控制器架构增强网络的灵活性和可靠性，然而动态流量不断变化引发控制器间的负载失衡。若在通信过程中需要生成新的流表项，则交换机会向控制器发送 Packet-In 请求，攻击者往往会利用这种机制发起分布式拒绝服务（DDoS）攻击，使控制平面容易引发安全问题，造成控制器过载甚至导致网络系统瘫痪。同时，对 DDoS 攻击引发的过载进行负载均衡会出现安全问题。因此，本文针对 SDN 多控制器架构下的负载失衡以及引发的安全问题进行研究，主要内容如下：

首先，针对 SDN 多控制器架构容易出现控制器负载不均衡和如何预防 SDN 成为 DDoS 攻击受害者的问题，本文设计一种负载均衡的三层框架，使控制器资源分配合理，在一定程度上增加了 DDoS 攻击成本。在该框架基础上，设计了多个模块以实现整个控制平面的负载均衡。控制器负载状态判定模块根据动态阈值方法设定控制器负载状态标志位，对整个控制器集群的负载进行管控。迁移交换机选择模块通过待迁移交换机的优先权决定迁移哪些交换机。主控制器重选模块采用改进多目标优化的遗传算法（GAIMO），并以控制器集群的负载均衡度、平均时延和交换机迁移成本作为效用函数来求解纳什均衡的最优部署。通过实验表明该算法整体上降低了控制平面的负载均衡度，有效地优化了多控制器中的网络性能。

其次，为了避免由于遭受攻击而导致控制平面频繁进行负载均衡，本文设计了一个基于 SDN 多控制器的 DDoS 攻击防御机制。SDN 架构对于 DDoS 攻击具有脆弱性，通过 SDN 的优势来抵御 DDoS 攻击是当前研究的热点。本文设计并实现了数据采集模块，对流表信息进行收集提取；数据处理模块通过提取的三元组特征来对网络流量进行分类；流量拦截模块采取溯源的方式及时对恶意流量进行识别并拦截。通过实验验证了 SDN 多控制器安全防御机制的可行性和可靠性，并有效地保证了多控制器网络的安全。

关键词：软件定义网络；网络安全；负载均衡；遗传算法；分布式拒绝服务攻击；多控制器部署

目 录

第一章 绪论

本章首先阐述了 SDN 架构存在的网络安全问题，说明了本文选题的研究意义。随后介绍了国内外对 SDN 多控制器网络架构下的安全机制和负载均衡的研究，最后阐述了主要研究内容和结构安排。

1.1 研究背景及意义

1.1.1 当前网络存在的问题

传统网络架构存在可扩展性差、管控难度大、运维成本高和网络资源利用率低等问题。因此，针对上述存在的网络问题，开展对新型软件定义网络（Software Defined Network，SDN）架构[1]的研究。通过将控制平面与数据平面分离，能够更方便地控制网络流量，实现网络便捷的配置管理。尽管如此，SDN 网络面临着新的问题，其解决方案与以往的传统架构不同。因此，在 SDN 中保证网络安全已成为当前研究的热点。

传统的 SDN 中小型网络采用单一控制器架构，由于资源和处理能力有限，难以及时地处理大量流量的请求，存在可扩展性和单点故障等问题。在大规模的网络环境中，随着转发设备和终端的增加，控制平面演变为多控制器协作的分布式架构，控制器共享相同的全局视图。在多控制器的架构下，由于网络不断通信，控制平面中不同控制器之间的负载存在一定的差异，当网络攻击导致流量负载急剧变化时，控制平面容易出现安全问题，负载过高的控制器更容易受到网络攻击。常见的分布式拒绝服务攻击[2]（Distributed Denial of Service，DDoS）就很可能通过攻击其中的一个或多个特定的过载控制器来破坏网络，在短时间内使用大量合法的分布式服务器向目标网络设备发送大量请求，数据转发层使用合理的请求使控制平面资源过载，导致控制器不可用，从而使合法用户无法获得服务。因此，特别是对于大型网络，必须要有一个稳定强大的 SDN 控制平面。

1.1.2 研究的目的和意义

SDN 系统架构通过控制器的集中控制实现对网络高效地配置和管理。然而，由于网络规模和流量规模的动态变化，根据交换机与控制器之间的交互过程，当网络中有新的流量到达时，若流表中无匹配的流表项，则会向控制器发送数据包请求路由信息，由于网络中流量容易在短时间内增多，控制器间可能会出现负载失衡现象，从而导致网络无法正常运行，网络服务得不到响应[3]。因此，

研究 SDN 多控制器间的负载均衡对保证网络服务质量来说十分重要。

控制器间的负载失衡情况主要是由不断增加的网络流量引发的，负载较高的控制器不仅在大量请求数据包到来之后不能及时处理，还可能由此遭受恶意的网络攻击，影响正常请求的设备间通信，而对于负载较低的控制器，其处理资源完全被浪费了。除此之外，负载失衡的情况还降低了 SDN 多控制器架构的安全性[4]。攻击者很容易在短时间内向网络设备发起异常流量攻击，使其中的某一台或几台控制器在短时间内迅速过载，骨干控制器容易遭受安全威胁甚至直接引发控制平面的级联故障。因此，提高 SDN 多控制器网络控制平面的安全性具有重要意义。

针对上述问题，本文对 SDN 多控制器负载均衡算法展开研究，采用动态交换机迁移[5]的方式，通过角色修改来调整交换机和控制器之间的匹配关系，核心思想是实现负载的转移，选择负载较高控制器下所管控的交换机，将其迁移到负载较低的控制器上，以此来维持控制平面的负载均衡，使控制平面的整体资源利用率得到提升，也能在一定程度上减少 DDoS 攻击的发生，从而保证整体 SDN 控制平面的安全。此外，本文对 SDN 安全防御机制展开研究，通过及时发现控制平面攻击的发生并进行拦截，来保证网络的正常通信，这对提升整个 SDN 网络架构的安全性具有重要作用。

1.2 国内外研究现状

1.2.1 SDN 控制平面安全机制研究现状

控制平面是整个多控制器网络的“大脑”，负责网络策略决策，而数据转发层通过获取的转发策略完成数据包的发送，控制平面与数据平面在整个网络中占据重要地位。SDN 的控制平面与数据平面的解耦特性又为攻击引入了新的方向，SDN 自身以及 OpenFlow 协议面临着新的安全问题[6]。在实际的 SDN 的多控制器分布式架构中，随着网络流量的不断到来，骨干控制器上的流量请求较多使负载加重，而其余的一些控制器上没有明显变化。因此，这就容易导致控制器间的流量差异较大，攻击者在识别出骨干控制器后发起流量淹没等恶意攻击，给网络的安全造成威胁。SDN 的安全策略[7]通过可编程设备上的应用程序，在网络入口的交换机上进行强制安全检查，为提高 SDN 多控制器的网络安全性，在检测到恶意攻击者之后，及时对数据包进行阻断。文献[8][9][10]详细分析了三层 SDN 网络架构中存在的安全问题，把 OpenFlow 协议中各个组成部分作为研究对象，分析在 SDN 网络架构中各个组成部分容易出现的新型安全问题，对网络中容易引发的攻击类型对了介绍，并详细阐述了其攻击原理及研究现状。Shin 等人[11]提出了一种 CloudWatcher 安全架构，由控制器捕获网络中到达的数据包，

安全架构下添加了安全模块，将数据包直接转发到控制器外部部署的一些入侵检测系统的安全设备上。

在 SDN 网络通信过程中会产生很多数据包，往往也会有恶意流量借此来向网络发动攻击，威胁 SDN 网络的安全。由于控制平面具有逻辑控制中心化的特点，容易引发控制器单点失效问题，而 DDoS 攻击[12]很擅长这样的攻击。在 SDN 网络中，DoS/DDoS 攻击是较为常见的且较为危险的一种网络攻击方式。分析 OpenFlow 交换机中的流行为和流量统计信息可以识别网络中 DoS/DDoS 攻击的发生。Jia 等人[13]提出了一种基于自组织映射的轻量级 DDoS 攻击检测方法。通过流量收集、特征提取和分类器模块识别恶意流量，将神经网络中的 N 维数据映射成二维图进行拓扑排序，收集统计特征相似的数据进行分类，从而区分网络中的合法和非法流量。Dong 等人[14]提出了一种改进的 K 近邻算法对 DDoS 攻击进行检测，并加入了 DDoS 攻击度的概念，该方法具有较高的攻击流识别率。Kalkan 等人[15]采用一种基于统计的 DDoS 攻击防御机制，主要包括名义、准备和主动三个阶段。名义和准备阶段采集、分析和处理数据，而主动阶段通过前两个获取到的数据进行决策判定，并检测网络中是否存在 DDoS 攻击。由于 DDoS 攻击源的隐蔽性不易被检测的特性，Liu 等人[16]主要针对数据层的 DDoS 攻击提出了一种基于因子分解机的多属性 DDoS 识别算法，并达到了很高的 DDoS 攻击检测总体精度。针对 SDN 多控制器网络架构上的 DDoS 攻击[17]，常见的检测方法就是在短时间内检测 Packet-In 消息，将超过一定阈值的流量认定为网络中存在 DDoS 攻击流，但是阈值的选取可能会影响最终的检测结果。需要通过更多的流表特征来分类流量，对 SDN 控制平面的安全机制展开进一步的研究。

1.2.2 多控制器负载均衡技术研究现状

以前的多控制器架构一般采取静态部署[18]方式，由于网络通信中的流量是不断动态变化的，多控制器域间的负载失衡问题越来越突出，往往通过改变控制器的部署位置和策略来均衡控制器集群间的负载，或者采用交换机迁移改变控制器与交换机之间的动态映射机制，以此来提高 SDN 控制平面的可靠性。基于交换机迁移的思想，Dixit 等人[19]采用动态部署的方式，并提出弹性分布式的控制器架构，当某个控制器的负载超过阈值时，采取交换机就近迁移方案来实现负载的转移，但如果就近控制器濒临过载，迁移后直接到其负载过重，算法不能很好地发挥降载作用。如果最近邻控制器的负载较重时，易导致迁移震荡的发生。Huang 等人[20]提出了基于聚类的遗传算法与合作集群方法，采用针对所有控制器上的请求分配概率的调度算法，但没有在指标权重分配上进行细致描述。Adekoya 等人[21]建立了一种负载均衡迁移模型，对迁移交换机的流量设

置了容量限制，以防止在迁移之后，重选的主控制器会发生过载，但需要进一步实验来验证其算法的有效性。

目前，对于控制器状态划分的研究，Lan 等人[22]提出预先定义的负载权重动态自适应的负载均衡策略，给每一台控制器一个权重系数，在很大程度上提高了控制器的整体资源利用率。Mokhtar 等人[23]提出一种多阈值负载均衡切换迁移方案，采用了传输负载信息的指示器来渐进动态地调整负载阈值，但指示器会增加负载均衡的计算成本且影响网络响应的实时性。目前对待迁移交换机的选择，Sahoo 等人[24]设计了最小化控制器集群负载差异的优化算法来实现负载均衡，算法在优化效果上较好地均衡了控制器间负载，但没有考虑到它们之间容量的区别，负载容量小的很容易过载，导致出现错误的交换机迁移。Xiao 等人[25]提出了一种 SDN 交换机迁移决策方案，通过迁移效益模型在迁出域集合中选出迁移交换机，将负载均衡率和传输时延作为衡量的指标，但是没有考虑到网络拥塞时的排队时延。

对于重新选取主控制器的问题，Ibrahim 等人[26]通过遗传算法（GA）来部署控制器，以最小化时延和控制器集群的负载差异为优化目标，算法的收敛速度快，能很快找到部署策略，但算法中的采用的选择算子使得出的策略并不是十分合理。Yuan 等人[27]提出一种基于 SDN 多控制器部署方案的遗传算法（GAPA）来解决多控制器部署问题，针对平均传播延迟进行寻最优值，从而获得部署策略结果，该方法在实现整个控制平面负载均衡方面具有良好的性能。但采用固定概率的交叉和变异算子会导致错失最优部署方案，在寻优方面的效果不佳。Mohanty 等人[28]采用一种有效的基于遗传算法的控制器布局求解方法（Proposed GA），以传播延迟和部署成本最小化为目标，找到控制器和交换机的最优布局映射方式，按照部署策略对交换机进行迁移，最终实现整个控制平面的负载均衡，但该算法的收敛速度慢，难以高效找到最优的映射矩阵，导致最终的部署时间较长。

针对重选主控制器问题，目前负载均衡对于整体网络中的综合优化研究尚不充足，对于很多因素都没有考虑在内，易导致主控制器的重新选取僵化。Schütz等人[29]提出了控制器部署的全面数学形式化来保持控制器集群的负载分布分均，以传播延迟最小化作为目标函数从而获得部署方案，没有考虑到发送和处理时延。Ibrahim等人[30]采用贪婪随机搜索（GRS）算法来完成网络中交换机与控制器间的动态映射，还针对网络情况可以重新分配控制器的位置、数量，来达到最大的资源利用率，最终实现控制平面负载平衡，提高了网络的可靠性和成本效益。为实现控制器与交换机的重新部署，杜众等人[31]提出在负载不同情况下分别采取交换机共享调度池算法（SPSS）和代价优先缓慢均衡算法

（CFSS）来调节各控制器的负载情况。当控制器负载较高时，通过SPSS算法建立共享调度池存放由它管控的交换机，其余轻载控制器从中可取走交换机，从而实现控制器负载从重到轻的转移。而当负载并非很高时，采用CFSS算法来决定是否进行迁移，评估交换机迁移的开销成本，满足迁移条件后再执行交换机迁移操作。陈飞宇等人[32]提出一种单目标免疫粒子群算法来动态迁移交换机，将通信开销最小的迁移策略解作为最终的部署方案。刘必果等人[33]将负载均衡度和通信开销作为优化目标进行控制平面负载均衡，采用多目标优化的NSGA-Ⅱ算法进行求解，但未考虑时延因素。Zhong等人[34]在判定控制器状态时采用了过载状态预测，并提出了一种收益评估的多控制器负载均衡策略，负载均衡程度有了明显的下降，但未考虑到时延等网络性能的优化。Zhou等人[35]通过动态自适应负载均衡算法（DALB）来调节控制器集群负载，在控制器内设计负载衡量模块、收集模块和决策制定模块，以此来减轻过载控制器的负担。通过优先迁出负载最重的交换机并迁入到负载最轻的控制器上，并以此均衡控制平面负载。但要进行过多次交换机迁移时，会使控制器集群间的通信开销迅猛增大。

综合国内外的研究现状，考虑到不同的负载均衡方案对网络性能的影响，目前大多数的多控制器负载均衡方案[36]普遍采用交换机迁移的方式，通过将负载转移的方式减少控制器之间的负载差异，采用优化算法对部署策略进行求解，但在迁移过程中大多数算法未充分考虑网络性能和迁移代价，以至于迁移效益比不高，对网络性能提升不大。

1.3 本文主要内容及结构安排

1.3.1 本文的主要研究内容

本文通过 SDN 多控制器负载均衡来降低骨干控制器被攻击的可能性，并提出了一种 SDN 控制平面的安全机制，在进行负载均衡策略之前，确保 SDN 多控制器网络的安全。本文的研究内容主要为：

（1）本文设计了一种三层的负载均衡结构框架。首先，提出了一种依靠整体控制平面负载状态的动态阈值调整方法，设置过载控制器负载判别器标志位。处于过载状态的控制器被降载，以平衡整个控制平面的负载。之后，针对待迁移交换机的选择，提出了一种基于流量请求速度、控制资源占比和迁移距离的优先迁移策略，将选出的交换机从过载控制器迁移到重选主控制器。最后，设计了一个基于改进遗传算法的主控制器重选算法，对算法中的算子进行优化设计，以解决由于控制器-交换机映射关系不能动态地适应不断变化的网络条件而带来的控制平面性能低下问题。

（2）在这项研究中，控制器与交换机的重映射问题被转化为一个多目标的优化问题。控制器集群的负载均衡度、通信时延和迁移成本被作为重选主控制器的理想效用函数。为了提供整个控制平面的负载平衡，使用非合作博弈策略确定纳什均衡下的最佳控制器部署。因此，针对上述的三目标进行优化，本文提出了一个基于改进遗传算法的算法来重选主控制器，并实现低负载均衡度、数据转发层与控制层之间的低时延以及交换机的迁移的低成本，使得重选主控制器的选择更加有效，并通过实验进行分析对比来验证算法的有效性。

（3）为保证 SDN 多控制器平面的安全，本文设计了一个基于 SDN 多控制器 DDoS 攻击的安全防御机制，分为三个模块包括数据采集模块、数据处理模块和流量拦截模块。通过数据采集模块提取流表信息，然后将提取到的信息进行分类，从而识别出恶意流量和正常请求流量，最终对恶意流量溯源进行拦截，保障 SDN 多控制器平面的安全，对提高控制平面安全性甚至整个网络的安全防御能力至关重要。

1.3.2 本文的主要结构

围绕整个研究内容，文章的组织结构如下：

第一章为绪论，主要介绍了当前网络中存在的安全问题以及研究目的与意义，详细阐述了 SDN 多控制器负载均衡技术和安全性的国内外研究现状，并说明了研究内容和结构安排。

第二章为相关技术架构。首先介绍了 SDN 的概念和体系架构、OpenFlow 交换机、控制器以及 OpenFlow 协议。接着分析了 SDN 网络中的关键技术，重点说明了多控制器的南向和东西向接口等技术。最后介绍了 SDN 多控制器控制平面的安全问题。

第三章对 SDN 分布式多控制器网络模型进行描述，并对网络模型进行参数设置，介绍了基于非合作博弈的 SDN 多控制器负载均衡策略。针对控制器集群中负载不均衡造成网络性能和安全性下降的问题，采用交换机与控制器重映射来实现负载均衡的解决方案，本文设计了一种三层 SDN 负载均衡框架，主要有控制器负载状态判定模块、迁移交换机选择模块和主控制器重选模块，对这三个模块分别进行了详细说明。

第四章先对主控制器重选问题进行分析，然后采取多目标优化对问题进行求解。然后介绍了传统的遗传算法思想，从而提出基于改进遗传算法的主控制器重选算法，对这一算法进行了详细的描述，并设计了约束条件以及优化目标。最后进行了负载均衡算法的实验对比和结果分析。

第五章针对 SDN 多控制器网络中所面临的安全性问题，阐述了在 SDN 网络环境下的 DDoS 攻击问题，并提出了基于 SDN 多控制器的 DDoS 安全防御机

制，进行系统模块设计，并分别详细地描述了数据采集模块、数据处理模块和流量拦截模块。然后通过仿真实验对该机制的可行性进行验证。

最后是总结展望。概括全文工作，总结研究中存在的不足，说明可以进一步开展研究工作的方向。