**第一章 绪论**

**1.1研究背景**

随着互联网的高速发展，运营商承载网络从最初简单Internet服务的“尽力而为”网络，逐步发展发展成能够提供涵盖文本、语音、视频等媒体业务的融合网络，其应用领域也逐步的向社会生活的各个方面渗透，深刻改变着人们的生产和生活方式。近年来云计算、大数据等新技术的兴起，面对云时代、大数据时代的高效、灵活的业务承载需求，传统网络的网络架构日益臃肿，面临一系列挑战：

1. 管理运维复杂：传统网络采用的是分布式控制平面，控制协议数量多，标准数量数以千计，如此庞大的控制协议体系，使得管理和维护网络变得愈发困难。

同时，设备厂商在实现这些标准协议时，都进行了一些特定的私有扩展，使得设备的操作维护变得更加复杂，进一步加剧了网络管理员操作维护网络的难度，同时大幅增加了网络的运维成本。

2. 网络封闭，创新困难：由于传统网络采用“垂直集成”的模式，控制平面和数据平面深度耦合，缺乏标准、开放的接口，且在分布式网络控制机制下，当需要在网络中部署新业务时，首先需要解决需求标准的定义，使得新技术的部署周期较长，严重制约网络的演进发展。

3. 设备日益臃肿：由于传统网络的技术体系采用“打补丁”式的演进策略，随着设备支持的功能和业务越来越多（例如，目前IETF发布的RFC标准超过7000个，且还在不停的增加新的RFC和Draft标准），其实现的复杂度显著增加。

传统网络的诸多限制导致网络架构需要改变。在这一背景下，业界一直在研究开发更加开放的新型的网络架构，促进网络逐渐向智能、开放、优化整合等方向转变。这种转变推动SDN软件定义网络的兴起。软件定义网络作为一种新型的网络架构，逻辑上集中的控制层面能够支持网络资源的灵活调度，灵活开放的接口能够支持网络能力的按需调用，将部分或全部网络功能软件化，更好地开放给用户，让用户更好地使用和部署网络，以适应快速变化的云计算、大数据以及更多的创新业务。

SDN作为一种对运营商网络具有重大影响的新技术，其价值已经被业界普遍认可，并在近些年发展迅速。但是随着对SDN架构开发和部署的不断深入, 安全性问题成为制约其发展的一个重要因素。一方面，SDN的出现给传统的网络安全研究带来了很多新的思路和解决方式；另一方面，作为一种全新的网络设计理念，其具有的集中控制性和开放性也会产生很多新的安全问题，比如控制器、基础设施层、控制器与应用层之间以及控制器和转发设备之间的安全问题等。