In the traditional network structure we are familiar with ,the cooperation of various network nodes are achieved in distributed system .Complete network protocol is running on each router , and each of them is provided with both forwarding ability and routing computational ability .The advantage of this architechture is that the network has strong reachability and fault tolerance and can avoid single point failure .However the disadvantages are obvious just like slowing network status is updated , implementation of new network policy is difficult and also , due to the distributed cooperation , each router cannot obtain the complete topology of the entire network in real time . DDoS (Distributed Denial of Service ) attack is launched by attackers utilizing the protocol vulnerabilities or insufficient network resources and the traffic volume attacks and SYN flood attacks are the major threats of the current network .Adversaries used to control a large mounts of bots and instruct them to send illegal traffic coordinately, which causes majority network resources be occupied by bots in a time window and and legitimate users would suffer from low network bandwidth, high jetter and high round trip time. Intelligent attacker can also coordinate several groups of bots to extend the time window as long as possible. In the traditional network architecture, all routers coordinate in a distributed way causing hard network status gaining and difficult topology view building, whatmore, once the commercial routers are running, it's impossible to change it's network policy dynamically. Moreover, DDoS attacks are simple to achieve, even non-computer major can lanch a complicate attack in several days, and the attack traffic is easy to hide and hide and disguise makes it difficult to distinguish from legitimate. Therefore, this attack method is easy to achieved in a very small cost and causing vast damage. The major challenge to mitigate the DDoS attack is: Difficult to distinguish the attack traffic. Difficult to obtain network status in traditional network architecture. Difficult to employ new security policy in traditional router's collaberate mode.**Background and Drawback**

SDN is a new network paradigm proposed by Nick et al in 2007. It uses contralization of control in logic to seperate the whole network into control plane and forwarding plane. The control plane, logically centralized, composed by one or more logically centralized Controller, is used to control network traffic and enforce traffic policy dynamically such as packet delivery policies, ip routing, ARP information query, etc. Date plane, comprized of some OpenFlow switches, is only resposible for simple data forwarding task. When the switch in topology edge received data packet, the packet field is extracted to match the rule in the switch installed by Controller. If it matches, the action corresponding to the peer is executed on the packet, otherwise the packet will be encapsulated in a packet\_in and delivered to the control plane. The controller can obtain appropriate route path by it's global topology function and traffic policy and then install rule to swithces along the path. In the SDN paradigm, controller has global topology ,programmability the the ability to enforce and change network traffic policies dynamically consequetly the whole network state can be monitored, network information can be collected and stored iterativelly. Detection algorithms can alse be excuted in Controller and enforce new traffic rule when attacking is detected. As we all know that machine learning techniques are very good at classification, and random forest, one of typical machine learning techniques, is good at classifying discrete data. By combine the virtue of machine learning and SDN, we proposed a new mechanism to mitigate DDoS named MLDS, which injecting the public traffic dataset into SDN network and utilizing the controller to collect the network characteristics. Thereafter transfering the network characteristics into vector and split the whole vector set into testing set and training set. We utilizing the training set to train the random forest module and testing set to examine the module. After module accuracy raise to the predefined value, We program the module into controller as a monitoring function to monitor the network traffic in realtime. When abnormal traffic is detected, we extract the packet characteristic by utilizing controller, and then install rules to instruct switch drop the illegitimate traffic. Meanwhile, controller can also collect network information in monitoring stage and retrain the random forest module to improve the module accuracy. This method fully utilizes the global control advantages of the SDN paradim and combines it with the machine learning classification capabilities to protect the availability of network services. The contribution of this paper is: Utilizing the SDN paradigm to collect traffic feature and moniter the network state in realtime. Combining the SDN with machine learning technology to mitigate the DDoS attack. Proposed iterative training method to improve the medule accuracy.**Research Scope and General Purpose**

*The rest of the paper is organized as follows. Section 2 provides relate work of other researchers in traditional network DDoS mitigation. Section 3 presents the technology of network state extracting in SDN enviroment and transform the collected feature into vector. Random forest model are trained and evaluated in section 4. Section 5 conclude the whole paper and we present the acknowledgement in section 6.****Content Arrangement***