（1）flow table saturation attack,

（2）control plane saturation attack,

（3）Topology poisoning attack,

（4）spoofing attack,

\*ARP攻击：攻击者企图通过发送ARP消息建立一个无效的地址映射。因为ARP协议没有机制可以验证发送者、回复以及各种信息的整合，所以攻击者就可以广播自己的MAC地址作为网关的MAC地址。

具体方法:攻击者伪装成网络中的某个节点，在接收到ARP消息之后，发送自己的MAC地址当作是源主机请求的MAC地址。

\*僵尸机

1. denial-of-service attack,

\*SYN泛洪攻击

\*DNS放大攻击

\*NTP攻击

\*一般攻击

\*混合攻击

（6）eavesdropping attack

（7）link discovery attack,攻击者企图欺骗控制器，使之在一个不存在的网络里建立一个新的连接，通过对经过此链路的数据流进行截听或者操控，可以掌握网络信息和该流量。

具体方法：网络通过LLDP（Line Layer Discovery Protocol）发送消息，以探听交换机之间的链路。攻击者通过伪造LLDP消息，并将之发送到目标交换机或者中继真正的LLDP消息，使控制器认为此链路存在。