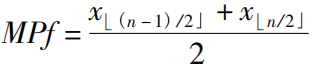
（1）An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking

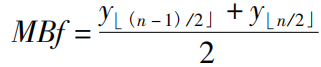
<IP src, IP dst, Srcport, Dstport, IP pro>

（2）《SDN 环境下基于 KNN 的 DDoS 攻击检测方法》

流包数中位数( Median of Packets per flow，MPf)：流表每道流中的数据包数目的中位数



流字节数中位值( Median of Bytes per flow，MBf)：流表中每道流的字节数的中位数



对流比( Percentage of Correlative flow，PCf)：对流即为交互流



端口增速( Ports Generating Speed，PGS)：随机生成端口号，速度上升



源IP增速( Source IP Growing Speed，SGS)：随机生成源IP地址，速度上升



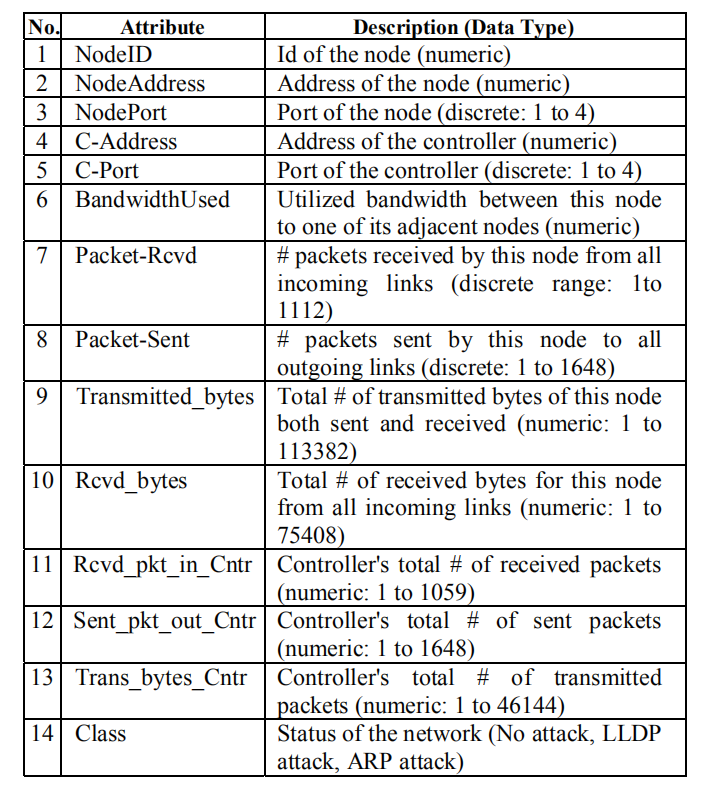
（3）《Detection as a Service: An SDN Application》

几乎是所有特征了：source IPv4 & IPv6 address, destination IPv4 & IPv6 address, source MAC address, destination MAC address, source port number, destination port number, metadata of packet, VLAN id,, SCTP source and destination ports, ICMP type and code, ARP opcode, ARP source and target IPv4 address, ARP source and target MAC address, MPLS label, TCP flags and other fields as specified in OpenFlow Switch 1.5.1 specifications

IP explicit congestion notification (ECN),

IP diffserv code point (DSCP)

（4）《Towards Prediction of Security Attacks on Software Defined Networks: A Big Data Analytic Approach》



（5）《RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks》

