**论文题目：**

**ZMap: Fast Internet-Wide Scanning and its Security Applications**

Durumeric, Z., Wustrow, E., & Halderman, J. A. (2013). ZMap: Fast Internet-wide Scanning and Its Security Applications. In *Proceedings of the 22nd USENIX Security Symposium* (pp. 605–619). Retrieved from https://zmap.io/paper.pdf

**论文总结：**

互联网范围的网络扫描有许多安全应用，如发现新的漏洞，跟踪网络防御机制等。但是现有的网络扫描工具不能满足大规模网络扫描的速度需求。一种新的模块化开源网络扫描工具zmap在一定程度上解决了这个问题，单台主机，在千兆网卡状态下，45分钟内完成全网络IPv4地址的扫描和探测，速度是常用的网络映射工具nmap的1300多倍。Zmap的性能提高得益于其针对大规模网络应用的特别优化，其中的核心优化总结如下：  
1. 探测优化，使用一个（cyclic multiplicative group）来随机选择目标地址，以保证目标路径不会拥塞（而不是像nmap一样限制传输速度来避免拥塞），跳过TCP/IP协议栈直接生成以太帧，从而以网卡的极限速度发送探测包，大大提高了探测速度。  
2. 无状态，不维护跟踪每个探测的连接状态而是使用类似SYN cookies的方法来区别有效的响应和网络背景流量，对每个扫描的主机，ZMap都依据特定的扫描密钥计算目标地址的MAC（使用UMAC方法），这个MAC值则分散在主动探测模块里的任何可用字段，用于校验。从而大大节省了内存等开销。  
3. 不重传，由于不保存连接状态，所以不需要重传，每个目标都是固定的探测包数目（缺省是1个），而nmap为了保存连接状态需要适应性的重传丢失的数据包，这样就大大提高了速度。