Internet-wide scanning has proven to be a valuable methodology for security research. While it is possible to perform an internet-wide scan, this method has been more accessible to attackers as compared to researchers and tools like Nmap take a lot of time. Zmap is capable of scanning ipv4 address up to 1300x faster than Nmap thanks to its architecture. It can help reveal new vulnerabilities, monitor deployment of mitigation and shed light on previously unknown things, tracking and adopting defensive mechanisms and more. This paper discusses the architecture of the scanner, profile its performance and efficiency and explore the offensive and the defensive implications of internet-wide network surveys. This paper also urges to be responsible citizens of the internet.

The paper compares Nmap with Zmap since it is very much like Zmap. It tells us how Zmap is better than Nmap. It focusses on the difference in probing methodologies, state of the connection and the retransmission policies. The research performed several experiments to compare ZMap to Nmap in Internet-wide scanning applications, focusing on coverage and elapsed time to complete a scan. Nmap and ZMap are optimized for very different purposes. Nmap is a highly flexible, multipurpose tool that is frequently used for probing many open ports on a smaller number of hosts, whereas ZMap is optimized to probe a single port across very large numbers of targets.

The paper successfully explains how Zmap’s modular design has helped achieved such a performance compare to Nmap. It tells us how it can achieve such speed, how Zmap is flexible and open to opting out of the scan and how it functions being almost stateless. One of ZMap’s most important architectural features is that sending and receiving packets take place in separate threads that act independently and continuously throughout the scan. The paper also experimentally confirms that Zmap can handle scanning 1.4M packets per seconds and that by sending a single SYN packet it covers up to 98% of the hosts and how it achieves a performance close to 1300x that of Nmap.

The paper explores most of the applications of the internet-wide scanning including the ability to gain visibility into previously opaque distributed systems, understand protocol adoption at a new resolution, uncover security phenomenon only accessible with a global perspective, monitoring outages, private communication to a group of people. However, high-speed scanning also has potentially malicious applications, such as finding and attacking vulnerable hosts.

Aware of the scale associated with Zmap, the paper responsibly provides a set of guidelines to follow when using such an application and makes the user aware of the kind of problems that one may run into while using it. It also rightfully stresses on the point of being responsible internet citizens. The paper also shows the kind of responses received during the study ranging from simply ignoring to downright retaliation. The paper acknowledges the recent work in a similar space and presents how Zmap excels in all the aspects of the previous techniques by staying in the limits and acting responsibly. The paper points out that there is additional work required when it comes to scaling up zmap for ipv6, increased ethernet speeds and intelligently excluding hosts that do not wish to participate.