ABSTRACT

Managing large networks consisting of thousands of network elements is becoming complex. However, organizations spread across multiple geographical locations have to run multiple management servers each managing a set of geographically localized devices. Network enterprises are looking forward to converge their existing wireless and wire line networks to leverage the benefits of a cost effective, revenue generating solution. The Internet is a collection of shared resources. Internet users share bandwidth and processing resources both in the network at routers and on the network edge at servers. However, the existing Internet architecture does not prevent nodes from consuming disproportionate resources. As a result in practice resource exhaustion does occur due to inefficiently scaling systems, selfish resource consumption and malicious attack. The current Internet architecture has limited support for both securing and identifying shared Internet resources. This resource sharing with respect to cooperative, selfish and malicious user models are studied for each case design a protocol that protects resource availability without modifying the existing internet infrastructure is presented. Design techniques and validate measurements for discovering shared internet resources including links and routers are also presented. The improvement achieved in the present work is established by comparing studies with publicly available resource networks.

Completely redesigning the protocols and network to improve resource usage is likely to prove impractical in terms of cost and coordination. The cost of individual routers range from tens to thousands of dollars. As a rough estimate there are approximately one hundred thousand routers deployed on the Internet. Thus, any solution that could not leverage the existing routing hardware would cost billions of dollars to implement. A compounding problem is coordination. The Internet is world-wide production system and any deployment of a redesigned network or protocols must globally coordinate and keep downtime to a minimum. Given the expense in modifying network hardware and the difficulty in coordinating global protocol update, the
motivation is resource sharing being improved without replacing existing protocols or modifying the network hardware.

Resource sharing is also complicated by the absence of a complete and accurate level map of the Internet. Without this map, an understanding of the distribution and usage patterns of network resources are limited. The location of routers and links and how they are shared are unknown and obtaining this map is difficult. Existing Internet protocols were not explicitly designed for monitoring of further Internet Service Providers (ISP’s). The local networks maps using are only known. In many cases active measurements and observations the network maps are inferred partially the Internet’s size, hardware diversity and ISP policy make these maps incomplete and inaccurate. Also, active measurements are limited by administrators who confuse measurement probes for attacks and generate “abuse reports” and even legal threats curtail the scope of experiments. What can be done to improve the completeness and accuracy of the map of the internet without causing the ire of network administrators? It is possible to secure and discover shared Internet resources without global protocol redeployment or architecture support.

The proposed work is focused on network performance monitoring tools, design and evaluation of protocols that secure the Internet’s shared resources without requiring network support or global protocol redeployment. The notion of security varies with respect to the attack model. This work demonstrates security in three distinct user assumptions, Co-operative, selfish and malicious users. Novel techniques for increasing the accuracy and completeness of Internet topology discovery are designed and evaluated. These techniques leverage existing protocol and hardware features and thus can be implemented on today’s Internet.