Chapter 7

Conclusion & Future scope

7.1 Conclusion Drawn

IPv6 and Internet Migration is the intricate convoluted problem today that demands time and large scale investment of resources. The solution for IPv4 exhaustion is yet to be conceived by corporates as an arduous problem thereby putting themselves at risk of insufficient time and economic resources. The major bottlenecks impeding the embracement of IPv6 is the infrastructural migration cost (software up-gradation, hardware costs, manpower training and network testing), ambivalent network performance of the new protocol and prospective security issues that might arise while deployment. Given the severity of problems in the current network scenario, IP migration process may be the only solution viable in the long run. Also IPv6 does provide substantial attributes and characteristics required by the modern day secure internet.

Though migration or transition between the two protocols is expected to take considerable amount of time, the transition mechanisms come into play for providing interoperability between the two protocols. Although, a number of transition techniques have been devised and standardized, developing an optimal one is still a hot research area and till date, no best feasible solution for transition plan has evolved. These transition techniques significantly attenuate the performance of the network as it is evident from chapter 3; where we made an empirical evaluation of four most commonly used transition mechanisms namely Dual Stack, Automatic 6to4 Tunneling, Manual 6in4 Tunneling and NAT-PT and made comparison of performance metrics with native IPv6 environment. The result from this evaluation inferred that transition techniques can only be seen viable for the migration period and may not be suitable for the long term deployment of applications on the internet. The only feasible solution for bandwidth efficiency and higher throughput is complete implementation of IPv6.

As seen in chapter 4, the colossal deployment of IPv6 into operational networks up-thrusts certain security issues. IPv6 introduces vulnerabilities in addition to those inherent in IPv4.While the existing security firewall, policies and infrastructure might be adequate for IPv4, the protocol security associated with IPv6 and IP migration networks needs to be assessed and analyzed. The next generation internet protocol IPv6 presents both advantages as well as certain drawbacks from the security point of view. Features such as mandatory usage of IPSec come with overheads

and performance issues. As evident from chapter 4 experiment, we notice that IPSec has significant impact on the network performance, which gets decreased while incorporating security. This performance decay affects Real time applications which are most sensitive to delay. So there is always a tradeoff between choosing better security or optimal performance.

As IPSec invigorates security to IPv6 by providing end to end communication security over the internet, however this security protocol does not foster security to the link local communication that uses Neighbor Discovery Protocol. As discussed in chapter 5, the security at the link layer provides an important role as the Internet being an open network is vulnerable to be exploited by attackers from both outside and inside the network. Utilization of IPSec security services to shield NDP messages has some potential problems like bootstrapping. The nodes need to be fully addressable before configuring IPSec security. Also, manual configuration of security associations in IPSec is a cumbersome and unrealistic task considering the bulk amount of messages in NDP. In chapter 5, we introduced SEND protocol and discussed its functionalities. We also discussed the implementation and deployment challenges of IPv6 SEND. The chapter carried analyses of the CGA security and computational complexity and finally proposed some techniques that can be used in optimizing the practical deployment of CGA in IPv6 networks.

In chapter 6, we discussed the IPv6 SLAAC process and highlighted some of its critical issues related to privacy and security. The chapter also proposed a novel and highly randomized technique for address generation that safeguards node's privacy and asserts address uniqueness on the link. The technique has a minimal computational cost and provides robust security against DoS attacks during the DAD process. For comparative performance analysis, we compared our technique with CGA algorithm. The results show that proposed technique improves computational time as compared to CGA.

7.2 Future Scope

IPv6 Security and Internet migration is the emerging area of research today which is being carried all over the world in multinational, corporate and government R&D organizations. In the initial chapter of this thesis we evaluated performance of IPv6 migration techniques and made an approach towards finding better technique among the existing migration techniques using the OPNET simulation environment. Although, we only evaluated existing migration techniques, the

future work in this area may be carried towards developing a better migration plan and techniques during the transition phase and evaluating it against current transition mechanisms. Focus is to be put on software side rather than upgrading existing hardware architecture which will be economical from implementation perspective. Similarly, evaluation and performance analysis of routing protocols and QoS models in IPv6 can be carried out.

In chapter 4, we saw that IPSec is a broader step towards security in IPv4 and Next Generation Internet Protocol IPv6. Although there is always a tradeoff between choosing better security or optimal performance, however the performance of the network can slightly be increased if complexities in IPSec are removed. In future, we can make use of caching and dynamic key generation techniques for optimization. In case of Real Time applications, QoS models and techniques can be implemented to avoid packet drop and delay. A stripped down version of IPSec can be incorporated in low power devices and mobile phones because they don't have large computational power. An approach like Header compression technique needs to be devised for accelerating IPSec enabled communication. Also in chapter 5, in case of CGA, work needs to be carried out in order to make it deployable for resource constrained devices like mobile phones. Use of multithreading techniques should be encouraged as it can be quite beneficial during the CGA address generation.