PREFACE OF THE THESIS

Today's world is full of Vulnerabilities in every corner of life. This was not the scenario of earlier decades and centuries. Government and nation need to employ and formulate secure policies for life and data of its people. Mechanism of cyber security is at the top and secure Wireless Network is also need of the time. If one analysis and evaluate these security methods in order to develop secure model, it would be a service for the nation and peace community of the world.

This evaluates why pre-RSNA methods fail for providing security to wireless Networks and what are the weaknesses and security issues of RSNA modes by way of developing real network testbeds and by simulating different network model in NS2 in order to conclude a secure model of WLAN and providing the ways to improve the performance of Network. This work is necessary to migrate to RSNA and making more highly secure and reliable RSNA methods. So security features, capabilities and aptitudes associated with WLAN through its framework for Robust Security Networks are evaluated, examined and elucidated in order to formulate it as guidance on the planning and deployment of RSNs.

During research, I understood that it is equally important to research as well as educating the users of cyber world with development of the secure model at the same time. I would not limit my journey till finishing of this research only and it would be continued with new efforts and methods in this direction of cyber security.
The Framework of this thesis is organized into chapters with their titles, main section and subsections. Each chapter contains the information relevant to chapter title. The Organization of chapters is as follows:

Chapter-1: Introduction:

Chapter-2 : Literature Review :
It defines information and network security with hierarchical order of security; security mechanism relevant to the thesis; threats and challenges to the security etc. Information of National and international organization/bodies formulating policies, procedures, standards and handling security incidents are described in this chapter. The functioning, objectives role and responsibilities of such bodies as well as various threat reports prepared by them are presented in it.
It covers WLAN; its deployment and architecture; Wireless security evolution; design of Wireless Security; threat and challenges; Secure routing protocols and Performance Metric analysis of WLAN.

Chapter-3 : Tools and Methods :
Network Simulators; Scanner and MAC Address Changer tools; WEP AND WPA-PSK key crackers methods and other Security measure tools used in the thesis are described in this chapter.

Chapter-4 : Result and Discussion : Simulation and Testbeds
The simulation model and developed Real Network Testbeds are presented, analyzed and discussed in this chapter.
Chapter-5 : Conclusion and Summary :

It summarizes the entire research effort. Accomplishment of task is concluded. Objectives as per synopsis are matched with the achievement and accomplishment. New ideas emerged out of it are suggested for future work.

(MOHID IZHAR)
Research Scholar