The current annual reports by Cisco, Symantec and Sophos, the market leading companies in the network security area, published in 2015, clearly state that attackers are using more advanced and sophisticated tools for unauthenticated access of resources. The report says, though there is a decrease in the number of zero day attacks, there is a noticeable increase in its impact. One of such unknown attack or zero day attack is a multi class attack in which attacker attacks by combining the characteristics of two or more attack types. Thus to detect multi class attacks along with single class attacks, we proposed a multi layered model in which existing IDS, detects the known attacks and the additional IDS detects multi class attacks. Based on the literature survey and experiments being conducted on such multi layered IDS, hike in the response time became the major challenge which in turn increased the packet dropping rate and the false alarm rate of multi layered IDS.

To reduce the response time, the proposed model uses Optimized Back Propagation Neural Network (OBPNN) as the high speed detection engine, reduced and normalized data and client-server architecture which uses light weight Jade based mobile agents. Experiments on the proposed model show that OBPNN based detection engine can process network traffic 16 times faster than the maximum packet transfer rate of 100 Mbps network. The recorded payload size of the agent is 2KB which is very less in comparison to 26KB recorded by other authors. Also, the recorded round trip time of agent is 110 ms, while it is 4.42 seconds recorded by others. Enhancements in the processing speed, agent size and mobile agent round trip time, could able to lower the response time of the detection process. Beyond this, the high speed additional behavioral layer has the capability to detect land and back multi class attacks. Hence, the model not only addresses the problem of identifying multi class attacks, but also reduces the response time to a greater extent, thus improving the performance of the detection rate.

The research work presented in this thesis has been implemented in two phases. The objective of the first phase is to reduce the response time and that of the second phase is to detect multi class attacks. In both the phases, model with the same architecture and deployment layout is used. The model is comprised of five major components: Back
Propagation Neural Network (BPNN), Data Normalization, Data Reduction, Mobile Agent and Multi Class Classifier. Work on multi class classifier has been applied for patenting and published by Indian patent office. Work on the other components has been either presented or published as research papers in well known journals or IEEE international conferences.

To present our research work appropriately, work of this thesis is divided into twelve chapters. First few chapters (Chapter 1 to Chapter 3) are based on the general discussion related to our research topic. Chapter 4 uncovers the proposed model with an outline view, while the individual components and their workings have been discussed in the next few chapters (Chapter 5 to Chapter 10). By integrating all the components, detailed working of the model is discussed in Chapter 11. Component wise results, overall results and conclusions are available in Chapter 12. Following is the extensive insight into the organization of the Chapters of the thesis.

Chapter 1 briefs about Intrusion Detection System (IDS). In this chapter, IDS, various approaches for classification of IDS and various alarm types are discussed. In Chapter 2, overall literature reviews comprised in five phases are presented. However, more detailed and component wise literature reviews are presented in the later chapters which address the various components of the proposed model. Back Propagation Neural Network (BPNN) is addressed in Chapter 3. Here, biological and computational model of neural network, feed forward neural network and feed backward neural network are discussed. In Chapter 4, the model is proposed along with its architecture and deployment layout. Overview of the model with summary of each component is briefed in this chapter while detailed discussions about each component are addressed in subsequent few chapters. Chapter 5 focuses on training and testing dataset. In this chapter, various behavior layers used for intrusion detection, selection of behavior layers and datasets for first phase and second phase of implementation are discussed in details.

Chapter 6 addresses Feature Reduction and N- Fold Validation in details. Chapter comprised of need for feature reduction and N-fold validation, literature review, selection of feature reduction technique and finally a model which does feature reduction and N-fold validation are presented. In Chapter 7, need for dataset normalization, analysis of
datasets used by the proposed model, data normalization model and its implementation are discussed in detail. **Chapter 8** focuses on Optimization of BPNN (OBPNN). In this chapter, need for parameter optimization, various parameters of BPNN, optimization model and its implementation are discussed. In **Chapter 9**, based on literature review, challenges of mobile agents and their solutions have been discussed in details. In **Chapter 10**, single class and multi class classifier, need of multi class classifier, literature review and model for multi class classification of network traffic are addressed. This chapter also discusses multi class dataset generation from single class dataset. After addressing every components of the proposed model in individual chapters, detailed working of the proposed model or research model is presented in **Chapter 11**. On the basis of the implementation of proposed model, in **Chapter 12**, results of each component, overall results of model, conclusion and feature work are outlined.