7. CONCLUSION

Unknown attacks are quickly becoming the next security challenge for today’s organizations. As time between the disclosure of a new vulnerability and the emergence of unique threats that operate against continues to diminish the system, so does the effectiveness of many conventional countermeasures that including patch management. Predictive learning techniques applied to intrusion detection would allow the system to develop a temporal model of data and permit the system to learn of intrusive behavior from temporal data and sequences of individual events.

Future networks and systems must be able to automatically configure themselves with respect to their security policies. The security policy specification must be dynamic and adapt itself to the changing environment. Those networks and systems should interoperate securely when their respective security policies are heterogeneous and possibly conflicting. There must be able to autonomously evaluate the impact of an intrusion in order to spontaneously select the appropriate and relevant response while an detection of unknown malware intrusion.

One of the biggest challenges in the network intrusion detection field is the limitation imposed by the use of well-known attack signatures that disable the detection of new unknown attacks. In order to conquer these limitations and inspired by intelligence principles, presented an intelligence based active defense model for network attacks which is on the basis of recent trend evolving techniques.

IIDPS is proposed with the best features of Intrusion detection system which is able to detect not only the known intrusions but also the unknown intrusions. ANN-AIS algorithms can be used along with the new methods for IIDPS. For detecting the unknown intrusions the proper knowledge base is to be formed after preprocessing the packets captured from the network. The preprocessing is the combination of partitioning and feature extraction. The partitioning of packets is based on the network services and extraction of attack feature is added to the knowledge base. The preprocessed attacks can
be classified by using association data mining classification which will be given to rule builder. Once the unknown intrusions are detected, that information can be added to the detector for further detection. The network intrusion detection system should be adaptable to all type of critical situations arise in network. This model based on a scheme of temporal logic (scheduler) in preparing schedule to check logs for possible intrusions, and detectors to detect normal and abnormal activity. If activity is normal then identify malware as known and reporting would be executed. If abnormal activity is found then classify into unknown malware category. The rule engine (Database) checks the rule to detect intrusion point and type of intrusion. The model also contains an expert system (ANN-AIS) to detect source of intrusion and suggests best possible prevention technique and suitable controls for different intrusions. This model also uses security audit as well as reporting mechanisms. The malicious activity database is stored for future intrusion detection and prevention evaluation. To detect the source by tracking, backward propagation approach is used. The rules are defined and are stored in the Rule engine of the system. Intrusion points and type is passed to expert system. Expert system evaluates that data with known malicious activity database and detects the source using backward propagation approach.

The intelligent intrusion detection prevention environment is like an automated process meet with many different events. An IIDPS, like a winning track team, needs many diversified skill sets. In this thesis, new schemes and Intelligence Intrusion Multi Detection Prevention System model to overcome the problems in finding unknown malware.

The proposed architecture of IIDPS with the Model Using Artificial Neural Networks is very effective and an efficient tool to study how IIDPS performs under various conditions. This architecture can be used to look into the malware activities and can also look for weakness in learning outcomes by statistically tracking unknown malware achievements. The proposed IIDPS model using neural networks helps to provide administrators with some insight on how the hybrid-learning model will perform under various conditions. It is anticipated that such a model will help the administrators and system users to make proper decisions based on the performance of the system.
As per experimentation it provide exact results for uncertainty attacks, it will help to find few initial values for unknown malware by using known family malware characteristics. Expected results are not predicted in other ways and methods. No solution is best for detecting all of the different attack types, and so many variables are involved that even a method with good accuracy may not be the best solution because it takes up too many resources.

Most of the anti malware tools provide solution for unknown attack as patch file through internet as updation. Apart from that intelligence intrusion detection prevention system and automated malware detection prevention systems provide continual updation without patch management. Apart from that port locking is also an alternative technique for avoiding unknown malware attack.

Experimental results which demonstrate the advantage of the IIDPS. When practical, experimental results include direct comparison between the resulting IIDPS model and results from re-accomplishing prominent tests from other research. The discussion also maps experimental findings to a common CPS, CPC model. It discusses the results and graph output being proposed for Intelligence access for Unknown Malware finding.

A number of other approaches have been studied only partially and remain the subject of considerable future research. Trap-based technologies and use of decoys and various types have only been partially explored, and offer numerous challenges to be effective methods of detecting sophisticated Unknown attacks.

The proposed methods reduce false positive and false negative considerably with no compromise in unknown percentage. The results obtained from the proposed methods are tabulated and plotted.

Limitation and Future Enhancements
As seemingly insignificant yet all-too-common obstacle for organizations trying to achieve an effective security solution is the inconsistent usage of related terminology. In many cases the term exploit is used interchangeably with threat. However, exploit technically refers only to the specific component of a threat that takes advantage of a vulnerability, as opposed to other components of a threat (e.g., propagation mechanisms to help it spread, or the actual payload). Not unlike the term vulnerability, the meaning of threat also varies somewhat with context. A mechanism (e.g., procedure, specific configuration, or program) that either eliminates a vulnerability otherwise reduces the potential for it to be exploited.

The main contributions of this work can be summarized as follows:

Security is hard to formalize, design, implement, verify, configure and use. It is particularly hard to use on a platform such as Windows, which is evolving, security-wise, along with its representative user-base.

The primary environment in which a typical Windows system exists has traditionally been hostile, especially after the advent of the Internet. While Linux systems share the same environment today, their traditional environments were comparatively trusted: research labs and universities. Similarly, Linux users have had backgrounds differing from Windows users.

In the first part of research work for proposing Intelligent Intrusion Detection Prevention System, few schemes were incorporated to identify the unknown malware with the help of known behavior of malware in database. Basic concepts of Intrusion Detection System and design principle of proposed Intelligence based security system named IIDPS. The phases of unknown malware detection have been described.
Besides, three new schemes using Euler Diagram, Allen Temporal event log algebra and QRA to identify and classify the unknown malware during the abnormal state in the network traffic and analyse unknown malware risk respectively. This is the work of investigation on the major trends in IIDPS technology and studying to figure out how existing features came into existence. This design and analysis of the overall architecture of an IIDPS are either totally domain dependent or they are just IIDP development shells. The advantage of the proposed model is that they are well customized for the chosen domain and are better tuned to the needs of their intended users. Also provides facilities and recipes to develop simple IIDPS in an easy and orderly fashion. Neural Network based architecture provides a personalized learning environment which intelligently analyzes and processes a Malware interaction and it is also easily adjustable for different domains.

In the second part of research work propose an algorithm for unknown malware detection and prevention. This is one of the solution towards the global malware detection system. The algorithm searches the signature database for the generated rules. Various scenarios arises from this situation also studied for further model implementation. This algorithm remedied the problem of basic standard algorithm (not able to stand the test for new and unknown malwares and a high false positive rate of around 30%). This indicates that the flaw in the filtering method as only those signatures were filtered out that were found in the training data. A high number of signatures were found in the clean programs in the test dataset. Assigning the final class outcome based upon the majority vote for malware and clean signatures in a file decreased the false positive rate significantly.

This algorithm remedied the problem of basic standard algorithm (not able to stand the test for new and unknown malwares and a high false positive rate of around 30%). This indicates that the flaw in the filtering method as only those signatures were filtered out that were found in the training data. A high number of signatures were found in the clean programs in the test dataset. Assigning the final class outcome based upon the majority vote for malware and clean signatures in a file decreased the false positive rate significantly.
In the third part of research work leads to the goal of IIDPS is to create a system that is adaptive and uses automatic responses to prevent network epidemics and high rate attacks. The adaptive mechanisms used in IIDPS is able to stop viruses and malwares much better than firewalls and traditional antivirus software as it can observe rate-based anomalies and is capable of preventing network epidemics from spreading more effectively and with fewer false positives than virus throttling. Additionally IIDPS can be installed on diverse hosts in many different network environments without manual rate threshold adjustments. Function of the proposed IIDPS starts with monitoring the incoming and outgoing traffic using sniffing tool. The network traffic is used by TSAM to calculate network traffic statistics. The monitored traffic is used as input to the PMM, which use the idea of infection-like-behavior in malware spreading to identify suspected malware traffic. Then administrators apply the number of hosts online as an input to ANNM, which uses the data that collected from other modules to classify the traffic into malware traffic or normal traffic, and to predict the percentage of infection in the network. To test the performance of IIDPS, the data were collected from the normal usage of three different users. The attacks used to test IIDPS were chosen to give a good sampling of high-rate attacks. The attacks cover scenarios when the machine protected by IIDPS was a victim in the attack (i.e. the attack was incoming, such as a denial of service SYN flood) and when IIDPS machine was the attacker (i.e. the attack was outgoing, such as malware propagation). Because IIDPS detects packets by comparing detectors with a bit string representation of the packet headers, attacks were also chosen to cover changes to different parts of the bit string representation. Since IIDPS can detect traffic coming both in and out of the protected machine, it can defend against attacks, when the protected machine is the victim as well as the attacker. To test the working of IIDPS to avoid different attacks, it is trained with the default parameter settings on each user’s data, and then tested on the highest rate attack data for each attack. The comparative analysis of IIDPS with CPC-CPS models and other Intrusion Detection Systems and Techniques reviewed in the literature survey in predicting and classifying the Unknown malware in the network. The classifiers using Classification Prediction Combined and Classification Prediction Separated models give better detection accuracy than the classifiers using other system features. As the result it is concluded that the proposed IIDPS produces good results in worm detection and produces perfect result with accuracy of 99.96% in detecting the presence of worm in the network even for unknown worms.

The designed intrusion detection and prevention system has been implemented with the simulation of WEKA tool connected with the standard datasets. The datasets are chosen from the researcher forum’s standard portals KDD, VXHeaven, CARO, CME and EICER. Performance of the IIDPS is
evaluated by conducting experiments with collected data and WEKA tool. The significant role of ANN in IIDPS is experimented through CPC and CPS models. The experimental findings of CPC and CPS with different worms are discussed. In addition, predicted infection percentage of TCP and UDP malware. The graphical results produced by the WEKA tools are explained. The results obtained from IIDPS are compared with existing IDS in the literature and are tabulated. The proposed methods reduce false positive and false negative considerably with no compromise in Unknown percentage. The results obtained from the proposed methods are tabulated and plotted.

Of course, it is crucial to address this issue in different wireless and mobile technologies available today such as Bluetooth, Infrared, RFID, Wifi, Wimax, 3G, 4G etc. Other technologies such as ad hoc and sensor networks, which introduce new type of services, also share similar requirements for an autonomous and spontaneous management of security.

Much work remains to be done to fully implement the full system. One of the main difficulties in developing new IIDPS is the time and cost required. A large team, including computer programmers, domain experts, and educational theorists, is needed to create just one IIDPS. So an important research issue is reducing the time and cost to develop such systems. Current strategies for doing this include the development of Malware analysis tools and creating systems in a modular fashion.

In the future, an experiment could be run with a larger and more balanced sample of Unknown malware. The confound with malware initiative could be removed for a better evaluation of various conditions. Another improvement would be to employ more tutorial strategies. A possible enhancement would be to allow the administrator to choose strategies dynamically according to unknown malware learning styles or what types of errors they make. A question that could be answered with another experiment is whether dialogs are more motivating for find unknown malware, or does dialog keep Unknown malware attention longer? Another experiment that controls for time rather than for the number of problems would examine whether IIDPS with dialog was worth the extra time.
The proposed algorithm for unknown malware detection and prevention in this work can be improved in future, to achieve more precise results and reduce the overall time consumption. The algorithm given is one of the solutions towards the global malware detection system. Its simplicity and effectiveness shown in this work make it highly practical to implement. Using multiple parameters as indicators of malware attacks, the integrated approach can reduce false positives.

Based on Algorithm in this thesis, there are still some issues for future study. The cost of the implementation of our algorithm in hardware design, and the difficulties on the deployment of monitoring components distributed in the Internet not yet analysed. Our future work includes the estimation of the resources necessary to implement the integrated solution and the study on a viable implementation.

New methods of detecting unknown attack, whether by Proactive or Other ways, remains an open and active area of research, and expect it to be so for some time to come. The new methods can be implemented using the swarm intelligent algorithms like Particle Swarm Optimization (PSO), Ant colony Optimization (ACO), Article Bee Colony Algorithms (ABC). Other popular algorithm alone not provide solution, use of combination of that provide lot of better solution than alone. Recent techniques and algorithm to produce still better results. A new operating security system cater with platform independency techniques fulfill the issues of unknown malware or new entrant of abnormal activities.