CHAPTER SEVEN
CONCLUSIONS
AND
RECOMMENDATIONS
FOR FUTURE WORK
7. CONCLUSIONS
In accordance with the primary objective of this research work that is to design an improved hybrid network intrusion detection system which is capable of providing a broader range to detection from a variety of network attacks while maintaining system at high performance level with reduce response time.

In the proposed system an improved NIDS is designed to provide the basic detection techniques so as to secure the systems present in the networks that are directly or indirectly connected to the Internet. An improved network intrusion detection system is an essential part that helps us in securing NIDSMAM which is connected to network; these systems permit the user to detect the both known and unknown attacks on the network. The proposed system enables the user to detect known and unknown types of network intrusion attacks and their source (IP address). The alarm systems and visual indications provided in the system notify the administrator (user) regarding the intrusion attacks being taking place so that immediate remedy actions could be taken to stop intrusion.

The following is just a first and of what should be the source of action while using the software and after an attack has been detected by improved NIDS. Unlike other conventional network intrusion detection systems, the present system also provides facilities for intrusion protection by detecting what type of attack and from which IP this attack is done and taking a proper action on that attack. The improved NIDSMAM is a light weight application having simpler structure as compared to existing NIDS systems yet provides protection from a variety of attacks. It is designed in such a way that it maintains the system at high performance level and reduced response time along with greater accuracy.

The clearly defined parameters for detection of known attacks are achieved by Jess rule engine. Improved network intrusion detection systems search for signs of an attack and make notifications when an intrusion (attack) is detected. In some cases they may take an action to stop the attack by shutdown the connection or report the incident for further analysis by network administrators. According to the detection methodology intrusion detection systems are typically categorized as misuse detection and anomaly detection systems. From a deployment perspective, they are been classified as network based or
host based although such distinction is coming to an end in today’s intrusion detection systems where information is collected from both network and host resources. In terms of performance, an improved NIDSMAM becomes more accurate as it detects more attacks and attempts to detect false alarms.

The improved NIDSMAM is written completely in Java. Thus, the present system is platform independent, yet it has been tested on WindowsXP. It can be tested on various other machines which run on different operating systems and which satisfy the requirements and prerequisites for the improved NIDSMAM. In NIDSMAM we have used both misuse and anomaly detection with the use of multi-agents.

Jade multi agents are used in the system which make the system distributed and independent of other agents. With these agents we can detect both types of attacks. For known attacks we have used snort rule in the system, and Jess format with Rete algorithm is also used in the system with makes the pattern matching very fast and improve the performance of the system.

Packets information in converted into facts and they are compared with the snort rules, and if they are matched we say that attack is known, and if the signature is not matched then we say that this attack is unknown by the system, and we are using anomaly detection with adaptive threshold algorithm. In anomaly detection, the attacks are not detected by misuse is checked with the threshold value, and if it excesses the value we say that is attack.

In accordance with the primary objective, the proposed NIDS application is able to detect intrusions on systems which are connected to network and it should display the required information to notify user regarding the type of risk the network is posing to the system. And also this system should be able to give all the information so that the intrusions those are more common to that the network can be analyzed at any time. The NIDSMAM application is tested with various environments and the results obtained are stored in the database for future analysis. This output would be in the form of messages displayed on the screen for various rules that were fired. Rules are fired basing on the facts that are given to the system during the testing phase. All these results are stored into the database. The storage of the results would be done along with information in the form of various columns like the attack occurred on the system, time at which it occurred, kind of intrusion that has happened and date of intrusion. This helps the end user to analyze the attacks that happened to the system at any point of time. A part from this any system is expected to be stable and also to be able to detect all the different kind of intrusions that
happen in the network. The testing methodology makes sure that the system will be able to detect the attacks present and also results are stored properly in the database in the decision support system DSS. The aimed NIDSMAM has succeeded to overcome the possible problem of the current solutions; it was capable to insert a mechanism for detecting attacks that objectives network. So, utilizing the multi-agent technology in designing and implementing the proposed NIDSMAM supplies more flexible and scalable system features, and overcomes the problems of heavy duty on network load.

On the other hand, in NIDSMAM developed constructs that will permit researchers to conduct further studies and research on the best techniques to protect the network from intruders by combining two methods misuse and anomaly detection system and the possibility boost the flexibility and extensibility in the system.

7.1 Goals achieved in the NIDSMAM

1) The main goal achieved in the NIDAMAM is the development of an improved network intrusion detection system which accomplish anomaly and misuse detection without compromising on system performance.

2) Improved network intrusion detection system through achieve very high accuracy in identification of known attacks as well as unknown attacks.

3) Improved network intrusion detection system through the development of a simple, light weight NIDS system for detection of both misuse and anomaly attacks.

4) Improved network intrusion detection system is to maintain and update a system level knowledge base for unknown attacks.

5) Another goal of NIDSMAM, improved network intrusion detection system is to achieve less complex structure, avoiding dead locks, less huge operations and reduce response time by implementing Multi-agents.

6) Another goal of NIDSMAM, improved network intrusion detection system is to provide a stronger protection to the system from majority types of intrusion attacks with lesser system processing time.
7) Yet another goal of NIDSMAM, improved network intrusion detection system is to update Snort rules database so as to include recent changes in rules soonerest as possible to achieve best possible protection from intrusion attacks.

8) Yet another goal of NIDSMAM is to inform user regarding intrusion attacks by means of charts and alarm signals.

9) Yet another goal of NIDSMAM is to provide a decision support system which enables the user to analyze system performance and helps in taking decisions related to system enhancement.

10) NIDSMAM its execution in software makes it cost efficient and as well as it can be used on any system that needs security. On the other hand, the select of the Jess software which uses a highly efficient algorithm (Rete) enables to accomplish and maintain the speed inside the software itself.

11) The signature detection technique will also be capable to detect attacks established by a malicious attacker who tries to change the behavior patterns with the target of retraining the anomaly detection module so that it will accept attack behavior as normal.

12) The goals of NIDSMAM have a response to deal and share information and resources in a distributed environment.

7.2 RECOMMENDATIONS FOR FUTURE WORK
The system may be enhanced by incorporating techniques corresponding to the future works listed below:
1) Extended our project to make it a distributed application where different modules of the same system running on different machines may interact with each other thus providing distributed detection and protection for all those machines on which the system is running.

2) Future advances in NIDSMAM are likely to continue to integrate more information from multiple sources making further use of artificial intelligence minimize the size of necessary to support signature databases.
3) Due to the high flexibility and extensibility given using the design of the system it will be easy to add more number of attacks to the system in the future.

4) We suggest designing the NIDSMAM system as a first primary model which will be enhanced in future using new technology to develop a system which is more powerful and detect more attacks.

5) We can make rules for packets which are detected by anomaly detection system. That the rule will use for misuse detection system. So, first time that attack is appearing as an unknown attack, but next time it will appear as a known attack.

6) For more detection of unknown attack, we can use more than one algorithm with adaptive threshold algorithm to analysis and estimate the results.