Chapter-6
Conclusion and Future Scope

Now, in this final chapter, we summarize the research work we have carried out, benefits of this research work, and future opportunities it opens for researchers.

6.1 Conclusion

In the beginning of this thesis we have started with problem formulation. We have asked following question:

“How to make anomaly based Network Intrusion Detection System usable while maintaining efficiency?”

We argued that anomaly based Network Intrusion Detection System can detect unknown attacks but suffers from false positive problem. Intrusion detection analyst cannot process such large number of alerts out of which most are false alert. Thus despite of several advantages anomaly based Network Intrusion Detection System is not usable. Today majority of popular open source and commercial Intrusion Detection Systems are signature based.

We have designed anomaly based Intrusion Detection System with the objective of reducing false positive rate. Three major components are designed in proposed model. The first component is preprocessing unit. Various functionalities incorporated in preprocessing unit to provide quality input to detection engine. The second component, detection engine is also designed considering reduction in false positive rate. Two most prominent soft computing techniques are ensemble to curb false alerts. The third component alert processing module also consists of various techniques to reduce false alerts. Alert aggregation, correlation, and categorization are used within alert processing module.
Network devices, host, and application status is stored in configuration database. Intrusion detection analyst supported configuration database helps in reducing false positives.

We improve the standard genetic algorithm and neural network algorithm based Intrusion Detection System by reducing 10% false positives. Based on the experimental results we can say that this research work is one step further towards making anomaly based Network Intrusion Detection System usable.

6.2 Benefits of this research work

The outcome of the research work is useful to other researchers who are working with intrusion detection or using soft computing techniques in their research work.

a. Processing large number of false alerts is neither feasible not acceptable. Reduced false positive rate demands less resources and increases credibility of IDS. Thus system becomes usable.

b. The approach clarifies various reasons which results in false positive. Intrusion detection analyst can avoid many such scenarios and help Intrusion Detection System to work effectively.

c. The suggested preprocessing approach can be utilized in many related areas like data mining and other soft computing based applications.

d. The experimental results and their interpretation will be helpful to other researchers working in the area of Intrusion Detection.

e. Ensemble approach of Neural Network and Genetic algorithm will be useful in other research areas like classification, pattern recognition, etc.

6.3 Future Scope

The research work and its encouraging results open several new directions. All these open questions will provide new research opportunities to the research community.
• In the detection engine we have used ensemble soft computing techniques. Genetic algorithm and neural network has performed as per our expectation. This opens research questions like Can we use fusion of other soft computing techniques? Can we fuse genetic algorithm and neural network in different way?

• One of the important factors in our proposed model is configuration database. It consists of current status of network devices, host, and applications. Creating and maintaining such configuration database is another challenge. It opens research question Can we have some algorithm which automatically creates and maintains the database?

• Our proposed module is heavily dependent on skill of intrusion detection analyst. In future researcher can work to reduce human dependency and takes most decision automatically.

• Another research question raised by our work is related to testing and evaluation of anomaly based Network Intrusion Detection System. KDD Cup 99 is really out dated (more than 16 years old) labeled dataset. This opens another research problem, Can we develop some dataset which represents modern attack and to evaluate anomaly based Network Intrusion System more effectively?
APPENDIX-A

Publication by Researcher


