CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION

Securing the organization and other private networks which are connected to the Internet from the existing and emerging attacks has been a big challenge for the security experts. DDoS attack is one kind of threat to the Internet users. Several DDoS detection algorithms have been in use for several years, special attention need to be given to meet the security attacks of today’s Internet communication under IPv6 protocol. IPv6 traffic is growing rapidly and every country is deploying IPv6 in their backbone network, the security vulnerabilities are also increasing. The existing DDoS detection algorithms do not detect all the kinds of attack that are specific to the IPv6 protocol. To detect different kinds of DDoS attacks, a number of mechanisms have been proposed. These algorithms cannot be used because of their resulting characteristics do not meet all the important required factors. K-means clustering based DDoS attack detection algorithm produces greater accuracy, but take more time to detect the attack and statistical based DDoS attack detection algorithms detect the attack very quickly, but result in a high number of false alarms. Taking into account of these matters, this research study proposes a resolution to improve the DDoS detection algorithm in terms of detection time, the detection rate and false positive rate.

An Entropy-Miner algorithm is given in this research study. The suggested solution in this thesis differs from most of the previously proposed DDoS detection algorithms. Unlike other detection approaches, in the first
The traffic flows are input into the statistical based entropy variation detection technique is applied to classify as normal and attack flows using an entropy threshold and then the suspected flows are further presented as input into the K-means clustering algorithm to verify their accuracy. This approach results in higher detection rate, very less detection time and very low false positive rate.

The salient characteristics of research work carried out in this field:

- An important and novel feature of the research work is that it detects both known and unknown DDoS attacks of IPv6 networks in an efficient fashion than the statistical based and data mining clustering based DDoS detection technique. The detection threshold of entropy value of normal and attack flows is dynamically set based on the network conditions. Existing DDoS attack detection algorithms use only constant threshold value to detect the DDoS attack.

- The proposed entropy-miner algorithm is extremely scalable. Every bit the net being a large scale network, the DDoS attack detection system must be extremely scalable. The proposed system combines both entropy variation technique and data mining, clustering technique and hence it can be taken to detect large scale DDoS attacks.

- This proposed work results in very low false positive rate. On that point are still outstanding matters, concerning the measurement error associated with most of the existing statistical based entropy variation detection techniques. The errors are more significant in heavily loaded networks and in
higher bandwidth networks. An accurate entropy-variation threshold measurement enhances the performance of the system by reducing false positive rates and improves detection rate.

- The intelligence of data mining K-means clustering can be effectively used to discover the novel DDoS attacks. It is detected using K-means clustering by grouping the flows based on their recent conduct. The primary principle of K-means clustering is to differentiate the attack flows from normal flows with the least exertion. This rule is given to find the various types of DDoS attacks. It uses various packet attributes chosen from entropy variation to quickly cluster the flows either as normal or attack flows. Since the clustering part operates only on a relatively lesser number of packets it processes the flows very rapidly.

- The Entropy-Miner is tested by bringing in some unknown attacks into the victim network. In a large scale network, many kinds of new DDoS attacks exist and it is necessary to test the performance of Entropy-Miner by introducing novel attacks. The proposed work shows better performance in detecting novel attacks than other methods.

The choice of Entropy-Miner algorithm as a solution in detecting DDoS attacks in IPv6 networks is motivated by the observed high variety of different kinds of DDoS attacks. Under this scenario, statistical based entropy variation detection techniques are known to degrade the overall detection performance in terms of higher false positive rates and their inability to differentiate flash events from DDoS attacks. K-means clustering based DDoS attack detection technique results in a higher detection rate and very
low false positive rate, however the detection time is very high compared to entropy variation based DDoS detection technique. The proposed Entropy-Miner detects both known and unknown DDoS attacks by combining both statistical based entropy variation technique and data mining based K-means clustering technique. This approach results in higher detection rate, very low false positive rate and requires very less time to detect DDoS attacks in IPv6 networks.

5.2 SCOPE FOR FUTURE DEVELOPMENT

Today’s Internet is vulnerable to variety of DDoS attacks. A DDoS detection algorithm should capture all flows and analyze the complete set of packet attributes for efficiently detecting DDoS attacks. The proposed work uses 7 of the packet’s attributes to calculate the entropy variance and to cluster the packets based on K-means clustering, to identify the suspected flaws. Instead of this approach, the research can be extended to use a very minimum number of packet attributes to do the same.

Routers determine the specific choice of route for every packet. A router shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. Entropy-Miner’s intelligence can also be applied in intermediate routers so that the source of the attack packets can easily be traced and if an attack happens, the packets can be dropped at the edge router of the attack source.

The research uses the entropy variation parameter and K-means clustering algorithm to detect DDoS attacks. The research may be extended to use any other statistical based techniques and any other clustering algorithms and also the proposed work uses the entropy variation first and K-means clustering next in detecting DDoS attacks. These can also be interchangeably used.