ABSTRACT

The Internet is a global system of interconnected computer networks that works (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks. Since it carries a vast range of information resources naturally its services are accessed by huge number of people globally.

The design architecture of the Internet permits the user to share its resources any where any time. During the resource sharing, data packets are routed through different networks till they reach their destination. While data are transferred among different networks, routers in the Internet do not perform any security verification of the requested source IP origin.

The lack of such a verification of the originality of each request opens the door for attackers to create fake identities and send a malicious request on the internet. As an impact of this activity the significant resources of network servers are unavailable for the legitimate users. The ultimate goal of the attacker is either to access the server resources illegally or make the server resource unavailable to the legitimate user access by simply floods
number of requests. Commonly employed network security vulnerabilities by
the attackers are man-in-the-middle attacks, Denial-of-Service (DoS) attacks,
etc.

Among different types of IP based network attacks DoS attack is
one of the serious issues on the Internet. Establishment of this type attack in
internet is easy and it is carried out with spoofing technique.

Thus it is mandatory for the user and the service providers to ensure
a secured data transmission on the data network by the establishing of a
suitable network attack detection system that can to detect various attacks on
the data network.

A best network attack detection system should operate with fewer
amounts of previous knowledge or without any type of the preceding
information. Keeping this in mind this study implemented a secured key
exchange based attack detection/prevention method which prevents efficiently
the unauthorized access of a resource server.

The attacker detection efficiency is further improved by preventing
the attacker involvement at the ingress of the resource server itself by
implementing a filter technique. By validating the inherent Internet
parameters of the requested source IP, the fake request is eliminated by
implementation of an IP2HP (IP to Hop count/t Packet transfer time) filter. In
this filtering technique, inherent internet parameters are validated with the
previously stored database. The efficiency of the attacker prevention is improved further in this filtering technique.

Detection of the origin of attacker is mandatory for any attack detection method so that the involvement of the attacker is completely prevented. To identify the source of the attacker this study implemented an Ant system algorithm based IP trace-back method to find the origin of the attack. An ant colony algorithm is a probabilistic technique used for finding the best path between the source and destination. According to the ethologists ants laying down a trail of pheromone for attracting and guiding other ants to reach food source and back to their nest. This behavioral concept of the ant algorithm is utilized in this research to identify the origin of the attack source. The detection efficiency of the origin of an attacker using this technique is enhanced. In this technique the metric pheromone intensity is used for the attack detection process.

To optimize the detection procedure further, another flow based metric called as entropy variation is also considered for the detection process. Entropy is an important factor in information theory, which is a measure of randomness. It measures the changes of randomness of data flows at a router for a given time interval. Therefore by considering the pheromone intensity and the entropy variation of each path between source and destination, the attack path is identified. The proposed attack detection approach is functioning without any modification of the existing routing mechanism.
Among the different attack detection techniques, based on the simulation results it is found that the ant system based IP traceback with the entropy variation approach is an efficient method for attack source identification on data network.