CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

This chapter focuses in-depth on the various research works done so far in IPv6 security against DDoS attacks, DDoS attack detection using statistical approach and DDoS attack detection using data mining approach. Vulnerabilities of the IPv6 protocol against DDoS attacks and the limitations of existing DDoS attack detection algorithms are presented in detail.

2.2 IPv6 SECURITY ISSUES

There are great expectations about the features of the IPv6 protocol, one of which is better network security. IPv6 provides network level security via IPSec. Because of the new features of IPv6 different level of new security issues are also raised. Radhakrishnan et al (2007) identified the various new possibilities of attack on IPv6 networks based on the new features of IPv6 protocol.

Carlos Caicedo et al (2009) has stated their work on IPv6 adoption exist within the networking community, including the vision that IPv6 is a failure and offer no important advantage over IPv4. Even as IPv6’s latest features will probably generate newer protocol attacks, the older known IPv4-related attacks will morph into new forms. IPv6 was designed with security in mind; security concerns could delay its success if sufficient efforts and resources are not dedicated to fully understanding IPv6-related security issues.
and vulnerabilities in IPv6-based network infrastructures. Several attacks can only be executed by a node in the network sector. It shows some of these attacks, securities provided by the DoS attack on Duplicate Address detection (DAD) protocol, Man-in-the-middle attack, and fake router implantation attack. Given IPv6’s growing importance, the development of techniques and tools to protect emerging IPv6-based networks is a current and pressing need.

Van Hauser (2008) developed the first set of IPv6 protocol attacks. The presentation shows that there are several IPv6 attacks that are new to DoS research. With a focus on host-based attacks, the important attacks presented are related to exploiting the Neighbor Discovery Protocol (NDP). It inspects the NDP and exposes vulnerabilities with the Duplicate Address Detection (DAD), allowing a malicious client to intercept or terminate communication to a local area network (LAN).

Luís Oliveira (2012) proposed a new method Neighbor Discovery (ND) protocol is proposed to mitigate DoS attacks. In IPv6 ND is used to perform multicast transmission. Neighbor discovery was simplified by replacing the address resolution process with an address registration mechanism.

The deployment of IPv6 has both benefits and drawbacks in security point of view. Many of the attacks applicable to IPv4 remain the same in principle to IPv6, but different in the way that they are applied. Troy Lancaster (2006) clearly depicted that the convenient number of hosts makes scanning of the network easier for attackers. Privacy extensions for stateless auto configuration can facilitate the generation of randomized interface identifiers to exploit the full 64-bit subnet, greatly reducing the need for administrator intervention whilst maintaining randomized addresses. However, if a node address has a very short lifetime the frequency of address
changing would display the behavior of a compromised system, which has been the source of a Distributed Denial of Service (DDoS) attack.

Xinyu et al (2007) goes into detail on the attacks that are exploitable under IPv6. This includes previous exploits that were carried over from IPv4 and new problems introduced by the IPv6 protocol. He provides a comprehensive list of attacks and analysis thereof under simple network implementations, without firewalls.

There are some ways to interfere with the normal behavior of the auto configuration process, causing redirection of traffic (Denial of Service). Special attention must be put on the Router Advertisement (RA), Router Solicitation (RS), Neighbor Solicitation (NS), Neighbor Advertisement (NA) and Redirect messages Alvaro Vives & Jordi Palet (2005). Using host firewalls IDS (Intrusion Detection Systems) for protecting hosts against these threats is very likely a wrong approach, as that would basically imply reinventing SEND; it is better to use SEND instead. There is no easy protection against these threats as the ND features are needed before a host can authorize itself to the other network components.

CAMNEP a new IDS model to detect DDoS attacks in IPv6 networks developed by Jiri Mensik (2012) detects the attacks very effectively. It uses various effective DDoS detection techniques such as Minnesota Intrusion Detection System (MINDS), Lakhina volume, Lakhnia Entropy and Time based Access Pattern Sequential hypothesis testing (TAPS). However the usage of multiple IPv6 addresses for a single host makes the TAPS algorithm scanning ineffective.

Wang Chao et al (2013) presented an intrusion detection system under IPv6 platform based on intrusion detection feature attribute reduction by using pattern matching, so as to expand the range of application and user
group of the security products. By the analysis and comparison of various pattern matching algorithms, the new algorithm realizes the intrusion feature module matching under IPv6, and make detection system be of high efficiency.

Baba & Matsuda (2002) presented a hop-by-hop packet logging approach for traceback. There are three major components in the system, namely, the sensor, monitoring manager and tracer. The tracer which is implemented in the routers, logs incoming packet information named, the packet feature, in a buffer memory called packet information area. It then replaces the packet’s data link-level identifier in its interface identifier and forwards the packet. The sensor monitors traffic at the victim. If the sensor detects an attack, it sends a tracing request to the monitoring manager which then manages the whole tracing process. The tracer identifies an adjacent node of an attack packet by searching in the packet information area and sends the result to the monitoring manager which in turn sends a tracing request to that node. This process continues until the source of the attack packet is identified. But this solution introduces a large processing overhead on the routers and is not scalable.

An alternative approach to IP traceback problem is packet marking. Savage (2001) introduced the probabilistic packet marking scheme for IP traceback. They have proposed a series of marking algorithms all having two main components, namely, a marking procedure and a path reconstruction procedure. The marking procedure is performed by the routers and the path reconstruction procedure is done by the victim. The simplest algorithm, node appending, appends each router’s address to the end of the packet as it travels through the network from source to the victim. This algorithm is infeasible because of the facts that it introduces high processing overhead and suffers from space constraints to perform the marking on the packets. Node sampling
algorithm reduces the space requirement and the processing overhead by allowing routers to mark the packets with a probability $p$. A 32 bit field is reserved for this purpose in the packet header. If $p$ is identical for all routers then the probability of receiving a packet marked by a router $d$ hops away from the victim is $p(1-p)^{d-1}$. Using this information, the victim reconstructs the attack path. Unfortunately, the number of packets required to perform this reconstruction is large and moreover the process significantly slows. These undesirable features are weakened to some extent by the edge sampling and compressed edge fragment sampling algorithms.

Ting Ma (2009) proposed a link signature based DDoS detection and traceback algorithm for IPv6. His proposal showed that it worked better in simulation environments and its scalability is a big issue. Andrey balenki et al (2000) presents a novel approach to IP Traceback - Deterministic Packet Marking (DPM). The proposed approach is scalable, simple to implement, and introduces no bandwidth and practically no processing overhead on the network equipment. It is capable of tracing thousands of simultaneous attackers during DDoS attack. All of the processing is done to the victim. The traceback process can be performed post-mortem, which allows for tracing the attacks that may not have been noticed initially. The involvement of the Internet service providers (ISP) is very limited, and changes to the infrastructure and operation required to deploy DPM are minimal. DPM performs the traceback without revealing the internal topology of the provider's network, which is a desirable quality of a traceback scheme.

A modified Deterministic Packet Marking algorithm was proposed by Hai-Xu Long et al (2013) to detect DDoS attack and trace back the attack source. The simulation results of the modified DPM algorithm show that the improved algorithm is effective in IPv6 network can reduce the burden on the edge router network. Network flow characteristics are needed for determining
the mark threshold and mark probability, it is a limitation of this algorithm. Law et al (2005) used probabilistic edge marking algorithm for traceback. Three fields \{start, end, distance\} is stored in the IP header. The start and end fields store the IP addresses of the two routers at the end points of the marked edge while the distance field records the number of hops between the marked edge and the victim site V. Each router will mark each packet destined for V with probability p. If marking is performed, the router records its IP address in the start field and sets the value of the distance field to zero. Otherwise, if the value of the distance field is equal to zero, the router records its IP address in the end field and then increments the distance field by one. If the distance field is not equal to zero, the router simply increments the distance field by one. At the victim site, based on the amount of received marked packets, the intensity of local traffic at each router in the attack path is computed. Based on these intensities the local traffics are ranked and the network domains generating more attack traffic are identified.

Belenky & Ansari (2000) introduced a new packet marking scheme called deterministic packet marking (DPM). The 16-bit packet identification field and the reserved 1-bit flag in the IP header are used for marking. When a packet enters the network, it is marked on the edge ingress router by the interface closest to the packet source. The address of the interface is split into two halves of 16-bits. With a probability of 0.5, either the first half or the second half is marked in the packet ID field. The flag bit is then set to 0 if it is the first half or to 1 if it is the second half. At the victim site, a table mapping the source address to the ingress address is maintained. On receiving a packet, the victim checks whether the table contains an entry for the source address of the packet. If not, it makes an entry for the source address with the available 16 bits of the ingress address. On the contrary, if the table has an entry with only 16 bits of the ingress address, it completes the ingress address in case, the other half is available. Thus, the victim can trace from which router, the
packets came. Though this method is simple, it is vulnerable to pollution by attackers.

Goodrich (2008) proposed the randomize-and-link approach to implement IP traceback based on the probabilistic packet marking mechanism. According to his method, every router X calculates a checksum value, $C = C(M_X)$, named as cord from its unique message $M_X$ (e.g., IP address) and fragments $M_X$ into several pieces, $M_0, M_1, \ldots, M_x$. The router then marks the packets probabilistically with $b$ bits, where $b = [I, C, M_i]$. The cord is usually quite large, for example, 14 out of 25 bits, so that it is hard for hackers to predict it. By inspecting the cord and the index, the victim can reconstruct the message, $M_X$ efficiently.

Currently not only PCs and servers but also numerous smart devices are also connected to the Internet. These devices can be addressed using IPv6 address space. Providing security services in smart object networks connected to the Internet is considered an open issue. Providing security in the resource constrained network is even more challenging when compared with standard networks. Therefore, special protocols and mechanisms have been developed for use in smart object networks. Luis et al (2012) has presented a security mechanism to prevent remotely initiated transport level DoS attacks. The proposed mechanism filters at the edge router the traffic received from the Internet and destined to smart object nodes. The edge router only forwards the Internet traffic into the smart objects network if the traffic meets predefined conditions. In the proposed solution, smart nodes use an adapted version of 6LoWPAN neighbor address registration mechanism to inform the edge router about the conditions used to filter the Internet received traffic.

Feslin Anish Mon et al (2012) proposed an enhanced ICMPV6 Trace back scheme, called ITrace-CP (ICMPV6 Trace back to Cumulative
that encodes cumulative attack path information. The ITrace-CP protocol was described and the mechanisms for constructing ITrace-CP messages were also depicted so that it contains the addresses of all the nodes on the attack path. The main objective of the proposed work is to determine the true source of DoS/DDoS attacks.

2.3 DDoS DETECTION MECHANISMS

In this section, a summary of existing literature on DDoS attack detection methods is presented. These methods are broadly classified into four categories as follows Monowar Bhuyan et al (2013):

1. Statistical based
2. Soft Computing
3. Knowledge based
4. Data mining and Machine learning

2.3.1 Statistical Based

Statistical properties of normal and attack patterns can be exploited for detection of DDoS attacks. Generally a statistical model for normal traffic is fitted and then a statistical inference test is applied to determine if a new instance belongs to this model. Instances that do not conform to the learnt model, based on the applied test statistics, are classified as anomalies.

Sushma Reddy et al (2012) proposed an effective and efficient IP Traceback scheme against DDOS attacks based on entropy variations. Here the packet marking strategies are avoided, because it suffers a number of drawbacks. This paper employs by storing the information about flow entropy variations at routers. Once the DDOS attack has been identified it performs
push-back tracing procedure. The Traceback algorithm first identifies its upstream router where the attack flows comes from and then submits the Traceback request to the related upstream router. Anitha G (2012) proposed a novel traceback method for DDoS attacks that is based on entropy variations between normal and DDoS attack traffic, then compare this variation with the router’s buffer’s capacity, which is fundamentally different from commonly used packet marking techniques.

Gabriel Macia-Fernandez et al (2008) present the low-rate DoS attack against concurrent servers (henceforth the LoRDAS attack). It is an evolution of the low-rate DoS attack against iterative servers, adapted for damaging more complex systems like concurrent servers. A concurrent server is characterized by allowing the processing of the received requests in a parallel way, not as in the iterative servers, where these are sequentially processed. Given that the bulk of the servers on the Internet are implemented as concurrent servers and, in many cases, these are a critical infrastructure, the existence of a DoS attack against them supposes a high risk and, therefore, its execution could have a wide impact.

Xinyu Yang et al (2007) defined the typical DDoS threats under IPv6 and also they use IPSec to detect those attacks. They proposed four attack models Flood, UDP-Flood, ICMP-Flood and Smurf. This method implemented based on the Neighbor Discovery and Router Discovery.

Sanjeev Khanna et al (2011) introduced an Adaptive Selective Verification algorithm which works based on selective verification. This algorithm employs a reservoir based random sampling to effectively sample the sequence of incoming packets from the client requests. The simulation results show that its effectiveness against its counterparts that under highly variable DDoS attack rate conditions also this algorithm detects those attacks very well.
Fei Wang et al (2012) employed a multi stage approach to detect subtle DDoS attacks. This approach uses network traffic state prediction, a fine-grained singularity detection and a malicious address extraction engine. It essentially uses joint deviation rate to detect the approximate start time of the attack. This technique effectively detects low-rate DDoS attacks.

Shui Yu & Wanlei Zhou (2008) proposed a community network that operates with the same Internet Service Provider, domain or the virtual network of different entities that are cooperating with each other. They noticed that the attackers use the same mathematical functions to control the speed of attack package pumping to the victim.

Giseop No & Ilkyeun Ra (2009) proposed a modified entropy calculation scheme called Fast entropy to compute the entropy variation at the intermediate routers with less overhead. This scheme reduced the computation time by 90% and maintained the same level of accuracy. But it produced a high number of false positives compared to the conventional entropy variation technique.

D-WARD proposed by Mirkovic et al (2002) identifies an attack based on continuous monitoring of bidirectional traffic flows between the network and the rest of the Internet and by periodic deviation analysis with the normal flow patterns. Mismatched flows are rate limited in proportion to their aggressiveness. DWARD not only offers a good detection rate, but also reduces DDoS attack traffic significantly. It uses a predefined model for normal traffic to detect anomalies in the two-way traffic statistics for each peer. However, if refuted, it gradually allows increased traffic rate.

Saifullah (2009) proposes a defense mechanism based on a distributed algorithm that performs with weight-fair throttling at upstream routers. The throttling is weight-fair because the traffic destined for the server
is controlled (increased or decreased) by leaky buckets at the routers based on the number of users connected, directly or through other routers, to each router.

Yang Xiang et al (2011) proposes two new and effective information metrics for low-rate DDoS attack detection: generalized entropy and information distance metric. These metrics can improve the system’s detection sensitivity by effectively adjusting the value of the generalized entropy and information distance metrics.

Another entropy based IDS system called A-NIDS Pablo Velarde et al (2012). They proposed Entropy space a new technique for detecting anomalous behavior traffic in a computer network is presented. The entropy space method is based on 3D-built on flow packet level, and then applies to the Pattern Recognition.

Chen (2009) presents a new detection method for DDoS attack traffic based on the two-sample t-test. It first obtains statistics for normal SYN arrival rate (SAR) and confirms that it follows the normal distribution. The method identifies an attack by computing (a) the difference between incoming SAR and normal SAR, and (b) the difference between the number of SYN and ACK packets. Unlike most previous DDoS defense schemes that only deal with either flooding or meek attack, the proposal uses two statistical tests to identify malicious traffic. It first compares the differences between the overall means of the incoming traffic arrival rate and the normal traffic arrival rate of the two sample t-test. If the difference is significant, it concludes that the traffic may include flooding attack packets. However, the low-rate attack traffic may pass the arrival rate test and make the backlog queue full. The approach then compares the two groups that contain different numbers of SYN and ACK packets from the two-sample t-test. If there is a significant difference, it recognizes that the attack traffic is mixed into the current traffic.
Anusha et al (2011) proposed an effective and efficient IP Traceback scheme against DDOS attacks based on entropy variations. This paper employs by storing the information about flow entropy variations at routers. Once the DDOS attack has been identified it performs push-back tracing procedure. The Traceback algorithm first identifies its upstream router where the attack flows comes from and then submits the Traceback request to the related upstream router.

Shui Yu et al (2012) proposed a community network that operates with the same Internet Service Provider, domain or the virtual network of different entities that are cooperating with each other. With such a federated network environment, routers can work closely to raise early warning of DDoS attacks to void catastrophic damages. It is observed that the attackers use the same mathematical functions to control the speed of attack package pumping to the victim. Based on this observation, the different attack flows of a DDoS attack share the same regularities, which is different from the real surging accessing in a short time period. Information theory, parameter called entropy rate, is applied to discriminate the DDoS attack from the surge legitimate accessing.

Sheng wen et al (2010) presented an approach for countering application-layer DDoS attack that mimics the normal users’ behaviors. The basic assumptions are: (1) abrupt changes in the traffic mean a possible existence of abnormal traffic; (2) the mess extent of various DDoS attacks is larger than the flash crowds. Based on the first point, we introduce a front-end sensor to detect the abnormal traffic and report its existence when abnormal traffic arrives. The second component which is used for distinguishing DDoS attack and flash crowd is activated or stopped by the signal ATTENTION or DISMISS from the front-end sensor. With the parameters of malicious IP addresses, the filter blocks the abnormal traffic and leaves the Website to be
safe. The analysis and experiments show that the proposed system performs well in countering various application-layer DDoS attacks and the delay for detection is kept in a range of N seconds.

Yang Xiang et al (2011) proposes two new and effective information metrics for low-rate DDoS attack detection: generalized entropy and information distance metric. The experimental results show that these metrics work effectively and stably. They outperform the traditional Shannon entropy and Kullback–Leibler distance approaches, respectively, in detecting anomaly traffic. In particular, these metrics can improve (or match the various requirements of) the system’s detection sensitivity by effectively adjusting the value of the order of the generalized entropy and information distance metrics. As the proposed metrics can increase the information distance (gap) between attack traffic and legitimate traffic, they can effectively detect low-rate DDoS attacks early and reduce the false positive rate clearly. The proposed information distance metric overcomes the properties of asymmetric of both Kullback–Leibler and information divergences.

Wang et al (2006) proposes a system model with an explicit algorithm to perform on-line traffic analysis. In this scheme, we first make use of degree distributions to effectively profile traffic features, and then use the entropy to determine and report changes of degree distributions, which changes of entropy values can accurately differentiate a massive network event, normal or anomalous by adaptive threshold. Evaluations of this scheme demonstrate that it is feasible and efficient for on-line anomaly detection in practice via simulations, using the traffic collected at the high-speed link.

Bin Xiao et al (2006) proposes a novel cooperative system for producing warning of a DDoS attack. The system consists of a client detector and a server detector. The client detector is placed on the innocent client side and uses a Bloom filter-based detection scheme to generate accurate detection
results yet consumes minimal storage and computational resources. The server detector can actively assist the notification process by sending requests to innocent hosts. Simulation results show that the cooperative technique presented in this paper can yield accurate DDoS alarms at an early stage.

Yu Gu et al (2004) develops a behavior-based anomaly detection method that detects network anomalies by comparing the current network traffic against a baseline distribution. The Maximum Entropy technique provides a flexible and fast approach to estimate the baseline distribution, which also gives the network administrator a multi-dimensional view of the network traffic. By computing a measure related to the relative entropy of the network traffic under observation with respect to the baseline distribution, we are able to distinguish anomalies that change the traffic either abruptly or slowly. In addition, our method provides information revealing the type of the anomaly detected. It requires a constant memory and a computation time proportional to the traffic rate.

Tao Peng et al (2000) proposes a simple but robust scheme to detect denial of service attacks (including distributed denial of service attacks) by monitoring the increase of new IP addresses. Unlike previous proposals for bandwidth attack detection schemes which are based on monitoring the traffic volume, our scheme is very effective for highly distributed denial of service attacks. Our scheme exploits an inherent feature of DDoS attacks, which makes it hard for the attacker to counter this detection scheme by changing their attack signature. Our scheme uses a sequential non parametric change point detection method to improve the detection accuracy without requiring a detailed model of normal and attack traffic. We demonstrate that we can achieve high detection accuracy in a range of different network packet traces.
2.3.2 **Soft Computing Based**

Learning paradigms, such as neural networks, radial basis functions and genetic algorithms are increasingly used in the DDoS attack detection because of their ability to classify intelligently and automatically. Jalili et al (2009) introduces a DDoS attack detection system called SPUNNID that works based on a statistical pre-processor and unsupervised artificial neural net. They use statistical pre-processing to extract features from the traffic, and an unsupervised neural net to analyze and classify traffic patterns as either a DDoS attack or normal.

Karimazad & Faraahi (2011) propose an anomaly based DDoS detection method based on features of attack packets, analyzing those using Radial Basis Function (RBF) neural networks. The method can be applied to edge routers of victim networks. Vectors with seven features are used to activate an RBF neural network at each time window. The RBF neural network is applied to classify data to normal and attack categories. If the incoming traffic is recognized as attack traffic, the source IP addresses of the attack packets are sent to the Filtering Module and the Attack Alarm Module for further actions. Otherwise, if the traffic is normal, it is sent to the destination. RBF neural network training can be performed as an offline process, but it is used in real time to detect attacks faster.

Gavrilis & Dermatas (2005) also present a detector for DDoS attacks in public networks based on statistical features estimated in short-time window analysis of incoming data packets. A small number of statistical descriptors are used to describe the behavior of the DDoS attacks. An accurate classification is achieved using Radial Basis Function neural networks.
Wu et al (2011) propose to detect DDoS attacks using decision trees and grey relational analysis. The detection of the attack from the normal situation is viewed as a classification problem. They use 15 attributes, which not only monitor the incoming/outgoing packet/byte rate, but also compile the TCP, SYN, and ACK flag rates, to describe the traffic flow pattern. The decision tree technique is applied to develop a classifier to detect abnormal traffic flow.

Nguyen & Choi (2010) develop a method for proactive detection of DDoS attacks by classifying the network status. They break a DDoS attack into phases and select features based on an investigation of DDoS attacks. Finally, they apply the k-nearest neighbor (KNN) method to classify the network status in each phase of DDoS attack. A method presented by Shiaeles et al (2012) detects DDoS attacks based on a fuzzy estimate using mean packet inter-arrival times. It detects the suspected host and traces the IP address to drop packets within 3 second detection windows.

Lately ensembles of classifiers have been used for DDoS attack detection. The use of an ensemble reduces the bias of existing individual classifiers. An ensemble of classifiers has been used by Kumar & Selvakumar (2011) for this purpose where a Resilient Back Propagation (RBP) neural network is chosen as the base classifier. The main focus of this paper is to improve the performance of the base classifier. The proposed classification algorithm, RBPBoost combines the output of the ensemble of classifier outputs and Neyman Pearson cost minimization strategy Scott & Nowak (2005) for final classification decision.

Gupta et al (2012) use ANN to estimate the number of zombies in a DDoS attack. They use sample data to train a feed-forward neural network generated using the NS-2 network simulator. The generalization capacity of
the trained network is promising and the network is able to predict the number of zombies involved in a DDoS attack with test error.

### 2.3.3 Knowledge Based

In knowledge-based approaches, network events are checked against predefined rules or patterns of attack. In these approaches, general representations of known attacks are formulated to identify actual occurrences of attacks.

Gil & Poletto (2001) introduce a heuristic along with a data structure called MULTOPS (MUlti-Level Tree for Online Packet Statistics), that monitor certain traffic characteristics which can be used by network devices such as routers to detect and eliminate DDoS attacks. MULTOPS is a tree of nodes that contains packet rate statistics for subnet prefixes at different aggregation levels. Expansion and contraction of the tree occur within a pre-specified memory size. A network device using MULTOPS detects ongoing bandwidth attacks by the presence of a significant and disproportional difference between packet rates going to and coming from the victim or the attacker. Depending on their setup and their location on the network, MULTOPS equipped routers or network monitors may fail to detect a bandwidth attack that is mounted by attackers that randomizes IP source addresses on malicious packets. MULTOPS fails to detect attacks that deploy a large number of proportional flows to cripple a victim.

Thomas et al (2003) present an approach to DDoS defense called NetBouncer and claim it to be a practical approach to high performance. Their approach relies on distinguishing legitimate and illegitimate use and ensuring that resources are made available only for legitimate use. NetBouncer allows traffic to flow with reference to a long list of proven legitimate clients. If packets are received from a client (source) not on the legitimate list, a
NetBouncer device proceeds to administer a variety of legitimacy tests to challenge the client to prove its legitimacy. If a client can pass these tests, it is added to the legitimacy list and subsequent packets from the client are accepted until a certain legitimacy window expires.

Obtaining a set of relevant features is a difficult problem in machine learning Langely (1994). As such, the focus of much of the prior work using machine learning techniques has been on demonstrating the ability of algorithms to group together flows according to application type and not on classifying traffic (Erman et al 2006, Hernandez et al 2003, McGregor et al 2004, Roughan et al 2004, Zander et al 2005 and Zander 2006). These techniques generally use only features obtained from a single flow such as packet sizes, interarrival times, or aggregate statistics. These approaches do not consider the application labels of the flows when forming the groups.

Hernandez-Campos et al (2003) studied, using an abstract model, how to represent application level communications. Their abstract model represents the communication patterns of a flow in “epochs” that store the amount of data traveling to both the sender and receiver, and the idle time between exchanges. The feature vectors for a flow are extracted from these epochs. Hernandez-Campos et al (2003) then use hierarchical clustering to group the flows based on similarity. They found when 5,000 flows were clustered that many of the clusters corresponded roughly to a single application. For example, one of their clusters contained web flows and another contained flows from mail protocols.

Roughan et al (2004) classified flows into four predetermined traffic classes (interactive, bulk data transfer, streaming, and transactional) using the Nearest Neighbor and the Linear Discriminate Analysis classification techniques. Roughan et al (2004) show that it is possible to
successfully separate the flows of different traffic classes using only flow statistics and give explanations to why their chosen flow statistics (average packet size, and flow duration) would work for the different traffic classes they studied.

McGregor et al (2004) analyzed packet sizes and interarrival times of different application types to determine whether different applications exhibit different packet size and interarrival characteristics. In analyzing plots of packet sizes and interarrival times, they found that while there were some distinguishing characteristics between applications it would be difficult to do rich traffic classification. McGregor et al. then proposed a methodology to use Expectation Maximization (EM) clustering that will group flows using flow statistics including byte counts, connection durations, and packet size statistics. The authors conducted a preliminary analysis using cluster visualization to examine the clusters and find that many of the clusters correspond to a single type of traffic class such as bulk data transfers and DNS traffic.

Zander et al 2005 and Nguyen et al 2005 extend the aforementioned work. Specifically, they look at maximizing intra-cluster homogeneity (or cluster purity) by investigating which set of features separate the flows from different applications with greatest accuracy. The traces used in this analysis are from a publicly available archive of traces and port-based analysis was used to establish the “base truth”. The authors have continued this work and recently used the C4.5 supervised machine learning algorithm to estimate the traffic trends in archival traces Zander et al (2006).

Wang et al (2010) present a formal and methodical way of modeling DDoS attacks using Augmented Attack Tree (AAT), and discuss an AAT-based attack detection algorithm. This model explicitly captures the particular subtle incidents triggered by a DDoS attack and the corresponding
state transitions from the view of the network traffic transmission to the primary victim server. Two major contributions of this paper are: (1) an AAT-based DDoS model (ADDoSAT), developed to assess potential threat from malicious packets to the primary victim server and to facilitate the detection of such attacks; (2) an AAT-based bottom up detection algorithm proposed to detect all kinds of attacks based on AAT modeling. Compared with the conventional attack tree modeling method, AAT is advanced because it provides additional information, especially about the state transition process. As a result, it overcomes the shortcomings of CAT modeling. There is currently no established AAT-based bottom up procedure for detecting network intrusions.

Dusi et al (2009) propose a statistical classification mechanism that could represent an important step towards new techniques for securing network boundaries. The mechanism, called Tunnel Hunter, relies on the statistical characterization at the IP-layer of the traffic that is allowed by a given security policy, such as HTTP or SSH. The statistical profiles of the allowed usages of those protocols can then be dynamically checked against traffic flows crossing the network boundaries, identifying with great accuracy when a flow is being used to tunnel another protocol.

Neto et al (2013) describes a traffic classification in the dark mechanism based on matching several empirical distributions representing computer applications with the one of the target traffic. The classifier combines two methods for performing such matching in real-time and on a packet-by-packet manner: one based on the Kolmogorov-Smirnov test, and another one based on the Chi-Squared test.

Limwiwatkul & Rungsawang (2004) propose to discover DDoS attack signatures by analyzing the TCP/IP packet header against well-defined rules and conditions, and distinguishing the difference between normal and
abnormal traffic. The authors mainly focus on ICMP, TCP and UDP flooding attacks. Zhang & Parashar (2006) propose a distributed approach to defend against DDoS attacks by coordinating across the Internet. Unlike traditional IDS, it detects and stops DDoS attacks within the intermediate network. In the proposed approach, DDoS defense systems are deployed in the network to detect DDoS attacks independently. A gossip based communication mechanism is used to exchange information about network attacks between these independent detection nodes to aggregate information about the overall network attacks. Using the aggregated information, individual defense nodes obtain approximate information about global network attacks and can stop them more effectively and accurately. For fast and reliable dissemination of attack information, the network grows as a peer-to-peer overlay network on top of the Internet. Previously proposed approaches rely on monitoring the volume of traffic that is received by the victim. Most such approaches are incapable of differentiating a DDoS attack from a flash crowd. Lu et al (2007) describe a perimeter-based anti-DDoS system, in which the traffic is analyzed only at the edge routers of an Internet Service Provider (ISP) network. The anti-DDoS system consists of two major components: (1) temporal-correlation based feature extraction and (2) spatial-correlation based detection. The scheme can accurately detect DDoS attacks and identify attack packets without modifying existing IP forwarding mechanisms at routers.

2.3.4 Data Mining and Machine Learning

Redhwan Saad et al (2013) analyzed the various data mining algorithms such as Classification, Link Analysis, and Sequence Analysis in the field of intrusion detection in IPv6 networks. They conclude that the applicability of this algorithm in real time condition is worth to be solved. Chandrashekhar Azad & Vijay Kumar Jha (2013) comprehensively analyzed the application and efficiency of various data mining algorithms in intrusion
detection techniques. The analysis showed that the top three data mining algorithms used are Naïve Bayes Classifier, Support Vector Machines and Hidden Markov Model.

Mohan Banerjee & Roopali Soni (2013) discuss the application of k-means clustering via Naïve Bayes classification in intrusion detection. The combination of these two algorithms used in order to improve accuracy, precision rate and reduce the false positive rate. In this paper, we apply one of the efficient data mining algorithms called k-means clustering via naïve bayes classification for anomaly based network intrusion detection. Experimental results on the KDD cup’99 data set shows the novelty of our approach in detecting network intrusion. It is observed that the proposed technique performs better in terms of Detection rate when applied to KDD’99 data sets compared to a naïve bayes based approach.

Mradul Dhakar & Akhilesh Tiwari (2014) propose a novel hybrid model for intrusion detection. The framework utilizes the crucial data mining-classification algorithms beneficial for intrusion detection. The proposed system is a hybrid intrusion detection framework based on the combination of two classifiers i.e. Tree Augmented Naïve Bayes (TAN) and Reduced Error Pruning (REP). The TAN classifier is used as a base classifier while the REP classifier is used as a Meta classifier. The Meta classification is the learning technique which learns from the Meta data and judge the correctness of the classification of each instance by base classifier. Experimental assessment shows that the developed framework has reduced the false alarm rate and increased the accuracy up to noteworthy extend which is a major concern in case of intrusion detection mechanism. Shuhai Zhang et al (2013) proposed a new approach that improves improves the particle swarm optimization algorithm and presents an attribute-weighted distance calculation method based on information gain ratio. This method for the division of spherical or
ellipsoidal data can obtain better clustering results. And the data set of KDD-cup 99 is used as the experimental data. The experimental results show that the method can detect many kinds of known network intrusion and also can detect many unknown network intrusions. At the same time, the method can maintain the higher intrusion detection rate and lower false alarm rate.

The attribute-weighted intrusion detection algorithm proposed by Lifang Wang et al (2013) is based on the information gain ratio firstly uses the improved particle swarm optimization to find the initial clustering core, secondly runs K-means. The algorithm proposed combines the stronger global optimization of the improved particle swarm optimization and the faster iteration speed of K-means to overcome the sensitive problem of the initial clustering selection and also solve the slow convergence of the improved particle swarm optimization.

Shih Yin Ooi et al (2013) analyzes the ID3, C4.5, and Best-First Tree is tested on NSL-KDD network intrusion dataset. The decision trees generated are used as a predictive model to detect anomaly connection for every unlabeled record in the test set depending on the selected features. The features are selected by using Consistency Subset Evaluator. From the experiment, it appears as the most optimal feature selection technique from WEKA to prepare the attributes for further classification through ID3, C4.5, and Best First Trees. Consistency Subset Evaluator filters unhelpful attributes while maintaining the consistency and hence able to increase the accuracy of algorithms by using lesser features.

Lee et al (2008) proposes a method for proactive detection of DDoS attacks by exploiting an architecture consisting of a selection of handlers and agents that communicate compromise and attack. The method performs cluster analysis. The authors experiment with the DARPA 2000 Intrusion Detection Scenario Specific Dataset to evaluate the method. The results show
that each phase of the attack scenario is partitioned well and can detect precursors of a DDoS attack as well as the attack itself.

Genetic Algorithm (GA) based DDoS detection strategy was introduced in Sang Min Lee et al (2012). This technique uses optimized traffic matrix with a reduced computational overhead in the formation of the matrix. The experiments were conducted using the DARPA 2000 dataset and this approach detects the attacks with short detection delay. This approach can be used in real time, since it employs only the source IP address and the arrival time of the incoming packet to construct the optimized traffic matrix. Fuzzy logic can also be used in DDoS detection algorithms. Fuzzy estimator Stavros et al (2012) based DDoS detection divides the entire problem into two stages. First stage detection of the occurrence of the DDoS attack and next identifying the source(s) of the attack. This method uses the arrival time of the packets as the main metric. Because of this, it produces a high number of false positives, but at the same time, the source of the DDoS attack was correctly and timely identified.

Sekar et al (2006) investigates the design space for in-network DDoS detection and propose a triggered, multi-stage approach that addresses both scalability and accuracy. Their contribution is the design and implementation of LADS (Large-scale Automated DDoS detection System). The system makes effective use of the data (such as NetFlow and SNMP feeds from routers) readily available to an ISP.

Zhong & Yue (2010) present a DDoS attack detection model that extracts a network traffic model and a network packet protocol status model and sets the threshold for the detection model. Captured network traffic values are clustered based on the k-means clustering algorithm to build initial threshold values for network traffic. All captured packets are used to build the packet protocol status model using the Apriori, Agrawal & Srikant (1994) and
FCM, Dunn (1973) algorithms. Whenever the current network traffic is over the threshold value, the network packet protocol status is checked to detect abnormal packets. If there are no abnormal packets, the current network traffic is clustered again by the k-means module to build a new threshold value model.

Cheng et al (2009) propose the IAI (IP Address Interaction Feature) algorithm considering interactions among addresses, abrupt traffic changes, many-to-one asymmetries among addresses, distributed source IP addresses and concentrated target addresses. The IAI algorithm is designed to describe the essential characteristics of network flow states. Furthermore, a support vector machine (SVM) classifier, which is trained by an IAI time series from the normal flow and attack flow, is applied to classify the state of the current network flows and identify the DDoS attacks. Experimental results show that the IAI-based detection scheme can distinguish between normal flows and abnormal flows with DDoS attacks effectively, and help identify fast and accurate attack flows when the attacking traffic is hidden among a relatively large volume of normal flows or close to the attacking sources. In addition, it has higher detection and lower false alarm rates compared to competing techniques.

Md. Al Mehedi Hasan et al (2014) compares Support Vector Machine and Random Forest classifiers for intrusion detection. The performances of these two approaches have been observed on the basis of their accuracy, false negative rate and precision. The results indicate that the ability of the SVM classification produces more accurate results than Random Forest and RF takes less time to train the classifier than SVM.

A two-stage automated system is proposed in Dainotti et al (2009) to detect DoS attacks in network traffic. It combines the traditional change point detection approach with a novel one based on continuous wavelet
transforms Haar (1910). The authors test the system using a set of publicly available attack-free traffic traces superimposed with anomaly profiles.

Li & Lee (2003) present a systematic wavelet based method for DDoS attack detection. They use energy distribution based on wavelet analysis to detect DDoS attack traffic. Energy distribution over time has limited variation if the traffic keeps its behavior over time. Gupta et al (2012) use ANN to estimate the number of zombies in a DDoS attack. They use sample data to train a feed-forward neural network generated using the NS-2 network simulator. The generalization capacity of the trained network is promising and the network is able to predict the number of zombies involved in a DDoS attack with test error. A port-to-port specific traffic on a router, called IF flow is introduced in Yan et al (2008). An important feature of IF is that it can amplify the attack to normal traffic ratio. An RLS (recursive least squares) filter is used to predict IF flows. Next, a statistical method using a residual filtered process is used to detect anomalies. Finally, the authors applied the method to three types of traffic: IF flows, input links and output links within a router, and compare the anomaly detection results using ROC curves. Results show that IF flows are more powerful than input links and output links for DDoS attack detection. Cheng et al (2009) proposes the IAI (IP Address Interaction Feature) algorithm considering interactions among addresses, abrupt traffic changes, many-to-one asymmetries among addresses, distributed source IP addresses and concentrated target addresses Cheng et al (2009). The IAI algorithm is designed to describe the essential characteristics of network flow states. Furthermore, a support vector machine (SVM) classifier, which is trained by an IAI time series from the normal flow and attack flow, is applied to classify the state of the current network flows and identify the DDoS attacks. Experimental results show that the IAI-based detection scheme can distinguish between normal flows and abnormal flows with DDoS attacks effectively, and help identify fast and accurate attack
flows when the attacking traffic is hidden among a relatively large volume of normal flows or close to the attacking sources. In addition, it has higher detection and lower false alarm rates compared to competing techniques.

The method presented in Xia et al (2010) can identify flooding attacks in real time and also can assess the intensity of the attackers based on fuzzy reasoning. The process consists of two stages: (i) statistical analysis of the network traffic time series using discrete wavelet transform and Schwarz information criterion (SIC) to find the change point of the Hurst parameters resulting from DDoS flood attacks, and then (ii) identification and assessment of the intensity of the DDoS attack adaptively based on an intelligent fuzzy reasoning mechanism. Test results from ns2 based simulation with various network traffic characteristics and attack intensities demonstrate that the method could detect DDoS flood attack timely, effectively and intelligently. Zhang et al (2012) present a CPR (Congestion Participation Rate) based approach to detect low-rate DDoS (LDDoS) attack using flow level network traffic. A flow with higher CPR value leads to LDDoS and consequent dropping of the packets. The authors evaluate the mechanism using ns2 simulation; testbed experiments and Internet traffic trace and claim that the method can detect LDDoS flows effectively. Another protocol specific feature based DDoS attack detection mechanism is introduced in Kashyap & Bhattacharyya (2012). It identifies a most relevant subset of features using correlation and can detect DDoS attacks with high detection accuracy. In Gelenbe & Loukas (2007), a mathematical model is presented to provide a gross evaluation of the benefits of DDoS defense based on dropping of attack traffic. Simulation results and testbed experiments are used to validate the model. In the same work, the authors also consider an autonomic defense mechanism based on the CPN (Cognitive packet Network) protocol and establish it to be capable of tracing back flows coming into a node automatically. Ghanea-Hercock et al (2007) provide a survey of the
techniques within the Hyperion project. They also suggest overall system architecture to improve the situational awareness of field commanders by providing an option to fuse and compose information services in real time. Gelenbe (2009) describes an approach to develop a self-aware network to provide end users the option to explore the state of the network to find the best ways to meet their communication needs. In Gelenbe (2011), a model is introduced for searching by N agents in an unbounded random environment. The model allows for the loss or destruction of searchers and finite lifetime.

2.4 SUMMARY

A detailed survey of the various IPv6 security issues and DDoS detection algorithms proposed so far in various literatures worldwide has been presented in this chapter. The demerits of various statistics, knowledge based, soft computing and data mining algorithms are analyzed. The limitations of using a single detection algorithm to detect DDoS attack are also presented. Need for a combined approach which works better in terms of speed and accuracy has also been discussed.