Volume XXII 2019
ISSUE no.1
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

DDoS detection and prevention based on artificial intelligence techniques

To cite this article: D. Glăvan, C. Răcuciu, R. Moinescu and N. F. Antonie, Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg. 134-143.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I1-018

DDoS Detection and Prevention Based on Artificial Intelligence Techniques

Dragoș Glăvan, Ciprian Răcuciu, Radu Moinescu, Narcis-Florentin Antonie

Military Technical Academy „Ferdinand I” – Systems Engineering for Defense and Security
dragos.glavan@gmail.com

Abstract. Distributed Denial of Service (DDoS) attacks have been the major threats for the Internet and can bring great loss to companies and governments. With the development of emerging technologies, such as cloud computing, Internet of Things (IoT), artificial intelligence techniques, attackers can launch a huge volume of DDoS attacks with a lower cost, and it is much harder to detect and prevent DDoS attacks, because DDoS traffic is similar to normal traffic. Some artificial intelligence techniques like machine learning algorithms have been used to classify DDoS attack traffic and detect DDoS attacks, such as Naive Bayes and Random forest tree. In the paper, we survey on the latest progress on the DDoS attack detection using artificial intelligence techniques and give recommendations on artificial intelligence techniques to be used in DDoS attack detection and prevention.

1. Introduction

Distributed Denial of Service (DDoS) attack is an attack using multiple distributed resources against targets, which will deprive authorized client from services. Attack targets include system resources, network bandwidth and other resources. DDoS attacks have been the most common and fatal attacks to the Internet. However, DDoS attack is hard to be detected, because attack traffic is similar to normal traffic in most case. DDoS attack is a major threat to availability, because it tries to prevent legitimate traffic between clients and servers. DDoS attacks can be huge volumes of traffic in short time, low volumes of traffic in long time, huge volumes of traffic in long time [4], of which the latter is hard to detect and prevent. With the development of cloud computing, Internet of Things (IoT), artificial intelligence techniques, DDoS attacks have been changing and it becomes harder to detect and prevent DDoS attacks. Even IoT devices can be used to launch DDoS attacks, such as light bulbs.

2. DDoS detection and prevention

2.1. DDoS classifications and features

DDoS attack can multiply the power of attack and have a large impact on the victims. IP spoofing and flooding attacks are two particular DDoS attacks. In IP spoofing, attackers impersonate as a trusted source. While in flooding attack, attackers send too many packets to disrupt the availability of services. There are three kinds of flooding dos attacks: TCP flood attack. Attackers will send too many TCP connection requests without acknowledging the SYN-ACK response server to the target victim server. The server will be down because these half connections consume too many system resources. TCP flood DDoS attack is one of the most commonly used attacks. ICMP flood attack (smurf attack). ICMP flood attack is to send ICMP packets with a spoofed IP source address. The owner of the spoofed IP address will be the potential victim, because it will be destination of many ICMP responses and be flooded. UDP flood attack. UDP flood attack is to send too much UDP packets to different port of a target in random way. DNS amplification attack. DNS amplification attack is an attack that attackers falsify the source address of the victim. The attacker sends a small request to the DNS server and DNS server will reply with a large response.

2.2. DDoS detection and prevention

Most common mechanisms to detect and prevent DDoS include attack prevention, attack detection, and attack reaction. It is hard to detect DDoS attacks, because it is hard to differentiate the attack traffic and normal traffic. When detecting DDoS attacks, the first step is to detect the abnormality from traffic. And machine learning classification methods can be used to differentiate the good and bad packets. Packets that are classified as attack traffic will be dropped. Some features to detect DDoS attack are number of packets, average of packet size, time interval variance, packet size variance, number of bytes, packet rate and bit rate.

2.3. Artificial Intelligence techniques

Typical artificial intelligence techniques include machine learning, speech recognition, and natural language processing. Machine learning algorithms have been applied to DDoS detection and defense, anomaly detection in particular. Most frequently used techniques are Naive Bayes, neural network, and support vector machine.

- Bayes classification

Bayes classifiers are commonly used machine learning classifying methods based on the application of Bayes theorem. Naive Bayes models include simple Bayes and independence Bayes.

- Artificial neuron network

Artificial neuron networks are composed of artificial neurons that can communicate with other neurons. Artificial neuron networks are to solve problems as the brain works and have been used in different fields.

- Support vector machine

Support vector machines are supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Support vector machines can efficiently perform linear and nonlinear classification.

2.4. Trend of DDoS attacks

We can summarize the DDoS trends as follows:

- Largest volumetric attack and highest intensity flood - The number of attacks is decreasing, however, volume, peak attack size and speed are all becoming larger, 36% of attack size peaked over 5 Gbps;
- Multi-vector DDoS attacks are the norm - 30% of DDOS attacks in 2017 uses more than three attack types and 6% utilizes more than 5 types. The more attack types used, it will be more difficult to be detected. TCP and UDP based attacks are two main attack types, including TCP SYN and TCP RST floods. With the increase of DDoS volume, peak attack size and speed, it will be more challenging to detect and mitigate DDoS attacks.

3. Applications of Artificial Intelligence in DDoS attack and prevention

Yuan proposes DeepDefense, a deep learning-based DDoS detection approach, to improve the performance of DDoS attack detection. He formulates the DDoS detection problem as a sequence classification problem and transform the packet-based detection to window-based detection. The DeepDefense is composed of CNN, RNN (recurrent neural network) and fully connected layers. RNN can learn features better than other machine learning methods, especially longer historical features. LSTM and GRU are used to eliminate scaling issues when RNN is used to trace the history from previous packets. RNN also has a better performance in generalization than random forest does.

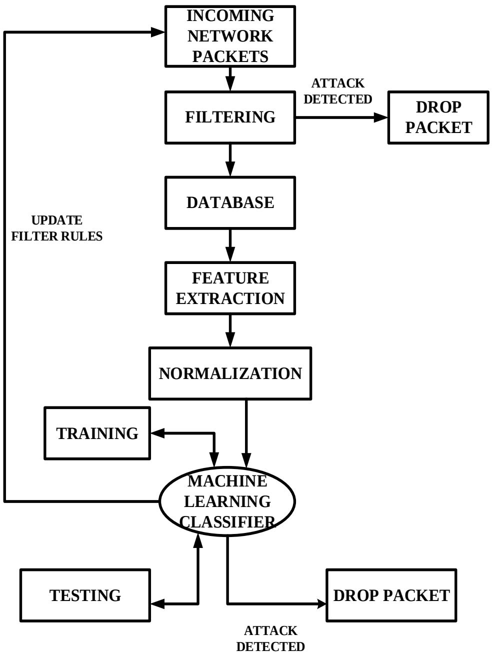

Figure 1 Architecture of DDoS Attack Detection Based on Machine Learning

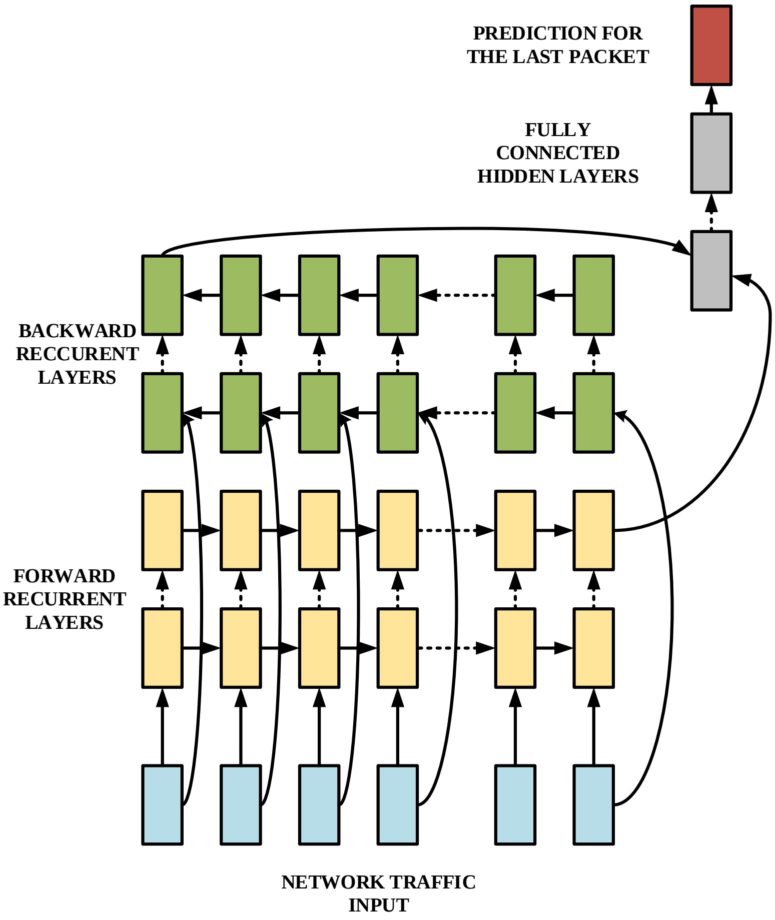
PREDICTION FOR THE LAST PACKET
FULLY CONNECTED HIDDEN LAYERS
BACKWARD RECCURENT LAYERS
FORWARD RECURRENT LAYERS
NETWORK TRAFFIC INPUT

Figure 2 Overall Network Architecture for DeepDefense

Heish proposes a DDoS detection system based on Neural-Network that is composed of five phase, packet collector, Hadoop HDFS, format converter, data processor and neural network detection module. They choose Hadoop distributed file system to store traffic data, use big data platform integrated the neural network to detect DDoS attacks by seven parameters. The detection system can analyze high velocity and volume network traffic and neural network can identify packet features efficiently.

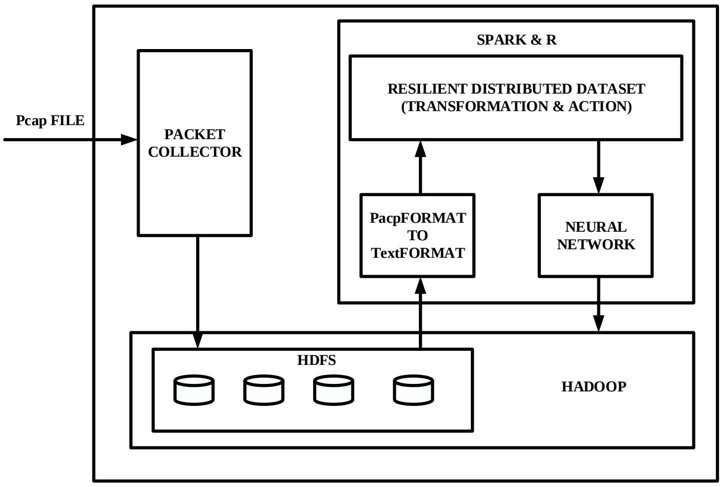

Figure 3 Detection system architecture

Berral extends a framework proposed by Zhang in 2006 to detect and prevent DDoS flood attacks based on machine learning. All nodes in the framework have the ability of learning independently and can react according to different situations. The well known cumulated sum algorithm is used to detect huge traffic volume. Classifiers and detectors are used to distinguish pattern of normal traffic, such as Naive Bayes. Each node has the algorithm that compares the accumulated sum of means for each time unit with a characteristic threshold to classify message. The mechanism can stop and avoid DDoS flood attacks or abuse at early time.

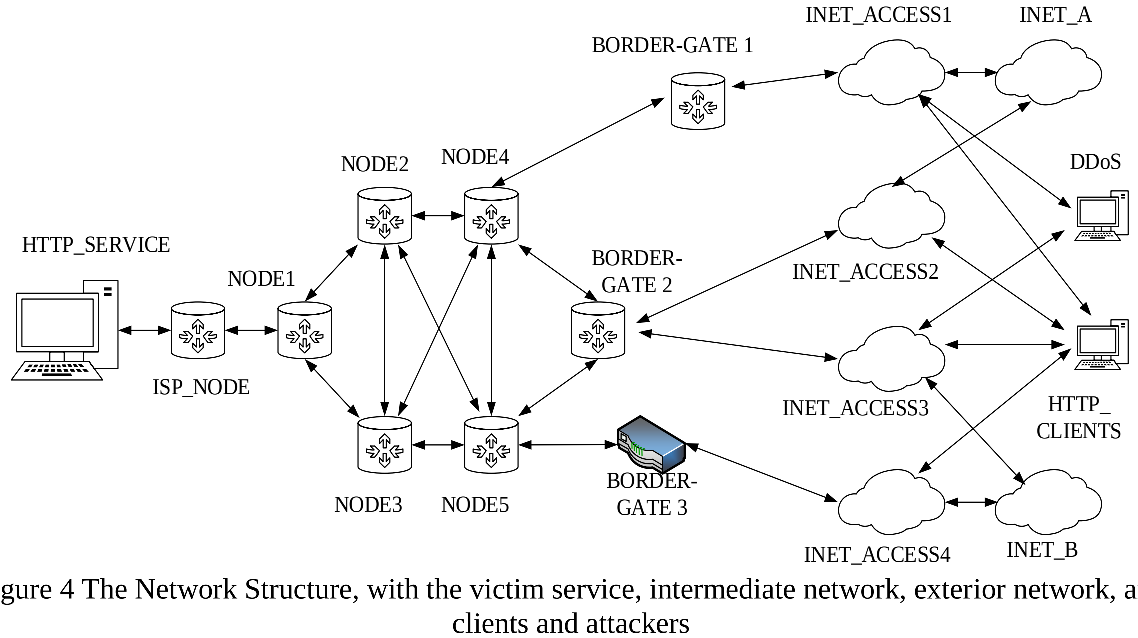

Figure 4 The Network Structure, with the victim service, intermediate network, exterior network, and clients and attackers

Kiruthika proposes a DDoS attack detection and mitigation model using machine learning algorithm. The model is composed of online monitoring system (OMS), spoofed traffic detection module and interface-based rate limiting algorithm. OMS uses automated tools and scripts to monitor the degradation and provide DDoS impact measurements. The spoofed traffic detection module incorporates hop count inspection algorithm to check the authenticity of incoming packet. He constructs legitimate records with IP and hop count to detect potential attacks. Hop count inspection algorithm is to check the authenticity of packet. HCF-SVM is trained and updated with source IP and respective hop count. The performance of the model is better than random forest and decision tree when classifying instance.

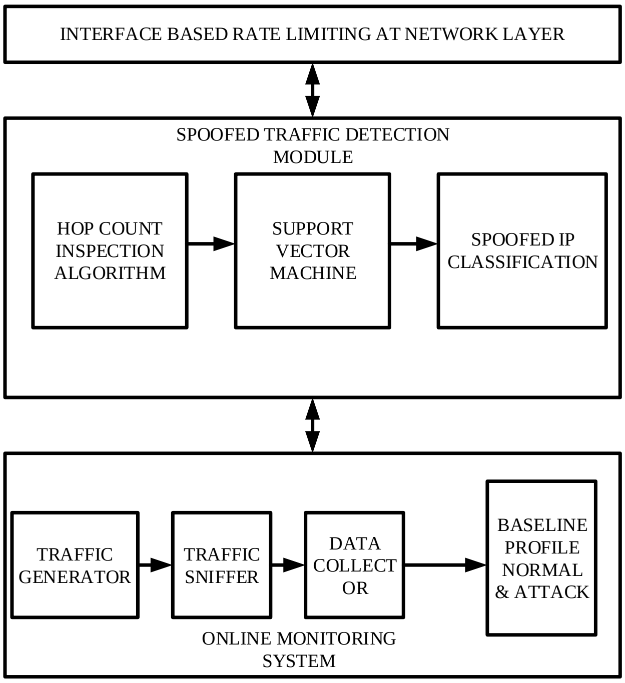
INTERFACE BASED RATE LIMITING AT NETWORK LAYER
SPOOFED TRAFFIC DETECTION MODULE
HOP COUNT INSPECTION ALGORITHM
SUPPORT VECTOR MACHINE
SPOOFED IP CLASSIFICATION
TRAFFIC GENERATOR
TRAFFIC SNIFFER
DATA COLLECT OR
BASELINE PROFILE NORMAL & ATTACK
ONLINE MONITORING SYSTEM

Figure 5 Proposed Model

Zhao develops a DDoS detection system based on neural network and implements in Apache Hadoop cluster and HBase system. The system has a neural network architecture that has the ability of adapting to new types of DDoS attacks. A Hadoop and HBase cluster is setup to process huge traffic, then a neural network model is designed to detect DDoS attacks. The neural network selects parameters from Hadoop and HBase cluster module, such as CPU usage, packet size and total number of TCP connections. He chooses the multi-factor detection approach instead of single factor detection approach to detect DDoS attack, which can improve the performance of detection.

Meitei design a model of system based on ANN and the packet header statistical information to detect DDoS DNS amplification attack. They classify the DNS traffic using machine learning classification algorithms, including decision tree, multi-layer perception (MLP), Naive Bayes and support vector machine (SVM). Then choose decision tree as machine learning classification models for its best performance. The selection approach is attributed based, optimal features are extracted from attributed selection algorithms like information gain, gain ratio and chi square. The feature parameters selected are inter packet arrival time, probability of occurrence of one IP address, answer, additional and authority of resource record, minimum packet size, average packet size and maximum packet size.

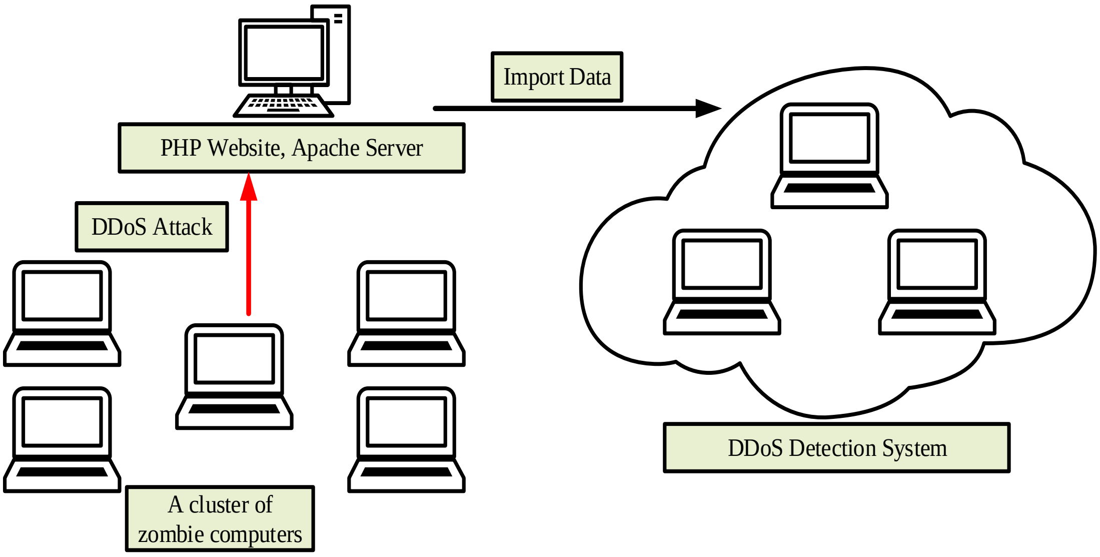

Figure 6 The overall process for the designed scenario

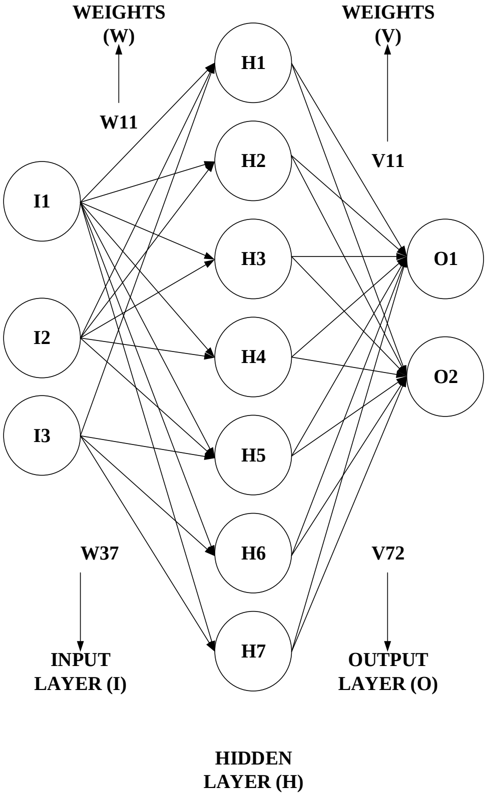

Figure 7 The neural network architecture for DDoS detection system

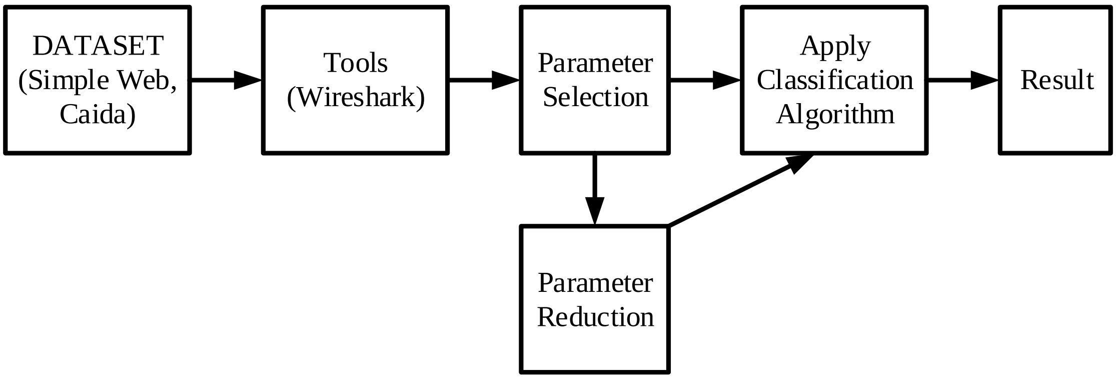

Figure 8 Model of Proposed system

Ndibwile proposes a simple network architecture that makes use of real web server, Bait server, and Decoy web servers to distinguish DDoS traffic from normal traffic. The architecture use a customized Intrusion Prevention System (IPS) at the network gateway that use rules generated by random tree machine learning algorithm through supervised learning. Decision tree is chosen to classify malicious traffic from normal traffic. Random tree machine learning algorithm using labeled datasets is used to avoid false positive traffic.

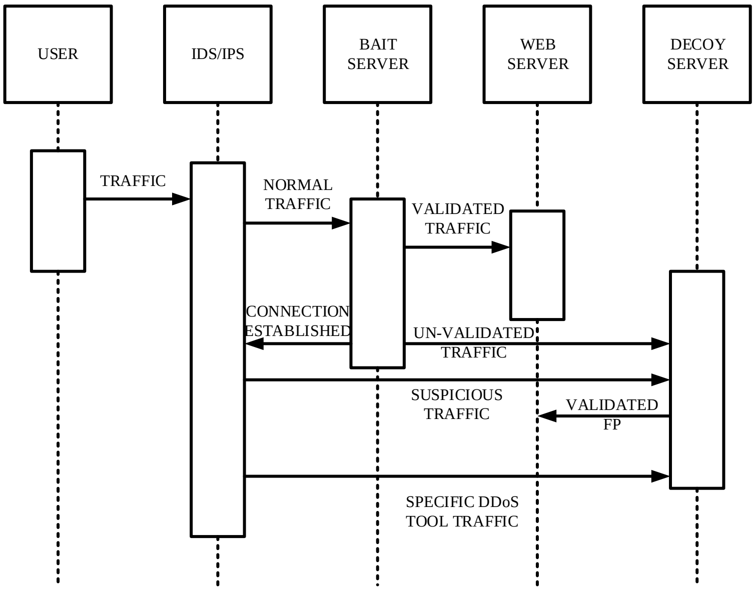

Figure 9 Mitigation of DDoS attack traffic sequence

Ramadhan designs a TCP flood DDoS detection system which uses Artificial Immune System(AIS). The system is composed of two main component, collection data and analysis data. In the AIS, there are many algorithms based on human immune functions, principles and models can be applied to detect attacks, such as Dendritic Cell Algorithm(DCA). The four phase of DCA are preprocessing and initialization phase, detection phase, context assessment phase, and classification phase. The system presents DDoS attack by danger signals. Danger signals has been predefined as danger, safe, PAMA and inflammation. PAMA is a confident indicator of an abnormality and different signals indicate different kinds of attacks.

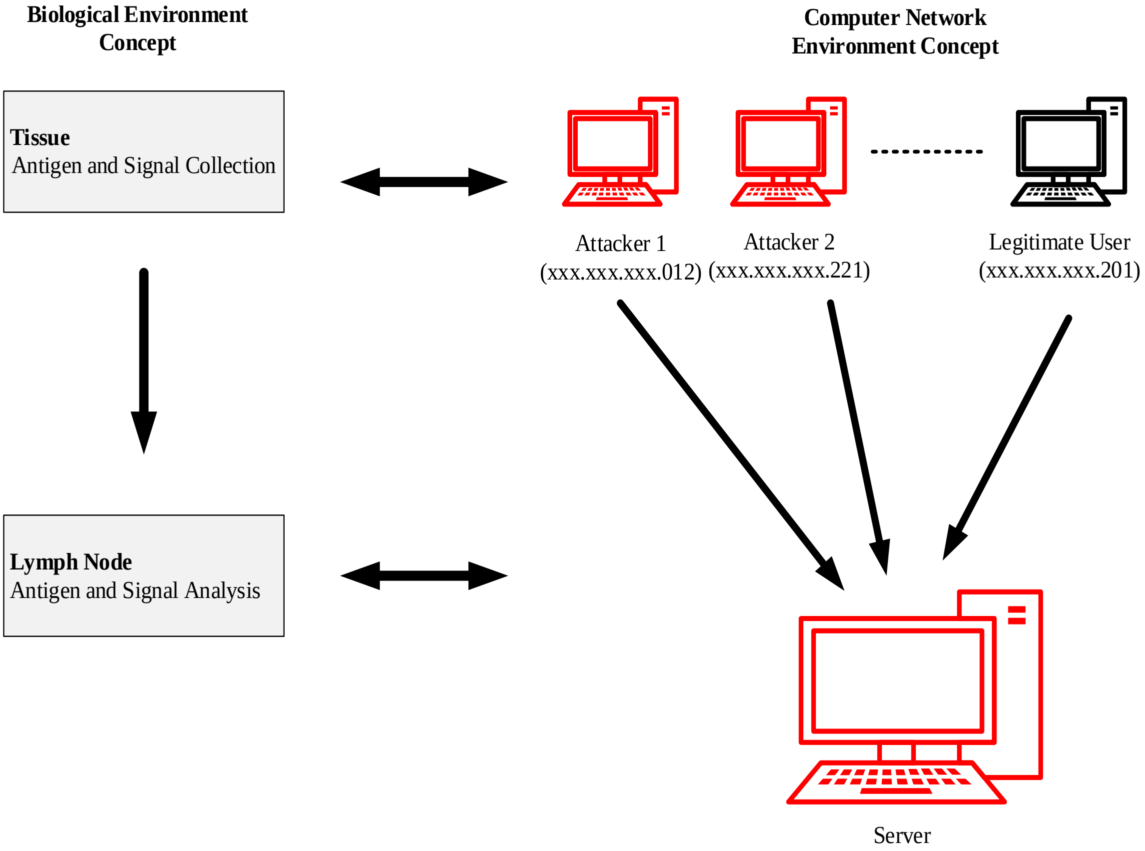
Biological Environment Concept
Computer Network Environment Concept
Tissue
Antigen and Signal Collection
Attacker 1
(xxx.xxx.xxx.012)
Attacker 2
(xxx.xxx.xxx.221)
Legitimate User
(xxx.xxx.xxx.201)
Lymph Node
Antigen and Signal Analysis
Server

Figure 10 Dentritic cell algorithm data structure

Peraković develops a detection and classification model system based on artificial neural network (ANN) architecture to detect DDoS attack. In the developed ANN model, traffic are classified as four kinds, class-DNS DDoS attack traffic, chargen DDoS attack traffic, UDP DDoS attack traffic and normal traffic. Parameters used in detection of DDoS are source IP address, destination IP address, protocol and packet length. Because of the correspondence of the features of UDP DDoS attack and those of normal traffic, the accuracy in detection and classification of UDP DDoS attacks is a little lower.

Anomaly based detection technique models the behavior of normal traffic to distinguish attack traffic from normal while the signature-based detection uses pattern matching to compare data instance with the signature already stored in the database. Machine learning based classifiers are experts in finding out patterns in the dataset with the help of features used to describe the data. Machine learning techniques can provide decision aids for the analysts and can automatically generate rules to be used for network intrusion detection system. Classifiers are tools that classify data based on specified features or patterns present in that data. Some of the worth noticing works in the field of DDoS detection includes the work of Gil and Poletto, in which they assume that packet rates between two hosts are proportional during normal operation. The work make use of a dynamic tree structure known as Multi Level Tree for Online packet statistics structure for monitoring packet rates for each IP address.

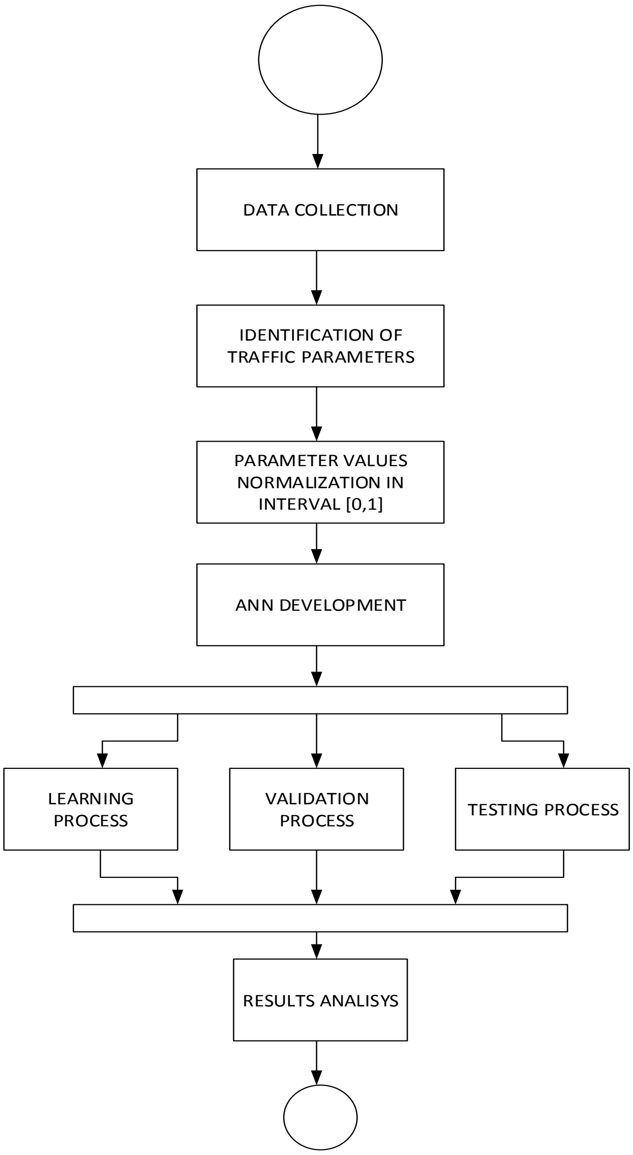

Figure 11 UML Activity diagram of proposed model development

4. Conclusion

DDoS attacks have been the major threats for the Internet and can bring great loss to companies and government. With the development of emerging technologies, such as cloud computing, Internet of things, artificial intelligence techniques, attackers can launch DDoS attacks with a low cost, and it becomes much harder to detect and prevent DDoS attacks. Some artificial intelligence techniques like machine learning algorithms have been used to classify DDoS attack traffic and detect DDoS attack, such as Naive Bayes and Random forest tree. In the paper, we survey on the latest progress on the DDoS attack detection using artificial intelligence techniques. Features that can be used to detect DDoS attack, such as number of packets, average of packet size, time interval variance, packet size variance, number of bytes, packet rate and bit rate. Among those artificial intelligence techniques, we recommend that random forest tree and Naive Bayes are used to classify malicious traffic and normal traffic for their better performance. Multi machine algorithms can be combined to detect DDoS attacks, which will have a better accuracy and performance.

References

[1] X. Yuan, C. Li and X. Li, *DeepDefense: Identifying DDoS Attack via Deep Learning*, IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, 2017

[2] M. Guri, Y. Mirsky and Y. Elovici, *DDoS: Attacks, Analysis and Mitigation*, 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 2017;

[3] R. F. Fouladi, C. E. Kayatas and E. Anarim, *Frequency based DDoS attack detection approach using naive Bayes classification*, 39th International Conference on Telecommunications and Signal Processing (TSP), Vienna, 2016;

[4] C. J. Hsieh and T. Y. Chan, *Detection DDoS attacks based on neural-network using Apache Spark*, International Conference on Applied System Innovation (ICASI), Okinawa, 2016;

[5] Zejun Ren, Xiangang Liu, Runguo Ye, Tao Zhang, *Security and Privacy on Internet of Things*, IEEE 7th International Conference on Electronics Information and Emergency Communication (ICEIEC 2017), Shenzhen, 2017;

[6] B. S. Kiruthika Devi, G. Preetha, G. Selvaram and S. Mercy Shalinie, *An impact analysis: Real time DDoS attack detection and mitigation using machine learning*, International Conference on Recent Trends in Information Technology, Chennai, 2014.

[7] G. Ramadhan, Y. Kurniawan and Chang-Soo Kim, *Design of TCP SYN Flood DDoS attack detection using artificial immune systems*, 6th International Conference on System Engineering and Technology (ICSET), Bandung, 2016;

[8] Josep L. Berral, Nicolas Poggi, *Adaptive distributed mechanism against flooding network attacks based on machine learning*, New York;

[9] T. Zhao, *A Neural-Network Based DDoS Detection System Using Hadoop and HBase*, IEEE 17th International Conference on High Performance Computing and Communications, New York, 2015;

[10] Lalit Meitei, Khundrakpam Johnson Singh, *Detection of DDoS DNS Amplification Attack Using Classification Algorithm*, International Conference on Informatics and Analytics, New York;

[11] J. D. Ndibwile, A. Govardhan, *Web Server Protection against Application Layer DDoS Attacks Using Machine Learning and Traffic Authentication*, IEEE 39th Annual Computer Software and Applications Conference, Taichung, 2015;

[12] D. Peraković, M. Periša, *Artificial neuron network implementation in detection and classification of DDoS traffic*, 24th Telecommunications Forum (TELFOR), Belgrade, 2016.