Reference article page: https://ieeexplore.ieee.org/document/9502698

Distributed Denial of Service (DDoS) is flooding threats that deny a legitimate user from accessing its intended service. Typically, attackers will create an illegal account to install the DDoS main program on a computer and install agents on many other computers on the Internet. During the attacking session, the main program will send orders to the agents. Once the agents receive the orders, the agents will attack the targets. It is one of the most prevalent threats that the Cybersecurity industry faces, as per the recent market research. Therefore, it is crucial to understand and detect different DDoS threats. There are mainly two major types of DDoS attacks refection-based and exploitation-based, and each of the DDoS attacks falls into either of the two categories.

Reflection-based DDoS threats are those kinds of attacks in which the hacker hides its identity by using third-party tools and components. The attack is initiated by sending the data packets to a reflector server with the source and IP address of the victim/target. These attacks are executed through the Application layer protocol using either Transport Control Protocol (TCP), User Datagram Protocol, or both of them simultaneously. The TCP-based attacks include MSSQL, SSDP, whereas UDP based attacks include NTP, TFTP and TCP/UDP-based combined attacks include DNS, LDAP, NETBIOS, and SNMP. The Exploitation-based attacks are similar to that of Reflection based attacks, and it also uses third-party software and components to remain anonymous when initiating the attack.

The article introduced several machine learning models to detect DDoS attack by using two datasets, CICDoS2017 and CICDDoS2019 to train the models. After that they use Accuracy, Precision, Recall, and F1 Score to evaluate the result, and report the detection rate with an equation to report the flows. Act Utilitarianism stated that "An action is right (or wrong) to the extent that it increases (or decreases) the total happiness of the affected parties."[1] By applying this rule, the action is right because it increases the total happiness of the affected party. The company will be satisfied with its efficiency on problem solving and further making profits out of it.

The DDoS threats are very costly in terms of bandwidth and power, resulting in the loss of confidential data. Therefore it has become essential to devise better algorithms to detect different types of DDoS Cyberthreats with higher accuracy while considering the computation cost of detecting these threats.

Machine Learning and Deep Learning methods are very useful nowadays. It especially have ability to detect the DDoS attack. Act Utilitarianism can be applied here because these two methods are effective to prevent DDoS attack and bring back the lost for the company due to the attacker. All the methods introduced in the article can be applied, the only difference is that it use different ML algorithm, and different metrics when identifying each type of threats. With Act Utilitarianism, the algorithm is working because these methods can detect and resolve the attacks. Therefore, it can increases the total happiness of the affected party to stop further costs and damages.

[1] Quinn, Michael J. *Ethics for the Information Age*. Pearson Prentice Hall, 2012.