Sample Entropy

Sample Entropy is a method used to detect DDoS attacks in SDN. There are two essential components to DDoS detection using entropy; **window size** and a **threshold**.

Window size is either based on a time period or number of packets. Entropy is calculated within this window to measure uncertainty in the coming packets. To detect an attack, a threshold is needed. If the calculated entropy passes a threshold or is below it, depending on the scheme, an attack is detected.

The main reason for choosing entropy is its ability to measure **randomness** in a network. The higher the randomness, the higher is the entropy and vice versa. Let W be a set of data with n elements and x is an event in the set. Then, the probability of x happening in W is shown in Equation 1. To measure the entropy, referred to as H, we calculate the probability of all elements in the set and sum that as shown in Equation 2.

$$W = \{x_1, x_2, x_3, \ldots, x_n\}$$

$$p_i = \frac{x_i}{n}$$

-------------- [1]

$$H = -\sum_{i=1}^{n} p_i \log p_i$$

-------------- [2]

The entropy will be at its maximum if all elements have equal probabilities. If an element appears more than others, the entropy will be lower. The size of W is called the window size. If there is a continuous stream of incoming data, it will be divided into equal sets that are called windows. In the window, each element and its occurrence are counted.

When packets arrive at the controller, the source address is always new. This is the reason they come to the controller. There has not been an instance of them in the table of the switch so they are passed on to the controller. For every new incoming connection, the controller will install a flow in the switch so that the rest of the incoming packets will be directed to the destination without further processing. Hence, any time a packet is seen in the controller, it is new.

The other known fact about the new packets coming to the controller is that the destination host is in the network of the controller. The network consists of the switches and hosts that are connected to it. Knowing the packet is new and the destination is in the network, the level of randomness can be quantified by calculating the entropy based on a window size. The window size is the number of incoming new packets that are used for calculating entropy. In this case, maximum entropy occurs when each packet is destined to exactly one host. Minimum entropy occurs when all the packets in a window are destined for a single host.

Being able to quantify randomness and have minimum and maximum based on entropy makes it a suitable method for DDoS detection is SDN. Using entropy, it is possible to see its value drop when a large number of packets are attacking one host or a subnet of hosts.