HW2 (35 Points)

1. What is misuse detection? (5 Points)
2. What is anomaly detection? (5 Points)
3. Please briefly discuss the advantages and disadvantages for misuse detection and anomaly detection. (5 Points)
4. In the paper of “Anomaly Detection of Web-Based Attacks”, authors have used “Chebyshev inequality” to quantify the length of the value for an attribute. What is the advantage of using Chebyshev inequality to quantify the anomaly? (5 Points)
5. What is the motivation behind the feature of “Sender IP Neighborhood Density” proposed in the SNARE paper? (5 Points)
6. You have designed a network protocol for a network of a control system. Each node in this network sends two types of packets (say, type-A and type-B). The behavior of the protocol of a node is well defined. Let us consider two scenarios:
   1. A node is expected to always send exactly two or exactly three type-A packets between two type-B packets.
   2. A node is expected to always send at least three type-A packets between two type-B packets.

Please design two finite state machines for these two scenarios, respectively. And show how they can be used to verify the anomaly of a sequence of packets, denoted as “AAAAAABAB”. (5 + 5 Points)