**Thesis Title:** A Framework for Improving the Performance of Signature-based Network Intrusion Detection Systems

**Name:** MENG Yuxin

**Abstract:**
Network Intrusion detection systems (NIDSs) have been widely deployed in different network environments (e.g., banks, schools) to defend against a variety of network attacks (e.g., Trojans, worms). Generally, a network intrusion detection system can be classified into two categories: signature-based NIDS and anomaly-based NIDS. In real-world applications, the signature-based NIDS is more prevalent than the anomaly-based detection as the false alarm rate of the former is much lower than the latter. However, we identify three major issues that can greatly affect the performance of a signature-based NIDS.

**Expensive signature matching.** The traditional signature matching in a signature-based NIDS is too expensive that the computing burden is at least linear to the size of an incoming string. Therefore, the operational burden of a signature-based NIDS could be significantly increased in a large-scale network environment.

**Overhead network packets.** In a large-scale network environment, a signature-based NIDS usually has to drop lots of network packets since the number of incoming packets exceeds its maximum processing capability.

**Massive false alarms.** Although the false alarm rate of a signature-based NIDS is much smaller than that of an anomaly-based NIDS. The number of false alarms generated by a signature-based NIDS can still increase the difficulty in analyzing true alarms and adversely affect the analysis results.

To mitigate the above issues, in this thesis, we propose several approaches in improving the performance of a signature-based NIDS such as Snort in the following three aspects:

**Signature matching improvement.** We design an exclusive signature matching scheme to help perform a more efficient signature matching with the purpose of enhancing the performance of signature matching in a heavy traffic environment.

**Network packet filtration and reduction.** To mitigate this issue, we advocate the method of constructing a packet filter such as blacklist-based packet filter, list-based packet filter and trust-based packet filter to help filter out target network packets for a signature-based NIDS such as Snort in terms of IP reputation. This packet filter can be deployed in front of a signature-based NIDS and reduce its workload in an intensive traffic network.

**False alarm reduction.** To resolve this issue, we design several false alarm filters such as machine-learning based false alarm filters, alarm filters using knowledge-based alert
verification and context-based alarm filters to help reduce false alarms (or non-critical alarms) that are generated by a signature-based NIDS.

**A Framework.** In addition, we further propose a framework by combining the above work to overall improve the performance of a signature-based NIDS such as Snort. As a case study of the framework, we implement an enhanced filter mechanism (shortly EFM) that consists of three major components: a context-aware blacklist-based packet filter, an exclusive signature matching component and a KNN-based false alarm filter. In particular, the component of context-aware blacklist-based packet filter is responsible for filtering out network packets in terms of IP reputation.

The exclusive signature matching component is implemented in the context-aware blacklist-based packet filter and aims to speed up the signature matching. At last, the component of KNN-based false alarm filter is responsible for filtering out false alarms which are produced by the context-aware blacklist-based packet filter and the NIDS.

In the evaluation, the experimental results demonstrate that our framework is promising and by deploying with the EFM, the performance of a signature-based NIDS such as Snort can be improved in the aspects of network packet filtration, signature matching improvement and false alarm reduction.