Chapter 1
Introduction

With the quickly growing use of Internet today, many network applications such as streaming media, email, instant messaging and on-line games are becoming more popular. Therefore, security is an important issue for networks in today's enterprise environment. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. Many methods have been developed to secure network infrastructure and communication methods over the Internet, including firewalls, encryption, and virtual private networks.

Intrusion detection is a relatively new addition to these techniques. Intrusion detection methods started a few years ago. Intrusion detection methods collect and use the information from known types of attacks and use this information to detect whether someone is trying to attack the network or particular hosts. Information collected this way can be used to boost network security, as well as for legal purposes. Both commercial and open-source products of this type are now available. Many vulnerability assessment tools are also available to assess different types of security holes. A comprehensive security system consists of multiple tools, including: a firewall, an IDS (Intrusion Detection System) [1] and an IPS (Intrusion Detection and Prevention System) [2].

An IDS consists of a set of techniques and methods that is used to detect questionable activity on a network. In other words, the IDS shields against 'attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer network.'

Because intrusion attempts always have signatures, like computer viruses, they can be detected using software which analyzes data packets to check if they contain any known Internet protocol intrusion-related signatures or anomalies. Based on a set of signatures and rules, the detection system is able to find and log suspicious activities and generate alerts [3, 4, 5].

Network IDS's (NIDS) are widely used and heavily depended upon. The continuous growth of network traffic and intrusion signature rule sets can affect the performance of these systems. The impact of an under-performing IDS is serious: a passive system will drop large amounts of network traffic and may miss attacks, while an in-line system acts as a bottleneck on network performance.

Snort [6,7] is an open-source NIDS. They are installed on a particular host and detect attacks targeted specifically to that host. Although all intrusion detection methods are still new, Snort is ranked among the top systems available today.

In this thesis, a novel detection architecture is proposed to redesign the original Snort detection engine. A system on Chip (SoC) platform is employed [8,9] to implement two major algorithms: EGF (Event Group Filter) and BCRM (Binary Correlation Match).