Introduction:

Today, the network is the business. Driven by business needs, enterprises and government agencies have developed sophisticated, complex information networks, incorporating technologies as diverse as distributed data storage systems; encryption techniques; Voice over IP (VoIP); remote and wireless access; and Web services. These networks have become more permeable as business partners access services via extranets; customers interact with the network through e-commerce transactions or Customer Relationship Management (CRM) processes; and employees tap into company systems through Virtual Private Networks (VPN).

For hackers, these well-traveled paths make networks more vulnerable than ever before and—with relatively little expertise—hackers have significantly impacted the networks of leading brands or government agencies. Cyber crime is also no longer the prerogative of lone hackers or random attackers. Today disgruntled employees, unethical corporations, even terrorist organizations all look to the Internet as a portal to gather sensitive data and instigate economic and political disruption.

With networks more vulnerable and hackers equipped to cause havoc, it’s no surprise that network attacks are on the rise. According to a 2001 report by Computer Security Institute (CSI) and the FBI, 70 percent of respondents acknowledged that their networks were attacked over the previous twelve months and 30 percent didn’t know whether their networks were attacked and couldn’t be sure!

In addition, Denial of Service attacks increased by an astonishing 33 percent over the same period. And all this took place across networks, where firewalls and manageable layer 2 switches had been installed in 90 percent of instances.

It’s clear that enterprises and government agencies need security vendors to step up and deliver innovative solutions that effectively protect their networks from malicious attacks and misuse.

Present state of knowledge:

When most people think of network security, they think Firewall. Firewalls are widely deployed as a first level of protection in a multi-layer security architecture, primarily acting as an access control device by permitting specific protocols (such as HTTP, DNS, SMTP) to pass between a set of source and destination addresses. Integral to access policy enforcement, firewalls usually inspect data-packet headers to make traffic-flow decisions. In general, they do not inspect the
entire content of the packet and can’t detect or thwart malicious code embedded within normal traffic. It should be noted that routers also offer some rudimentary protection through packet-filtering processes. While firewalls and router-based packet filtering are necessary components of an overall network security topology, they are insufficient on their own.

Network IDS products inspect the entire content of every packet traversing the network to detect malicious activity. This content inspection technique provides deeper packet analysis compared to a firewall or a router. Intrusion Detection Systems are effective when sophisticated attacks are embedded in familiar protocols, such as an HTTP session, which would normally pass undetected by a firewall. It’s not surprising that the processing power required for an Intrusion Detection System is an order of magnitude higher, when compared to a firewall.

Network protocols can be used to facilitate attacks on networked services. One way of carrying out an attack is to manipulate the functional behavior of a protocol.

A protocol’s functional specification (for example, for an Internet protocol it’s RFC) can be used as a guideline when designing and implementing systems that monitor and control incorrect operation. We propose that a specification of a protocol’s normal operational behavior, in addition to its functional specification, could be an essential tool when designing and parameterising systems, such as the dropping mechanism described earlier, that monitor and control a protocol’s nonfunctional anomalous behavior.